



**NON-PERSONAL DATA: CONCEPTUALIZATION OF THE TERM
IN THE LEGAL FRAME AND A COMPARATIVE ANALYSIS
AMONG DIFFERENT JURISDICTIONS**

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY

By

JAISHREE GAUR

Ph. D. REGN NO. PhD/LAW/00702

DEPARTMENT OF LAW

2026

NON-PERSONAL DATA: CONCEPTUALIZATION OF THE TERM IN
THE LEGAL FRAME AND A COMPARATIVE ANALYSIS AMONG
DIFFERENT JURISDICTIONS

BY

Jaishree Gaur

Dr. Kuldeep Singh Panwar

Submitted In partial fulfillment of the requirements for the Degree of
Doctor of Philosophy in Law of Nagaland University



नागालैण्डविश्वविद्यालय

NAGALAND UNIVERSITY

(संसदद्वारापारितअधिनियम1989, क्रमांक35केअंतर्गतस्थापितकेंद्रीयविश्वविद्यालय)

A Central University established by an Act of Parliament No.35 of 1989)

मुख्यालय : लुमामी, जिला : जुन्हेबोटो (नागालैण्ड), पिनकोड – 798627

Hqrs : Lumami, Dist. Zunheboto (Nagaland), Pin Code – 798627

वेबसाइट / Website : www.nagalanduniversity.ac.in

Department of Law

Ref. No.

Dated-

Certificate

This is to certify that this Ph.D. Thesis entitled, “NON-PERSONAL DATA: CONCEPTUALIZATION OF THE TERM IN THE LEGAL FRAME AND A COMPARATIVE ANALYSIS AMONG DIFFERENT JURISDICTIONS” is an authentic and original work carried out by Ms. Jaishree Gaur bearing Regd. No. PhD/LAW/00702 with effect from 13/09/2022, based on her field study conducted under my supervision.

The Thesis fulfils all the norms of Ph.D. Thesis under the rules and regulations of Nagaland University.

To the best of my knowledge, the Thesis has not been submitted to any university or educational institute for award of any degree or diploma.

This Thesis may therefore be placed before the External Examiner for evaluation.

Dr. Kuldeep Singh Panwar

Dr. Kuldeep Singh Panwar

(Head)

(Supervisor)

DECLARATION

Nagaland University

November, 2025

I, JAISHREE GAUR, hereby declare that the subject matter of this Thesis is the record of work done by me, that the contents of this Thesis did not form basis of the award of any previous degree to me or to the best of my knowledge to anybody else, and that the thesis has not been submitted by me for any research degree in any other University/Institute. This is being submitted to the Nagaland University for the degree of Doctor of Philosophy in Department of Law.

(Scholar)

(Head)

(Supervisor)

ACKNOWLEDGEMENT

With profound gratitude and humility, I first and foremost thank the Almighty for His endless blessings, guidance, and strength throughout this journey. It is only by His grace that I found the perseverance and clarity to overcome challenges and stay true to my purpose.

I express my deepest gratitude to my Supervisor, Dr. Kuldeep Singh Panwar, for his invaluable guidance, encouragement, and patience during the course of my research. His constant motivation, insightful feedback, and unwavering support have been instrumental in shaping the direction and quality of this work. I am truly privileged to have worked under his supervision.

I extend my sincere thanks to all the faculty members and staff of the Department for their continuous support, cooperation, and for fostering an environment conducive to academic growth and research excellence. Their encouragement has played a vital role in the successful completion of this study.

My heartfelt thanks also go to my batchmates, with whom I began this journey, and to my friends at the hostel, who stood by me with care, laughter, and warmth. Their presence and support have made this journey more meaningful and bearable during the most demanding times.

I owe everything to my parents, Dr. Janak Raj and Mrs. Bindu Gaur, whose unconditional love, sacrifices, and faith have been my greatest strength. I am deeply grateful to my sister, Mrs. Vandana Gaur, and brother-in-law, Mr. Harinder Singh Shergill, for their constant encouragement and affection, and to my younger brother, Mr. Manav Raj, for his love, positivity, and unshakeable belief in me. I extend my heartfelt thanks to all my family members, whose blessings and support have sustained me throughout this journey.

I am especially thankful to my best friends, Dr. Marvi and Ms. Shweta Dubey, for being my pillars of strength. Their understanding, endless patience, and ability to listen

to my rants, frustrations, and countless moments of self-doubt have been invaluable. I could not have asked for better companions on this journey.

My sincere gratitude is extended to some very special friends of mine who stood by me during this journey, Ms. Jharna Sharma, Ms. Medha Shekar, Mr. Anvitarth Tripathi, Ms. Mandavi Singh, Ms. Simran Sapra, Ms. Yashika, and Ms. Muskan. Their encouragement, kindness, and unwavering support have meant a great deal to me during the completion of this work.

Finally, I express my sincere appreciation to everyone who has supported, guided, or inspired me in any way. Each gesture of kindness, word of encouragement, and act of help has contributed to the successful completion of this thesis.

Jaishree Gaur

TABLE OF CONTENTS

Contents	Page No.
List of Tables	i
List of Figures	ii
Table of Abbreviations	vii
CHAPTER 1: INTRODUCTION	1
1.1 Introduction	1
1.2 Conceptual Framework	3
1.3 Literature Review	5
1.4 Research Gap	15
1.5 Statement of the Problem	20
1.6 Rationale	22
1.7 Objectives	23
1.8 Hypothesis	23
1.9 Scope and Limitations	23
1.10 Research Methodology	25
1.11 Plan of Study	30
CHAPTER 2: THEORETICAL FOUNDATIONS OF DATA AS AN ASSET: CLASSIFICATION AND TYPOLOGIES	33
2.1 Introduction	33
2.2 Understanding Data	39
2.3 Value of Data	46
2.4 Laws and Governance of Data: Global and Indian Perspectives	61
2.5 Various Types of Data	67
2.6 Major Data Categories: Personal Data and Machine-Generated Data	82
2.7 Conclusion	84
CHAPTER 3: CONCEPTUALISING NON-PERSONAL DATA: DEFINITIONS, SOURCES, TAXONOMIES, AND A PROPOSED LEGAL DEFINITION	86
3.1 Introduction	86
3.2 Defining Non-Personal Data	87
3.3 Classification and Types of Non-Personal Data	98
3.4 Jurisprudence on Non-Personal Data	107
3.5 Stakeholders in the Non-Personal Data Ecosystem	137
3.6 Core Issues and Challenges	141
3.7 Proposed Legal Definition of Non-Personal Data: Analytical and Jurisprudential Explanation	143

3.8 Conclusion	150
CHAPTER 4: COMPARATIVE LEGAL FRAMEWORKS GOVERNING NON-PERSONAL DATA: A CROSS- JURISDICTIONAL ANALYSIS	153
4.1 Introduction	153
4.2 Conceptual Framework for Non-Personal Data Regulation	168
4.3 Country-Specific Analysis	180
4.3.1 EU: Germany	181
4.3.2 EU: France	184
4.3.3 EU: Finland	186
4.3.4 EU: Estonia	189
4.3.5 United States	191
4.3.6 United Kingdom	193
4.3.7 Canada	195
4.3.8 Australia	196
4.3.9 China	198
4.3.10 Japan	200
4.3.11 Singapore	201
4.3.12 South Korea	203
4.3.13 Brazil	205
4.3.14 Kenya	206
4.4 Comparative Analysis	208
4.5 Conclusion	216
CHAPTER 5: GOVERNANCE IMPERATIVES IN NON- PERSONAL DATA: NEED FOR REGULATORY INTERVENTION	220
5.1 Introduction	220
5.2 Rationale for Non-Personal Data Regulation	223
5.3 Proposed Governance Principles	229
5.3.1 Harmonized Definitions	230
5.3.2 Data-Sharing Ecosystems	231
5.3.3 Ethical Governance	232
5.3.4 Balanced Innovation and Control	234
5.3.5 Global Cooperation	235
5.4 Implementation Strategies	236
5.4.1 Policy Development	239
5.4.2 Technological Infrastructure	240
5.4.3 Capacity Building	242
5.4.4 International Collaboration	243
5.5 Conclusion	246

CHAPTER 6: GOVERNANCE FRAMEWORK FOR NON- PERSONAL DATA IN INDIA: EVOLUTION, CHALLENGES, AND PROSPECTS	249
6.1 Introduction	249
6.2 Evolution of Data Governance Framework in India	251
6.3 Analysis of the Proposed Non-Personal Data Governance Framework	259
6.4 Salient Features of Proposed Non-Personal Data Governance Framework	266
6.5 Analysis of Legal Issues Relating to NPD Framework	275
6.6 Non-Personal Data Governance in India – Current Status	280
6.7 Gaps in the Indian NPD Governance Framework	286
6.8 Judicial Status	293
6.9 Conclusion	298
CHAPTER 7: EMPIRICAL ANALYSIS OF LEGAL AWARENESS AND GOVERNANCE OF NON-PERSONAL DATA	302
7.1 Introduction	302
7.2 Public in General	307
7.3 Legal Professionals	327
7.4 Law Students	347
7.5 IT Professionals	367
7.6 Key Comparative Findings	385
7.7 Key Findings of the Overall Analysis	392
7.8 Conclusion	396
CHAPTER 8: CONCLUSION AND RECOMMENDATIONS	397
8.1 Conclusion	397
8.2 Hypothesis Testing	401
8.3 Recommendations	408
8.4 Final Reflection	413
<i>Bibliography</i>	<i>414</i>
<i>Annexures</i>	
<i>Annexure I</i>	
<i>Annexure II</i>	
<i>Annexure III</i>	

List of Tables

Table No.	Title	Page No.
4.1.	Comparative Table	212
5.1.	International Cooperation and Harmonization in Non-Personal Data Governance	244
6.1.	Comparative analysis of Report version1 and Report version 2.	261
7.2.1	Summary of Key Responses from the General Public on Awareness and Perceptions of Non-Personal Data	323
7.3.1.	Summary of Key Responses from Legal Professionals on Awareness and Perceptions of Non-Personal Data	343
7.4.1.	Summary of Key Responses from Law Students on Awareness and Perceptions of Non-Personal Data	362
7.5.1	Summary of Key Responses from IT Professionals on Awareness and Perceptions of Non-Personal Data	381
7.6.1	Consolidated Comparison Table (Common Questions Only)	387
7.6.2	Group-Specific Questions (Non-Common Questions)	389
8.2.1.	Summary of Percentage Responses on Understanding and Distinction Between Personal and Non-Personal Data	401
8.2.2.	Summary of Percentage Responses on Adequacy of Laws, Transparency, and Global Harmonization	404

List of Figures

Figure No.	Title	Page No.
2.1	Data Value Creation	55
2.2	Various types of Data	67
3.1	Types of Non-Personal Data	97
7.2.1	Understanding of Data Concepts	307
7.2.2	Distinction Between Personal and Non-Personal Data	307
7.2.3	Awareness of Indian Legal Framework	308
7.2.4	Need for Legal Provisions on Non-Personal Data	309
7.2.5	Effectiveness of Global Uniform Laws	309
7.2.6	Adequacy of Indian Law for Personal Data Protection	310
7.2.7	Sufficiency of Indian Regulations for Non-Personal Data	311
7.2.8	Awareness of Organizational Use of Non-Personal Data	311
7.2.9	Need for Legal Protection of Non-Personal Data	312
7.2.10	Concern Over Data Usage by Organizations	313
7.2.11	Need for Uniform Global Data Protection Laws	313
7.2.12	Support for Stronger National Laws	314
7.2.13	Personal Experience with Data Privacy Issues	315
7.2.14	Action Taken After Data-Related Issues	316
7.2.15	Reasons for Inaction	317
7.2.16	Awareness of Privacy as a Fundamental Right	317
7.2.17	Awareness of Legal Remedies for Privacy Breach	318
7.2.18	Knowledge of Relevant Authorities	319
7.2.19	Understanding of Complaint Process	319
7.2.20	Disclosure by Organizations or Government	320
7.3.1	Understanding of Data Concepts (Legal Professionals)	326
7.3.2	Capability to Distinguish Between Personal and Non-Personal Data	327
7.3.3	Awareness of Indian Legal Framework on Data Protection	328
7.3.4	Necessity for Specific Legal Provisions on Non-Personal Data	328
7.3.5	Preference for Global Uniform Data Protection Laws	329
7.3.6	Adequacy of Indian Legal Framework for Personal Data	330
7.3.7	Sufficiency of Indian Legal Provisions for Non-Personal Data	330
7.3.8	Confidence in Applying Data Protection Laws	331
7.3.9	Need for Specialized Legal Training	332

7.3.10	Knowledge of International Data Protection Laws	332
7.3.11	Amendment Necessity in Existing Data Protection Laws	333
7.3.12	Clarity of Legal Distinction Between Personal and Non-Personal Data	334
7.3.13	Need for Comprehensive Non-Personal Data Regulations	334
7.3.14	Awareness of Non-Personal Data Regulations in Legal Community	335
7.3.15	Sufficiency of National Legal Frameworks	336
7.3.16	Need for Collaboration Between Law Enforcement and Cyber Experts	336
7.3.17	Relevance of International Frameworks	337
7.3.18	Exposure to Data Misuse or Breach Cases	338
7.3.19	Pursuit of Legal Action in Data-Related Issues	338
7.3.20	Reasons for Non-Pursuit of Legal Action	339
7.4.1	Understanding of Data Concepts (Law Students)	346
7.4.2	Distinguishing Between Personal and Non-Personal Data	347
7.4.3	Awareness of the Indian Legal Framework	347
7.4.4	Need for Legal Provisions on Non-Personal Data	348
7.4.5	Preference for Global Uniform Laws	349
7.4.6	Inclusion of Non-Personal Data in Legal Education	349
7.4.7	Confidence in Indian Legislation Regulating Non-Personal Data	350
7.4.8	Effectiveness of Global Regulations	351
7.4.9	Awareness of Data Protection Law Implications	351
7.4.10	Preparedness for Data Privacy Cases	352
7.4.11	Legal Regulation of Non-Personal Data	353
7.4.12	Inclusion of Specialized Courses on NPD Laws	353
7.4.13	Awareness Needs Among Legal Practitioners	354
7.4.14	Separate Legal Framework for Non-Personal Data	355
7.4.15	Awareness of Privacy as a Fundamental Right	355
7.4.16	Data Privacy as a Future Legal Concern	356
7.4.17	Exposure to Data Protection Laws in Curriculum	357
7.4.18	Familiarity with Legal Distinction Between Data Types	357
7.4.19	Awareness of Legal Remedies for Privacy Breaches	358
7.4.20	Confidence in Guiding Data Privacy Complaints	359
7.5.1	Understanding of the Concept of Data	366
7.5.2	Ability to Distinguish Between Personal and Non-Personal Data	367
7.5.3	Awareness of Indian Data Protection Framework	368
7.5.4	Necessity of Legal Provisions for Non-Personal Data	368

7.5.5	Preference for Global Uniform Data Protection Laws	369
7.5.6	Adequacy of Indian Regulations for the Technology Sector	370
7.5.7	Distinct Legal Protections for Non-Personal Data	370
7.5.8	Need for Comprehensive Non-Personal Data Regulation in India	371
7.5.9	Importance of Global Standards for Non-Personal Data Governance	372
7.5.10	Legal Consideration for Economic Value of Non-Personal Data	372
7.5.11	Impact of Indian Data Protection Laws on Professional Activities	373
7.5.12	Effectiveness of Anonymization in Safeguarding Privacy	374
7.5.13	Advocacy for Transparent Government Data Policies	375
7.5.14	Adherence to International Data Protection Standards	375
7.5.15	Influence of Fundamental Right to Privacy on Data Handling	376
7.5.16	Engagement with Non-Personal Data at Work	377
7.5.17	Familiarity with Indian Laws on Non-Personal Data	377
7.5.18	Challenges in Differentiating Data Types	378
7.5.19	Experience of Privacy Breaches Due to Unclear Legal Regulations	379
7.5.20	Support for Global Uniform Laws on Non-Personal Data	379
7.6.1	Comparative Findings	384
7.7.1	Key Findings of the Overall Analysis	391

Table of Abbreviations

Abbreviation	Full Form / Description
ACCC	Australian Competition and Consumer Commission
AI	Artificial Intelligence
AIIB	Asian Infrastructure Investment Bank
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
ASEAN	Association of Southeast Asian Nations
CCPA	California Consumer Privacy Act
CCPA (India)	Central Consumer Protection Authority
CCI	Competition Commission of India
CCIER	CUTS Centre for Competition, Investment and Economic Regulation
CCTNS	Crime and Criminal Tracking Network & Systems
CDR	Consumer Data Right (Australia)
CERT-In	Indian Computer Emergency Response Team
CIS	Centre for Internet and Society (India)
CNIL	Commission nationale de l'informatique et des libertés (France)
COPPA	Children's Online Privacy Protection Act (United States)
COVID-19	Coronavirus Disease 2019
CRM	Customer Relationship Management
CSIR	Council of Scientific and Industrial Research
CUTS	Consumer Unity & Trust Society

Abbreviation	Full Form / Description
DAU Policy	Data Accessibility and Use Policy, 2022 (India)
DATA Act	Data Availability and Transparency Act, 2022 (Australia)
DBMS	Database Management System
DFFT	Data Free Flow with Trust
DGA	Data Governance Act
DMA	Digital Markets Act
DPA	Data Protection Authority / Data Protection Act (as applicable by country)
DPDPA	Digital Personal Data Protection Act, 2023 (India)
DPDPA Rules	Digital Personal Data Protection Rules (India, Draft)
DPDP Bill	Draft Personal Data Protection Bill, 2019 (India)
DPI	Digital Public Infrastructure
DSL	Data Security Law (China)
DSA	Digital Services Act
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EDPB	European Data Protection Board
EU	European Union
FDI	Foreign Direct Investment
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
GoI	Government of India
HIPAA	Health Insurance Portability and Accountability Act (United States)

Abbreviation	Full Form / Description
IAPP	International Association of Privacy Professionals
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
IEC	Institutional Ethics Committee
IICA	Indian Institute of Corporate Affairs
IIT	Indian Institute of Technology
IMDA	Infocomm Media Development Authority (Singapore)
IMF	International Monetary Fund
IoT	Internet of Things
IP	Intellectual Property
IPAB	Intellectual Property Appellate Board
IPC	Indian Penal Code, 1860
IPR	Intellectual Property Rights
ISP	Internet Service Provider
ISO	International Organization for Standardization
IT	Information Technology
IT Act	Information Technology Act, 2000 (India)
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
ITES	Information Technology Enabled Services
K-DATA	Korea Data Agency
KISA	Korea Internet & Security Agency (South Korea)

Abbreviation	Full Form / Description
LGPD	Lei Geral de Proteção de Dados (General Data Protection Law, Brazil)
MCA	Ministry of Corporate Affairs (India)
MeitY	Ministry of Electronics and Information Technology (India)
METI	Ministry of Economy, Trade and Industry (Japan)
ML	Machine Learning
MNC	Multinational Corporation
MoSPI	Ministry of Statistics and Programme Implementation (India)
MPC	Model Penal Code
MSE	Micro and Small Enterprises
MSME	Micro, Small and Medium Enterprises
MSIT	Ministry of Science and ICT (South Korea)
NABH	National Accreditation Board for Hospitals and Healthcare Providers
NASSCOM	National Association of Software and Service Companies
NATGRID	National Intelligence Grid
NDC	National Data Commissioner (Australia)
NDGFP	National Data Governance Framework Policy (India)
NDHM	National Digital Health Mission (India)
NDSAP	National Data Sharing and Accessibility Policy, 2012 (India)
NEP	National Education Policy, 2020
NGO	Non-Governmental Organization
NLP	Natural Language Processing
NPCI	National Payments Corporation of India

Abbreviation	Full Form / Description
NPD	Non-Personal Data
NPDA	Non-Personal Data Authority (Proposed, India)
NPG	Non-Personal Governance Framework (India, MeitY 2020)
NPM	New Public Management
OAIC	Office of the Australian Information Commissioner
ODPC	Office of the Data Protection Commissioner (Kenya)
OECD	Organisation for Economic Co-operation and Development
OGD	Open Government Data Platform (India)
OGD Portal	Open Government Data Platform India (data.gov.in)
OSINT	Open-Source Intelligence
PBD	Privacy by Design
PBT	Privacy by Technology
PDPA	Personal Data Protection Act (Singapore)
PHI	Protected Health Information
PII	Personally Identifiable Information
PIPA	Personal Information Protection Act (South Korea)
PIPL	Personal Information Protection Law (China)
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PMLA	Prevention of Money Laundering Act, 2002 (India)
RBI	Reserve Bank of India
RTI	Right to Information
SA	Strongly Agree

Abbreviation	Full Form / Description
SDG	Sustainable Development Goals
SPDI	Sensitive Personal Data or Information
TRAI	Telecom Regulatory Authority of India
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
USA	United States of America
US	United States
VCDPA	Virginia Consumer Data Protection Act
VPN	Virtual Private Network
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

NON-PERSONAL DATA: CONCEPTUALIZATION OF THE TERM IN THE LEGAL FRAME AND A COMPARATIVE ANALYSIS AMONG DIFFERENT JURISDICTIONS

CHAPTER 1

INTRODUCTION

- 1.1 Introduction*
- 1.2 Conceptual Framework*
- 1.3 Literature Review*
- 1.4 Research Gap*
- 1.5 Statement of the Problem*
- 1.6 Rationale*
- 1.7 Objectives*
- 1.8 Hypothesis*
- 1.9 Scope and Limitations*
- 1.10 Research Methodology*
- 1.11 Plan of Study*

1.1 Introduction

“Data is the new oil, and like oil, it is valuable, but if unrefined, it cannot really be used.”¹ — Clive Humby (2006).

As the world commits to protecting personal data, embodied in India’s *Digital Personal Data Protection Act, 2023*², which safeguards individuals’ digital privacy, there persists a pressing yet underappreciated challenge: the legal stewardship of *Non-Personal Data (NPD)*. *NPD* encompasses datasets that do not identify individuals, such as weather patterns, supply chain analytics, and industrial telemetry. These

¹ *The World’s Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² Digital Personal Data Protection Act, 2023.

repositories hold vast promise for fueling artificial intelligence, intelligent governance, evidence-based policymaking, and broader societal advancement.

Despite this potential, India's regulatory narrative remains skewed. While the DPDP Act (enacted in August 2023)³ rigorously governs personal data, the conceptualization and codification of *NPD* continue to lag behind. An expert committee under the Ministry of Electronics and Information Technology (MeitY) has outlined a vision for a standalone *NPD* governance framework.⁴ It proposed classifying *NPD* into *public*, *community*, and *private* categories; creating roles such as *data custodians* and *data trustees* to safeguard community interests; and establishing a dedicated *Non-Personal Data Authority* to oversee rights, harms, and economic benefits grounded in the principles of sovereignty, simplicity, innovation, privacy, and public benefit.⁵

Complementing this, the draft *Data Accessibility and Use (DAU) Policy, 2022* sought to open anonymized, government-held *NPD* for research and governance purposes, envisioning the establishment of bodies such as an *Indian Data Office* and an *Indian Data Council* to harmonize standards, metadata, and sharing protocols across ministries.⁶ However, these initiatives remain largely aspirational; there is still no comprehensive or enforceable legal regime for *NPD* in force.

The responsible unlocking of innovation must be balanced against the risks of collective harms through re-identification or misuse⁷, as well as against the failure to ensure that the benefits of data accrue equitably to communities and the nation, rather than being concentrated within private entities.⁸ The distinction between personal and *Non-Personal Data* is increasingly becoming unclear, especially in mixed or de-identified datasets, pose genuine privacy threats that unregulated *NPD* frameworks must urgently address. While India has made commendable progress in establishing

³ *Id.*

⁴ Report of the Committee of Experts on Non-Personal Data Governance Framework, at 1–3 (Ministry of Elecs. & Info. Tech., rev. Dec. 16, 2020), <https://openfuture.eu/wp-content/uploads/2022/05/Indian-2020-report-by-the-committee-of-Experts-on-Non-Personal-Data-Governance-Framework.pdf>.

⁵ *Id.* at 13–14, 25–27, 28–30, 20–24.

⁶ Draft India Data Accessibility & Use Policy, 2022, at 5–10, 12–15 (Ministry of Elecs. & Info. Tech. Feb. 21, 2022), <https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022>.

⁷ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra* note 4, at 10–12.

⁸ *Id.* at 15–18, 23–25.

mechanisms for personal data protection, the legal architecture for *NPD*, a resource of immense strategic and civic value, remains embryonic.⁹

For India to fully harness its digital potential in artificial intelligence, governance, and inclusive development, the creation of a coherent, principled, and enforceable *NPD* regulatory ecosystem is no longer optional, it is indispensable.¹⁰

1.2 Conceptual Framework

The conceptual framework of the present study delineates the foundational constructs, institutional relationships, and normative principles guiding the governance of *Non-Personal Data (NPD)* in India. It provides the theoretical grounding for subsequent analysis and methodological inquiry.

A theoretical model for the regulation and management of *Non-Personal Data (NPD)* in India must begin with clear foundational elements: definitions, principles, classification, institutional architecture, and guiding goals, all arranged within a coherent and interlocking structure.¹¹

NPD should be conceptually defined as any data that does not pertain to the identity of a natural person, for instance, de-identified, aggregated, or machine-generated information. Recognizing, however, the boundary between personal and *Non-Personal Data* is frequently indistinct, especially when mixed or potentially re-identifiable datasets are involved, this framework must embrace a degree of flexibility in categorization, acknowledging the possibility of re-identification and the presence of unclear boundaries.¹²

NPD may be further classified into three types: public, community, and private. Public *NPD* includes datasets such as anonymized land records or public health data; community *NPD* covers data such as utility usage patterns or mobility information collected by public or private actors; and private *NPD* comprises proprietary analytics,

⁹ *Id.* at 8–9, 1–3.

¹⁰ *Id.* at 45–50.

¹¹ *Id.* at 5–7.

¹² *Id.* at 6, 8–9, 10–12.

industrial insights, or commercial datasets generated by enterprises.¹³ These categories coexist with the functional forms of *Non-Personal Data*, such as anonymized, aggregated, machine-generated, and industrial data, reflecting both its governance dimension and technological character.

Anchored to this taxonomy are the guiding principles of sovereignty (the state's custodial role over data resources), simplicity (minimizing compliance burdens and fostering usability), innovation (unlocking economic and social value), fairness (ensuring equitable benefit-sharing among stakeholders), and privacy protection (preventing misuse or re-identification).¹⁴

The framework envisions distinct institutional roles. Data trustees should represent community interests; data custodians should manage datasets responsibly, transparently, and in compliance with ethical standards; and a central *Non-Personal Data* Authority should be established to oversee classification, access rights, compliance, dispute resolution, and enforcement. This Authority should coordinate with Data Management Units across ministries and be mandated to enforce standards, promulgate metadata norms, and issue sharing protocols through an Indian Data Office or similar nodal body.¹⁵

An overarching National Data Governance Framework Policy (NDGFP) should provide the structural legitimacy for these institutions and their interrelations. Existing measures, such as India's *National Data Sharing and Accessibility Policy (NDSAP)*, which promotes open access to government-generated, non-sensitive datasets, should be harmonized within this new *NPD* framework to enable accessibility and reuse while respecting the spectrum of sensitivity and ownership.¹⁶

This conceptual architecture must be outcome-oriented, designed to facilitate artificial intelligence research, evidence-informed policymaking, public-interest innovations,

¹³*Id.* at 13–14.

¹⁴*Id.* at 20–24.

¹⁵*Id.* at 25–27, 28–30; Draft India Data Accessibility & Use Policy, 2022, *Supra* note 6, at 12–15.

¹⁶ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra* note 4, at 35–38; National Data Sharing and Accessibility Policy, at 4–6 (Dep't of Sci. & Tech. Feb. 9, 2012), https://dst.gov.in/sites/default/files/NDSAP_2012.pdf.

and equitable economic opportunity, while carefully balancing those objectives against the potential risks of misuse, harm, or erosion of privacy.¹⁷

In essence, the proposed conceptual framework weaves together definition, categorization, principles, governing institutions, and policy instruments into a unified and structured tapestry, establishing a principled, scalable, and inclusive foundation for India's *Non-Personal Data* governance.¹⁸

1.3 Literature Review

The study of *Non-Personal Data* (NPD) has emerged as an important discipline positioned at the crossroads of information law, technology regulation, and public policy. The existing literature indicates that although global discussions have traditionally focused on personal data protection and privacy, the understanding and conceptualization of *Non-Personal Data* remain relatively underexplored¹⁹, data that has been anonymized, aggregated, or generated by machines, has gradually emerged as an independent subject of legal inquiry.²⁰ This review organizes the existing scholarship, statutes, policy papers, online commentaries, and jurisprudence around five broad themes: (i) legal statutes and legislative frameworks, (ii) government policies and institutional blueprints, (iii) expert and online commentaries, (iv) academic and journal literature, and (v) judicial precedents and constitutional foundations.

The objective of this literature review is to examine the intellectual and legal development of *Non-Personal Data* (NPD) governance both in India and globally, to identify conceptual gaps, and to situate the present research within an ongoing body of theoretical and practical debates.²¹

¹⁷ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra* note 4, at 40–42.

¹⁸ *Id.* at 45–50.

¹⁹ Vidushi Marda, *Non-Personal Data: The Case of the Indian Data Protection Bill, Definitions and Assumptions*, Ada Lovelace Inst. (Oct. 15, 2020), <https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/>.

²⁰ *Id.* at 2–3.

²¹ *Id.* at 1.

1.3.1 Legal Statutes and Frameworks

The Indian legal landscape concerning *Non-Personal Data* remains underdeveloped and fragmented. The Information Technology Act, 2000 (IT Act) remains the foundational statute governing electronic transactions, cybersecurity, and certain aspects of data protection.²² However, it is fundamentally oriented toward *personal data* and *information security*, rather than anonymized or aggregated datasets.

Section 43A of the Information Technology Act provides for compensation in cases of negligence in safeguarding personal data²³, whereas Section 72A penalizes the disclosure of personal information without consent or in breach of a lawful contract.²⁴ These provisions, though significant, do not extend to datasets that are anonymized or aggregated.²⁵ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 similarly focus on user-generated content, intermediary obligations, and traceability of “first originators.”²⁶ While these are essential for addressing privacy and misinformation, they do not engage with *NPD*’s value for research, innovation, and policy modelling.²⁷

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a major milestone in India’s privacy law framework.²⁸ It confers data rights upon individuals, creates obligations for data fiduciaries and processors, and establishes the Data Protection Board of India as the primary regulatory body responsible for enforcing compliance, adjudicating breaches, and ensuring accountability under the data protection framework.²⁹ Yet, its very name and scope reveal its limits: the Act explicitly confines itself to *personal data*.³⁰ There is no reference to anonymized, aggregated, or machine-generated information, data forms that underpin modern

²² Information Technology Act, 2000, § 1.

²³ *Id.* §§ 2(w), 43A.

²⁴ *Id.* § 43A.

²⁵ *Id.* § 72A.

²⁶ *Id.*; see also Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).

²⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India), <https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf>.

²⁸ *Id.* Rules 3–4.

²⁹ Digital Personal Data Protection Act, 2023.

³⁰ *Id.*

artificial intelligence, urban planning, industrial automation, and environmental monitoring.³¹

In contrast, other jurisdictions have moved toward specialized treatment of *NPD*. The European Union, under *Regulation (EU) 2018/1807 on the Free Flow of Non-Personal Data*, encourages the unrestricted movement of anonymized data within the Union, recognizing it as an economic and research resource.³² The EU *Data Governance Act (2022)* and *Data Act (2023)* further codify principles for data sharing, data altruism, and industrial access, addressing the competitive and ethical dimensions of non-personal datasets.³³

In the United States, sectoral statutes such as the *Health Insurance Portability and Accountability Act (HIPAA)* and the *California Consumer Privacy Act (CCPA)* include de-identification standards but treat *NPD* as a by-product of privacy regulation rather than as a resource requiring governance.³⁴ The absence of an overarching law allows contractual mechanisms and industry norms to dominate, but it also creates fragmentation and uncertainty.³⁵

India's current statutory framework therefore remains asymmetrical: robust in personal data protection, silent on *Non-Personal Data* stewardship. This silence creates ambiguity around issues of ownership, equitable access, re-identification risks, and benefit-sharing.³⁶ For example, anonymized datasets generated by private entities often contain commercially valuable insights. However, in the absence of adequate regulatory safeguards, such data may fall within a grey area that neither qualifies as

³¹ *Id.*

³² *Id.*

³³ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, 2018 O.J. (L 303) 67, <https://eur-lex.europa.eu/eli/reg/2018/1807/oj/eng>.

³⁴ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act), 2022 O.J. (L 152) 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868>; Regulation (EU) 2023/2854 of the European Parliament and of the Council of 22 December 2023 on Harmonised Rules on Fair Access to and Use of Data (Data Act), 2023 O.J. (L 327) 1, <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>.

³⁵ Health Insurance Portability and Accountability Act, 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.); California Consumer Privacy Act, 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2023).

³⁶ *Id.*

undisclosed information (trade secret protection) under Article 39 of the TRIPS Agreement nor enjoys protection against unfair or unauthorized use.³⁷

The literature highlights that the lack of a comprehensive legal definition and regulatory framework for *Non-Personal Data (NPD)* limits India's capacity to ensure ethical use, innovation, and sovereignty in its digital economy.³⁸ The existing legal instruments collectively underscore the necessity of a dedicated statutory regime for Non-Personal Data.³⁹

1.3.2 Government Policies and Institutional Frameworks

India has made tentative but vital forays into conceptualizing the governance of *NPD*. Among the most influential is the “*Report of the Expert Committee on Non-Personal Data Governance Framework (2020)*” chaired by Kris Gopalakrishnan.⁴⁰ This committee proposed a policy architecture for treating *NPD* as a national resource with social and economic value.⁴¹

The Committee's report classified *NPD* into three categories:

- Public *NPD*, such as anonymized land or health records generated by public authorities;
- Community *NPD*, such as utility usage or mobility data collected by public or private actors; and
- Private *NPD*, such as proprietary analytics or algorithmically derived insights.⁴²

³⁷ Report of the Committee of Experts on Non-Personal Data Governance Framework, at 1–3 (Ministry of Elecs. & Info. Tech., rev. Dec. 16, 2020), <https://openfuture.eu/wp-content/uploads/2022/05/Indian-2020-report-by-the-committee-of-Experts-on-Non-Personal-Data-Governance-Framework.pdf>.

³⁸ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994).

³⁹ Marda, *Supra note* 19, at 4–5.

⁴⁰ *Id.* at 5.

⁴¹ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra note* 37.

⁴² *Id.* at 1–2.

The Committee recommended institutional roles such as data custodians, data trustees, and a central *Non-Personal Data Authority (NPDA)* to oversee data classification, access rights, and compliance.⁴³ The guiding principles, sovereignty, public benefit, privacy, simplicity, and innovation, provided a normative foundation for policy formulation.⁴⁴ The framework also introduced the concept of *data sharing for public value* to democratize access while preserving legitimate interests of private holders.⁴⁵

In parallel, the Data Accessibility and Use (DAU) Policy, 2022 sought to open up anonymized government-held data for research, governance, and commercial reuse.⁴⁶ Drafted under the National Data Governance Framework Policy (NDGFP), it envisioned an *India Datasets Programme* to standardize metadata and monetize value-added datasets at equitable price points.⁴⁷ However, public consultations revealed concerns about potential monetization of public data, leading to revisions and delays in adoption.⁴⁸ The ongoing debate between open access and commercialization highlights the tension between public good and private incentive in data governance.⁴⁹

The National Data Sharing and Accessibility Policy (NDSAP), introduced in 2012, mandates that non-sensitive government datasets generated with public funds be made available in both human- and machine-readable formats.⁵⁰ This policy laid the foundation for open data initiatives such as the *Open Government Data (OGD) Platform India*, enabling transparency and citizen participation.⁵¹ However, the NDSAP does not address private or community-held *NPD*, nor does it institutionalize metadata standards or anonymization protocols.⁵²

⁴³ *Id.* at 13–14.

⁴⁴ *Id.* at 25–30.

⁴⁵ *Id.* at 20–24.

⁴⁶ *Id.* at 35–38.

⁴⁷ Draft India Data Accessibility & Use Policy, 2022, at 5–10 (Ministry of Elecs. & Info. Tech. Feb. 21, 2022), <https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022>.

⁴⁸ *Id.* at 12–15; Draft National Data Governance Framework Policy, at 4–6 (Ministry of Elecs. & Info. Tech. May 2022), <https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf>.

⁴⁹ Draft India Data Accessibility & Use Policy, 2022, *Supra note 29*, at 16–18.

⁵⁰ *Id.*

⁵¹ National Data Sharing and Accessibility Policy, at 4–6 (Dep’t of Sci. & Tech. Feb. 9, 2012), https://dst.gov.in/sites/default/files/NDSAP_2012.pdf.

³⁴ *Id.* at 7–8.

⁵² *Id.* at 9–10.

Collectively, these policies outline a nascent but fragmented governance trajectory. The Expert Committee and NDGFP articulate strong normative visions, but their absence of statutory backing and operational infrastructure undermines implementation.⁵³ The DAU Policy and NDSAP provide functional pathways for public-sector data but fail to extend their reach to private or community data.⁵⁴ In a rapidly digitizing economy such as India's, where data generation outpaces regulation, the challenge lies in transforming these policy fragments into a cohesive, enforceable, and inclusive governance ecosystem that spans all categories of *NPD*.⁵⁵

1.3.3 Online Commentaries and Emerging Discourse

The policy and scholarly conversation around *NPD* have been enriched by digital platforms, expert analyses, and thought leadership pieces that provide both critique and insight. Commentaries from think tanks, independent researchers, and specialized law blogs serve as crucial supplements to formal academic literature, given the novelty of the field.⁵⁶

The Ada Lovelace Institute and legal researcher Vidushi Marda have critically assessed India's *NPD* framework, arguing that reliance on exclusion-based definitions, where *Non-Personal Data* is merely defined by what it is not, creates ambiguity and potential overreach.⁵⁷ The concern centres on *mixed datasets*, where de-identified or aggregated data may still contain residual identifiers, leading to privacy risks under personal data laws.⁵⁸

Legal blogs such as SpicyIP have examined possible conflicts between a future *NPD* regime and India's international trade obligations, particularly under the TRIPS Agreement, where certain forms of anonymized commercial data may qualify as trade

⁵³ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra note 37*, at 45–50.

⁵⁴ Draft India Data Accessibility & Use Policy, 2022, *Supra note 6*, at 12–15.

⁵⁵ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra note 37*, at 45–47.

⁵⁶ Marda, *Supra note 19*, at 1.

⁵⁷ *Id.* at 2–3.

⁵⁸ *Id.* at 8–9.

secrets.⁵⁹ The risk of over-regulation, they argue, could undermine proprietary innovation if all forms of anonymized data are treated as quasi-public resources.⁶⁰

Platforms like InternetGovernance.org and CIS-India (Centre for Internet and Society) provide ongoing policy commentary.⁶¹ They highlight the need for an empowered *Non-Personal Data* Authority to safeguard national interests, ensure ethical data sharing, and maintain sovereignty.⁶² CIS-India has raised concerns over the NDGFP's proposed monetization model, arguing that without procedural safeguards, public datasets could become sources of inequitable profit rather than collective benefit.⁶³

Other specialized inputs, such as those from Yale-Wikimedia Law School collaborations, illuminate the rationale behind the Expert Committee's proposals, emphasizing community benefit, accountability, and equitable economic redistribution through a dedicated *NPD* authority.⁶⁴ Law firms such as LexOrbis and AGAMA Law analyze the patchwork nature of current laws, emphasizing that the IT Act was designed for an earlier internet era and cannot accommodate the complex challenges of *NPD* governance.⁶⁵

Collectively, these commentaries serve dual purposes: they sustain an informed policy dialogue and expose critical lacunae in existing regulatory mechanisms. Their observations about definitional clarity, conflicts with trade law, institutional design, and enforcement feasibility underscore the urgency of translating policy concepts into actionable law.⁶⁶

⁵⁹ Revised Non-Personal Data Governance Framework and Intellectual Property Implications – Part I, SpicyIP (Feb. 9, 2021), <https://spicyip.com/2021/02/revised-non-personal-data-governance-framework-and-intellectual-property-implications-part-i.html>.

⁶⁰ *Id.*

⁶¹ *Id.* (commentary on NDGFP).

⁶² Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra* note 37, at 15–18.

⁶³ Brief Analysis of Non-Personal Data Governance Framework in India, Lexology (Oct. 29, 2020), <https://www.lexology.com/library/detail.aspx?g=259584ff-fb42-4d02-8ddf-9cf8c0925d34>.

⁶⁴ Marda, *Supra* note 19, at 5.

⁶⁵ *Id.* at 1.

⁶⁶ Rahul Matthan, Non-Personal Data and the Public Interest, 16 INDIAN J.L. & TECH. 1 (2020).

1.3.4 Scholarly and Journal Literature

Academic scholarship provides the theoretical foundation for *NPD* governance by probing questions of ownership, stewardship, institutional design, and fundamental rights.⁶⁷

Articles in the Indian Journal of Intellectual Property Law & Technology (IJILT) have examined whether anonymized, aggregated, or derived datasets can be accommodated within existing intellectual property regimes.⁶⁸ These analyses note that traditional IP frameworks, designed for creative works and inventions, do not easily apply to algorithmically generated or machine-derived data.⁶⁹ The literature therefore advocates for a *sui generis* legal approach that recognizes data as a shared yet regulated resource.⁷⁰

Policy papers published by organizations such as CUTS International (CCIER), NIPFP, and IDFC Institute have emphasized that the concept of “public interest” in *NPD* frameworks remains under-defined.⁷¹ They caution that without clear criteria, the rhetoric of community benefit could be co-opted by large corporations.⁷²

Scholarly commentary in technology law journals further discusses *NPD* within constitutional jurisprudence. Some authors argue that *NPD* governance could analogically draw upon the principles established in India’s natural resource jurisprudence, particularly in cases such as the *2G Spectrum* litigation and *Centre for Public Interest Litigation v. Union of India*⁷³. These judgments recognized that certain resources, like airwaves and minerals, constitute national assets requiring stewardship

⁶⁷ *Id.* at 10–12.

⁶⁸ *Id.* at 13–14.

⁶⁹ Future of Non-Personal Data Governance in India: A Consumer Perspective, CUTS Int’l (2021), <https://cuts-ccier.org/pdf/policy-brief-future-of-NPD-governance-in-india.pdf>; NIPFP Working Paper No. 246, Disclosures in Privacy Policies (2018), https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf; Data Governance Network, IDFC Inst. (2019), <https://www.idfcinstitute.org/projects/state-capacity/data-governance-network/>.

⁷⁰ Future of Non-Personal Data Governance in India, *Supra note* 69, at 5–7.

⁷¹ *Ctr. for Pub. Interest Litig. v. Union of India*, (2012) 3 S.C.C. 1 (India).

⁷² *Id.* ¶¶ 7–10.

⁷³ NIPFP Working Paper No. 246, *Supra note* 69, at 15–18.

and equitable allocation.⁷⁴ A parallel can be drawn for *NPD* as a *digital commons* that demands custodial governance rather than unrestricted commodification.⁷⁵

Internationally, journals like the *Computer Law and Security Review*, *Yale Journal on Regulation*, and *Harvard Journal of Law & Technology* have begun addressing the intersection of data governance and competition policy.⁷⁶ They examine how anonymized datasets influence artificial intelligence ecosystems, create informational asymmetries, and reshape market dynamics.⁷⁷ Comparative research highlights models from the EU's *Data Act*, Japan's *Data Free Flow with Trust* framework, Singapore's *Trusted Data Sharing Framework*, South Korea's *Digital Framework Act (2021)*, and Kenya's *Open Data Policy (2020)*, all of which provide insights for India's evolving ecosystem.⁷⁸

This academic discourse underscores that *NPD* governance is inherently multi-disciplinary, bridging information law, intellectual property, economics, and ethics.⁷⁹ It also stresses the gap between conceptual frameworks and practical implementation, calling for empirical studies that test anonymization standards, examine sectoral case studies, and assess institutional capacity.⁸⁰

1.3.5 Judicial Precedents and Comparative Jurisprudence

Although Indian courts have not yet adjudicated directly upon *NPD*-specific disputes, several judgments provide constitutional and jurisprudential foundations relevant to its governance.⁸¹

The landmark judgment in “*Justice K. S. Puttaswamy v. Union of India (2017)*” recognized the right to privacy as a fundamental right guaranteed under Articles 14, 19, and 21 of the Indian Constitution.⁸² The Court's test of *legality, necessity, and*

⁷⁴ Paul De Hert & Vagelis Papakonstantinou, *The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?*, 34 *COMPUT. L. & SEC. REV.* 179 (2018).

⁷⁵ *Id.* at 20–22.

⁷⁶ Regulation (EU) 2023/2854, *Supra* note 16; Japan's Data Free Flow with Trust (DFFT) Framework (2019), https://www.meti.go.jp/policy/it_policy/intl/dfft/index.html.

⁷⁷ Marda, *Supra* note 19, at 4.

⁷⁸ *Id.* at 5.

⁷⁹ *Id.* at 1.

⁸⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁸¹ *Id.* ¶¶ 119–120.

⁸² *Id.* ¶ 65.

proportionality for intrusions into informational privacy offers guiding principles for *NPD* regulation.⁸³ Even though anonymized data lies outside the immediate domain of personal data, Puttaswamy’s recognition of informational self-determination implies that the governance of re-identifiable datasets must adhere to constitutional safeguards.⁸⁴

Comparatively, European jurisprudence clarifies that fully anonymized data falls outside the GDPR’s scope, but pseudonymized data, where re-identification remains possible, continues to attract data protection obligations.⁸⁵ The *Court of Justice of the European Union (CJEU)*, in the “*Breyer v. Germany*” emphasized that identifiability is a contextual and dynamic test.⁸⁶ This precedent suggests that Indian law should adopt a risk-based approach to anonymization rather than assuming a binary distinction.⁸⁷

Indian resource jurisprudence, particularly the *2G Spectrum Case (Centre for Public Interest Litigation v. Union of India)*, articulates the public trust doctrine, holding that certain resources belong collectively to the people and must be managed in the public interest.⁸⁸ Extending this reasoning, scholars argue that *NPD*, especially community-generated datasets, could be treated as a digital public resource requiring custodial regulation.⁸⁹

Internationally, courts in Australia, Canada, and the European Union have considered issues of data access and sovereignty in cases involving government-held anonymized data.⁹⁰ Judicial reviews in these jurisdictions balance innovation incentives with public interest and data protection.⁹¹ Such comparative jurisprudence demonstrates how

⁸³ General Data Protection Regulation, Regulation (EU) 2016/679, art. 4(5), 2016 O.J. (L 119) 1.

⁸⁴ *Patrick Breyer v. Bundesrepublik Deutschland*, Case C-582/14, ECLI:EU:C:2016:779 (CJEU Oct. 19, 2016).

⁸⁵ *Id.* ¶ 45.

⁸⁶ *Ctr. for Pub. Interest Litig. v. Union of India*, *Supra* note 71.

⁸⁷ *Id.* ¶ 7.

⁸⁸ *See, e.g.*, Privacy Act, R.S.C. 1985, c. P-21 (Can.).

⁸⁹ *Id.*

⁹⁰ Marda, *Supra* note 19, at 5.

⁹¹ *Id.* at 4–5.

courts can mediate the intersection between open data and privacy, offering instructive models for India as it develops its own *NPD* legal infrastructure.

Overall, case law both Indian and international underscores that future *NPD* regulation must integrate privacy safeguards, state stewardship, and recognition of anonymization limits within a constitutionally sound framework.

1.4 Research Gap

Despite the growing recognition of *Non-Personal Data (NPD)*, encompassing anonymized, aggregated, or machine-generated datasets, as a vital resource for innovation, artificial intelligence, public policy, and research, the academic and policy discourse in India continues to reflect notable conceptual and empirical voids.⁹² While the subject has been acknowledged as central to the emerging data-driven economy, systematic inquiry into its legal, institutional, and socio-economic dimensions remains limited.

The Expert Committee on *Non-Personal Data Governance Framework* (2020), constituted under India's Ministry of Electronics and Information Technology (MeitY), provided an initial blueprint by recommending an independent *Non-Personal Data Authority* and classifying *NPD* into *public*, *community*, and *private* forms.⁹³ Although this framework represented an important conceptual advance, it remains largely theoretical and has not been operationalized through legislative or institutional means. Parliamentary debates, inter-ministerial consultations, or subsequent policy drafts have yet to convert these recommendations into enforceable regulatory architecture. As a result, India's *NPD* governance landscape is presently characterized more by aspiration and speculation than by normative clarity or practical implementation.

⁹² Vidushi Marda, *Non-Personal Data: The Case of the Indian Data Protection Bill, Definitions and Assumptions*, Ada Lovelace Inst. (Oct. 15, 2020), <https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/>.

⁹³ Report of the Committee of Experts on Non-Personal Data Governance Framework, at 1–3, 13–14, 28–30 (Ministry of Elecs. & Info. Tech., rev. Dec. 16, 2020), <https://openfuture.eu/wp-content/uploads/2022/05/Indian-2020-report-by-the-committee-of-Experts-on-Non-Personal-Data-Governance-Framework.pdf>.

Scholarly critiques have identified several critical oversights in this regard. Legal and policy scholars have questioned whether the proposed governance framework adequately reflects India's economic realities, technological diversity, and social asymmetries. Key academic publications and policy briefs underline that concepts such as *public interest*, *community ownership*, and *data sovereignty* remain vaguely defined, often serving as rhetorical placeholders rather than legally enforceable principles. Without operational clarity, these terms risk privileging state or corporate actors while excluding marginalized communities whose data often underpins digital ecosystems.

Further, the literature highlights that mechanisms for data sharing, access, and reuse, central to the proposed *NPD* architecture, lack corresponding *capacity-building provisions* for researchers, start-ups, or civic innovators. Consequently, even when non-personal datasets are made available, a large segment of potential beneficiaries remains unable to utilize them effectively due to technical, financial, or institutional constraints. This disconnect undermines the policy goal of democratizing data access and reinforces existing hierarchies of knowledge and innovation.

Empirical research, which is critical for understanding how data actually flows, is used, or misused within real Indian contexts, remains sparse. Very few studies have systematically explored how non-personal datasets are collected, processed, or shared across public and private institutions. Case-specific analyses, such as those concerning *AgriStack* and agricultural data governance, provide important insights but also reveal tensions between potential community upliftment and inadvertent data appropriation.⁹⁴ The lack of regional, sectoral, and socio-economic granularity in existing research prevents a clear understanding of who benefits from *NPD*-based innovation and who bears the associated risks.

A broader body of comparative and critical literature situates India's efforts within the *global data governance debate*. Analysts note that, in the absence of a concrete *NPD* regime, India has largely remained a passive observer, studying how jurisdictions like

⁹⁴ Shreehari Paliath, *What Is a Digital AgriStack and Why Indian Farmers Are Opposed to It*, Bus. Standard (Jan. 13, 2022), https://www.business-standard.com/article/economy-policy/what-is-a-digital-agristack-and-why-indian-farmers-are-opposed-to-it-122011300175_1.html.

the European Union, Japan, Singapore, South Korea, and Kenya operationalize *Non-Personal Data* frameworks rather than developing a context-specific path of its own. The European Union's *Data Governance Act* and *Data Act*, for example, emphasize structured sharing, interoperability, and community participation, while Japan's principle of *Data Free Flow with Trust* and South Korea's *Digital Framework Act* balance openness with technological accountability.⁹⁵ India, despite its scale and digital capacity, has yet to evolve an equivalent enforceable system that embeds these principles in law and practice.

The legal and infrastructural dimensions of *NPD* implementation, such as metadata standards, equitable pricing of public datasets, anonymization protocols, and transparent access mechanisms, also remain under-researched. These are essential operational preconditions for any data-sharing regime, yet few studies provide empirical benchmarks or comparative analysis to guide policy design. The socio-legal implications arising from the blurring of boundaries separating personal and *Non-Personal Data* have often been acknowledged but rarely examined in a systematic way. With advanced analytics and artificial intelligence capable of re-identifying anonymized data, policymakers lack a clear evidence base to balance innovation with privacy safeguards.⁹⁶

These conceptual, empirical, technical, and normative deficiencies collectively point to the urgent need for a multidimensional research agenda. Such an agenda must integrate doctrinal inquiry, comparative analysis, and empirical investigation to generate a nuanced, evidence-informed foundation for future regulation. Studies must unpack ground realities, evaluate socio-economic implications, test the robustness of anonymization techniques, assess community participation, and analyze governance proposals in practice. Only through such comprehensive and interdisciplinary research

⁹⁵ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act), 2022 O.J. (L 152) 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868>; Regulation (EU) 2023/2854 of the European Parliament and of the Council of 22 December 2023 on Harmonised Rules on Fair Access to and Use of Data (Data Act), 2023 O.J. (L 327) 1, <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>; Japan's Data Free Flow with Trust (DFFT) Framework (2019), https://www.meti.go.jp/policy/it_policy/intl/dfft/index.html.

⁹⁶ Michèle Finck & Frank Pallas, They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR, 10 INT'L DATA PRIVACY L. 11 (2020).

can India move from aspirational policy blueprints to a cohesive and operational *Non-Personal Data governance regime*.

Key Identified Gaps

i. Superficiality of the Conceptual Discourse

The ongoing conversation around *NPD* in India remains largely superficial. It often reduces the concept to the simple anonymization of existing datasets, overlooking more complex and dynamic categories such as *machine-generated data*, *sensor data*, *industrial telemetry*, and *algorithmic outputs*. These forms of data are increasingly central to artificial intelligence, smart manufacturing, and predictive governance, yet they receive minimal attention in Indian policy or academic circles. The Expert Committee's attempt at classifying *NPD* into *public*, *community*, and *private* categories was a useful starting point, but the economic valuation of such data, its potential for competitive advantage, and the risks of monopolization remain underexplored.⁹⁷

ii. Absence of Nuanced Economic and Legal Analyses

There is a lack of in-depth research on the intersection of *NPD* with competition law, trade regulation, and intellectual property. Questions regarding *ownership* and *benefit-sharing*, particularly in multi-stakeholder contexts where both public and private entities contribute to data generation, have not been adequately addressed. Legal ambiguities persist over whether non-personal datasets constitute *intangible assets*, *commons*, or *public goods*, and what remedies may exist in case of misuse or exclusionary control.

iii. Inadequate Empirical Investigations

Empirical research remains both thin and one-dimensional. Most analyses rely on descriptive policy evaluation rather than quantitative or qualitative evidence. There is an acute shortage of large-scale surveys, interviews, or field-based studies that capture multi-stakeholder perspectives. The voices of *legal professionals*, *technology experts*,

⁹⁷ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra* note 37, at 13–14.

data practitioners, law and policy students, and the general public, each of whom interacts with data differently, are notably absent. Without such triangulated data, policy design remains speculative and disconnected from ground realities.

iv. Limited Sectoral and Regional Analysis

Sector-specific studies on *NPD*, such as those concerning agriculture, health, education, and urban governance, remain sporadic. For instance, discussions around *AgriStack* and agricultural data governance reveal insufficient consultation with farmer communities and limited accessibility, particularly due to the absence of documentation in regional languages. Similarly, studies on urban mobility or environmental data have not adequately examined data quality, consent practices, or public benefit outcomes.

v. Power Asymmetries and Community Ownership

The literature has not systematically explored how *community rights over NPD* are structured or how value from collective data is distributed. The question of data ownership in cases where multiple entities are involved, for example, operational data from aircraft engines shared among manufacturers, airlines, and maintenance providers, remains unresolved. This lack of clarity exacerbates power imbalances between global corporations, data intermediaries, and local communities.

vi. Implementation Gaps in Institutional Design

Despite the ambitious theoretical frameworks proposed by the Expert Committee, including the *Non-Personal Data Authority*, *Data Trustees*, and *Indian Data Office*, India lacks tangible and actionable policy guidance suited to the realities of emerging economies. Proposed institutions exist largely on paper, without clear mandates, enforcement mechanisms, or budgetary support. This renders them ineffective as tools for regulation or accountability.

vii. Weak Linkages Between Policy Vision and Legal Enforceability

Many of India's *NPD* policy documents rely on aspirational language, emphasizing openness, innovation, and community benefit without specifying enforceable legal duties or sanctions. The absence of justiciable obligations weakens institutional

legitimacy and limits the ability of affected parties to seek redress in cases of misuse or exclusion.

viii. Insufficient Comparative and Cross-Jurisdictional Analysis

Few Indian studies provide comparative evaluations of global frameworks. Jurisdictions such as the European Union, Japan, Singapore, South Korea, and Kenya have implemented distinct yet instructive models for *NPD* governance. Their experiences with data intermediaries, trust-based sharing mechanisms, and value redistribution offer critical lessons for India, but these have not been systematically synthesized or adapted to the domestic context.⁹⁸

ix. Neglect of Ethical, Cultural, and Rights-Based Perspectives

The discourse around *NPD* governance often overlooks ethical questions regarding autonomy, consent, and distributive justice. As data becomes a collective resource, issues of *representation* and *accountability* acquire greater importance. The rights of communities to influence how their anonymized or aggregated data is used, particularly in public policy and artificial intelligence systems, have not been sufficiently examined.

1.5 Statement of the Problem

India stands at a juncture where the promise of harnessing *Non-Personal Data (NPD)* comprising anonymized, aggregated, or machine-generated datasets such as environmental metrics, infrastructure logs, and industrial telemetry for innovation, governance, and societal progress is substantial undercut by a profound regulatory vacuum. While existing efforts including the Expert Committee's 2020 framework and the proposed National Data Governance Framework Policy (NDGFP) bear valuable conceptual offerings such as categorizing *NPD* into public, community, and private classes, defining roles like data custodians and trustees, and advocating for a *Non-Personal Data Authority* these proposals remain largely symbolic and aspirational,

⁹⁸ Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR INT. 989 (2016).

without translating into enforceable law or clear actionable implementation structures.⁹⁹

Definitional ambiguity reigns (*NPD*) remain tethered to simplistic notions of anonymization ignoring nuanced forms such as sensor outputs, IoT data, or de identified but re-identifiable mixed datasets raising serious questions of privacy erosion through de-anonymization. The absence of empirical clarity around stakeholder needs, concerns, and capacities ranging from communities whose livelihoods depend on data-driven interventions, to policymakers grappling with practical regulatory design has left policymakers guided by theory rather than lived realities. Equity and ownership concerns remain largely overlooked: without stratified analysis as data governance risks concentrating control in the hands of a few private or state actors, undermining communal rights and public access to high-value datasets. NDGFP articulates visionary principles such as enabling innovation, safeguarding sovereignty, and promoting public interest there remains a palpable gap in translating these principles into concrete, context-sensitive policies tailored to an emerging economy like India where data generation far outpaces the machinery of regulation.

This regulatory inaction and conceptual fuzziness hamper India's ability to unlock *NPD*'s economic and social value, while exposing society to unintended repercussions such as privacy violations, policy capture, and infrastructural inequities. India lacks a clear, and actionable legal and institutional framework for *Non-Personal Data* one that delineates *NPD*'s definition with precision, grounds regulation in stakeholder realities, balances innovation with rights and equity, and transitions from conceptual blueprints to enforceable safeguards so that the vast promise of *NPD* can be realized responsibly and inclusively.

⁹⁹ Report of the Committee of Experts on Non-Personal Data Governance Framework, *Supra note 37*, at 45–50; Draft Nat'l Data Governance Framework Pol'y, at 4–6 (Ministry of Elecs. & Info. Tech. May 2022), <https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf>.

1.6 Rationale

The necessity to establish a governance framework for *Non-Personal Data (NPD)* in India stems from its vast untapped potential as a driver of innovation, AI advancement, evidence-based policymaking, and economic growth, which remains limited due to the absence of coherent regulation. India's policymaking landscape has begun to acknowledge *NPD*'s importance through references in the National Strategy for Artificial Intelligence, which emphasizes the utilization of government data for “*public good*”¹⁰⁰, and the Economic Survey's depiction of anonymized data as a “*public good*”¹⁰¹ these references remain aspirational, and the absence of a comprehensive regulatory ecosystem limits realization of *NPD*'s promise. The 2020 Expert Committee report on *NPD* governance laid conceptual foundations proposing principles like sovereignty, public benefit, privacy, simplicity, and innovation; categorizing *NPD* into public, community, and private data; and suggesting institutional machinery like a *Non-Personal Data Authority*. India remains without any legally enforceable structure to operationalize these ideas. At the same time, the 2022 Data Accessibility & Use (DAU) Policy, envisioned to unlock government-held anonymized *NPD* for research and governance, currently lacks procedural clarity for stakeholder engagement or actionable mechanisms.¹⁰² This regulatory void impedes equitable access to data and innovation and risks reproducing power asymmetries where high-value datasets remain concentrated within a few private or state actors.

Moreover, in a rapidly evolving digital ecosystem, theoretical proposals alone are insufficient; India needs tangible, tailored policy instruments that address unique challenges such as re-identification risks, community ownership, benefit-sharing, and infrastructural capacities. Learning from international frameworks like the EU's successful free flow of *NPD* regulation and broader data governance norms that balance economic utility with democratic participation reinforces the importance of

¹⁰⁰ Nat'l Strategy for Artificial Intelligence #AIforAll, at 20–22 (NITI Aayog June 2018), <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>.

¹⁰¹ Econ. Survey 2018–19, ch. 10 (India), <https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/echapter.pdf>.

¹⁰² Draft India Data Accessibility & Use Pol'y, 2022, at 5–10, 12–15 (Ministry of Elecs. & Info. Tech. Feb. 21, 2022), <https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022>.

clear rights, access protocols, and safeguards. In essence, the rationale for advancing India's *NPD* governance is clear: a modern, actionable, and rights-sensitive regulatory structure is essential to channel *NPD*'s economic, social, and technological potential equitably, while safeguarding against misuse, exclusion, and unintended harm catalyzing responsible innovation and inclusive development in service of national and public interests.

1.7 Objectives

In the present research work, the following will be the objectives of the study:

- i. To discuss the meaning and the concept of *Non-Personal Data* in understanding the different types of data.
- ii. To understand the concept of *Non-Personal Data* under International and National legal sphere.
- iii. To analyze and compare the different National and International legal framework for the regulation of Non-Personal Data.

1.8 Hypothesis

This study is premise on the assumption that:

- A uniform legal definition of the term *Non-Personal Data* is essential for safeguarding the digital economy.
- The lack of streamlined legal frameworks for Non- Personal Data governance across jurisdictions enable its misuse by corporations for monetary gain.

1.9 Scope and Limitations

Scope

The scope of *Non-Personal Data (NPD)* governance in India encompasses the definition, management, and use of datasets that are not tied to identifiable individuals ranging from inherently non-personal streams like weather or supply-chain data to anonymized records derived from data concerning individuals that lies at the confluence of innovation, public interest, and privacy. According to the Expert

Committee on *NPD*, data qualifies as "non-personal" when it either never related to an individual or has undergone a process of removing identifiers. This *Non-Personal Data (NPD)* is further categorized into public (e.g., government-held anonymized land records or health data), community (raw data collected by municipalities or utilities), and private (derived or proprietary insights developed by private entities). The governance scope thus spans the entire lifecycle of these datasets from classification and anonymization, to institutional roles like data custodians and trustees, to the suggested establishment of a regulatory body the *Non-Personal Data Authority* to oversee rights, safeguarding, and equitable benefit-sharing. It includes mandatory data-sharing mechanisms for public good, economic development, or sovereign needs, while balancing safeguards against re-identification and misuse. The Data Accessibility & Use (DAU) Policy of 2022 situates government-held *NPD* for research and governance under its remit, proposing institutional platforms like an India Data Office, Data Management Units in ministries, and metadata and anonymization standards.

Limitations

Despite increasing focus on the potential of *Non-Personal Data (NPD)* to drive innovation, economic growth, and evidence-based policymaking, India's progress toward a comprehensive regulatory framework remains constrained by several challenges. Though the Expert Committee's 2020 proposal envisioned bold institutional structures like a standalone *Non-Personal Data Authority* and a standalone law these frameworks remain largely theoretical, lacking empirical grounding and legislative traction. A chief limitation is the over-reliance on assumptions rather than empirical evidence as many critiques note, the framework is predicated on presumed market imbalances and does not systematically engage with real-world data ecosystems or the differing roles of start-ups and incumbent players. There exists conceptual ambiguity as the delineations of "public," "community," and "private" *NPD* often overlap, and assessing the real possibility of separating *NPD* from personal or mixed datasets, particularly in an era when de-anonymization is increasingly feasible, remains highly uncertain. The proposal fails to engage with established legal fundamentals such as proprietorship, intellectual property rights, or

privacy rights tied to anonymized data raising concerns over conflicts with existing regulatory regimes and the potential for overlap or incoherence. The absence of stakeholder inclusion especially from communities whose data could be most impacted and weak enforcement mechanisms further undermine the framework's efficacy. While design proposals envision fair data sharing, they fall short of articulating how benefits would be equitably distributed or how exploitation risks would be mitigated. These combined limitations underscore the urgent need for a grounded, coherent, and evidence-informed approach to *NPD* governance one that transcends conceptual blueprints to deliver clarity, precision, and genuine societal value.

1.10 Research Methodology

This research employs a mixed-methods approach, integrating doctrinal legal analysis with empirical survey inquiry, aiming to develop a holistic perspective on how *Non-Personal Data (NPD)* is conceptualized and governed. The methodological design ensures that theoretical dimensions of law and policy are examined alongside the perceptions and experiences of real-world stakeholders. Such integration allows the study to bridge normative and practical perspectives, producing findings that are both conceptually rigorous and empirically grounded.

The doctrinal component of this research involves a systematic and critical review of primary and secondary legal materials. Primary sources include India's *Personal Data Protection Bill, 2019*¹⁰³, the *Digital Personal Data Protection Act, 2023*, and both versions issued by the *Kris Gopalakrishnan Committee Reports on Non-Personal Data Governance Framework*. The comparative dimension draws upon major international instruments, including the European Union's *General Data Protection Regulation (GDPR)*, *Regulation (EU) 2018/1807 on the Free Flow of Non-Personal Data*, *Directive (EU) 2019/1024 on Open Data and Reuse of Public Sector Information*, and the *Data Governance Act (2020)*. Other global references include the United Kingdom's *National Data Strategy (2020)*¹⁰⁴ and Australia's *Data Availability and*

¹⁰³ Personal Data Protection Bill, Bill No. 373 of 2019 (India).

¹⁰⁴ Nat'l Data Strategy, at 1–5 (U.K. Dep't for Digit. Culture, Media & Sport Sept. 9, 2020), <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>.

*Transparency Bill (2020)*¹⁰⁵, each of which offers useful insights into evolving data governance models.

Secondary sources encompass scholarly and policy-oriented literature that contributes to the theoretical framing of the research. Important works include Michèle Finck and Frank Pallas's article "*They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR*"¹⁰⁶ and Wolfgang Kerber's "*A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*."¹⁰⁷ Reports released by the "OECD" addressing issues related to cross-border data movement and value generation also function as important references for contextual analysis.¹⁰⁸ Judicial decisions are analyzed to explore how courts have approached questions of data classification, anonymity, and access in the global context. These include *YS v Minister voor Immigratie, Integratie en Asiel (Joined Cases C-141/12)*¹⁰⁹ and *C-372/12*, *Peter Nowak v Data Protection Commissioner (Case C-434/16)*¹¹⁰, *Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14)*¹¹¹, and *Scarlet Extended SA v SABAM (Case C-70/10)*¹¹². Together, these doctrinal materials help to define the conceptual parameters of *NPD* and facilitate a comparative assessment of regulatory models across jurisdictions, providing the legal foundation on which the empirical analysis is built.

The empirical component supplements the doctrinal study by capturing the perspectives of individuals who interact directly or indirectly with data governance

¹⁰⁵ Data Availability and Transparency Act 2022 (Cth) (Austl.), <https://www.legislation.gov.au/Series/C2022A00011>.

¹⁰⁶ Michèle Finck & Frank Pallas, *They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR*, 10 Int'l Data Privacy L. 11 (2020), <https://academic.oup.com/idpl/article-abstract/10/1/11/5802594>.

¹⁰⁷ Wolfgang Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, GRUR Int. 989 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2858171.

¹⁰⁸ OECD, *Cross-Border Data Flows: Taking Stock of Key Policies and Initiatives* (2022), https://www.oecd.org/en/publications/cross-border-data-flows_5031dd97-en.html.

¹⁰⁹ *YS v Minister voor Immigratie, Integratie en Asiel*, Joined Cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081 (CJEU July 17, 2014), <https://curia.europa.eu/juris/document/document.jsf?docid=155113>.

¹¹⁰ *Peter Nowak v Data Protection Commissioner*, Case C-434/16, ECLI:EU:C:2017:994 (CJEU Dec. 20, 2017), <https://curia.europa.eu/juris/document/document.jsf?docid=198059>.

¹¹¹ *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, ECLI:EU:C:2016:779 (CJEU Oct. 19, 2016), <https://curia.europa.eu/juris/document/document.jsf?docid=184668>.

¹¹² *Scarlet Extended SA v SABAM*, Case C-70/10, ECLI:EU:C:2011:771 (CJEU Nov. 24, 2011), <https://curia.europa.eu/juris/document/document.jsf?docid=115202>.

frameworks. Data were collected through structured questionnaires distributed electronically via Google Forms. This method allowed voluntary participation and flexibility, enabling respondents to engage at their convenience while ensuring informed consent prior to participation. The digital format also permitted real-time interaction, including conditional branching based on responses, thereby increasing the precision of data collection. The empirical study focused on capturing levels of awareness, perceptions of legal adequacy, ethical concerns, and practical experiences relating to *NPD*.

The target population consists of individuals from four professional or experiential categories who collectively represent the key stakeholders in data governance. These categories are legal professionals, information technology professionals, law students, and members of the general public. Legal professionals were included because *NPD* governance ultimately depends on legal interpretation, compliance, and enforcement; their insights shed light on the adequacy of statutory frameworks and implementation challenges. IT professionals offer technical insight, being directly engaged in generating, handling, and safeguarding information, and are well positioned to assess the practicality of anonymization and related governance methods. Law students, as emerging professionals and researchers, represent the transitional generation whose academic training reflects evolving legal standards and policy perspectives. Their responses provide valuable insight into the preparedness of future legal actors and the adequacy of legal education on data governance. The general public is included to ensure that the study reflects citizen awareness, perceptions, and trust in data governance mechanisms, offering a balanced and socially grounded understanding of *NPD* governance.

To ensure representative and equitable participation, the study employs a stratified sampling technique, dividing respondents equally among the four identified categories. Stratification allows for balanced representation and facilitates comparison across groups while preserving the diversity of experiences. Participants aged seventeen and above were included to ensure sufficient understanding of the subject matter, while no maximum age limit was set to account for generational variations in perception and awareness. Gender inclusivity was prioritized by welcoming responses

from participants identifying as male, female, transgender, or preferring not to disclose their gender. This inclusive approach minimizes sampling bias and promotes equity in representation.

The inclusion criteria specify that participants must belong to one of the four identified groups and demonstrate basic familiarity with law, technology, or data-related concepts, except in the case of the general public, for whom this was not mandatory. Participation was voluntary, and consent was obtained prior to data submission. Individuals who did not fall within the identified categories, failed to provide complete responses, or submitted duplicate entries (identified through IP or email tracking) were excluded from the dataset to preserve the integrity and accuracy of the findings.

A total of four hundred valid responses were targeted for the survey, with one hundred respondents from each group. The sample size was calculated through the application of “*Cochran’s formula*”, which is appropriate in the context of large or indeterminate populations. The formula is expressed as:

$$n = \frac{Z^2 \times p \times (1 - p)}{e^2}$$

“Where Z represents the standard normal deviation” at “the desired confidence level (1.96 for 95 percent confidence)”, “p represents the estimated proportion of the population possessing the characteristic of interest (0.5 to ensure maximum variability)”, and “e represents the acceptable margin of error (0.05 or 5 percent)”. When these values are substituted, the computed sample size equals 384.16, which was rounded up to 385 for practical adequacy and further increased to 400 to accommodate potential non-responses or incomplete submissions. This number provides both statistical reliability and sufficient stratification for comparative analysis.¹¹³

Data collection through Google Forms offered the advantages of efficiency, security, and wide accessibility. The structured questionnaire contained both closed-ended and

¹¹³ William G. Cochran, *Sampling Techniques* 77–78 (3d ed. 1977).

open-ended questions, the former including Likert-scale and dichotomous formats to capture the degree of agreement or awareness, and the latter designed to elicit deeper qualitative insights. The responses were automatically compiled in digital form and processed after data cleaning to remove incomplete or duplicate entries. Because the study involved no biological, financial, or personal identifiers, ethical risks were minimized.

The collected data were analyzed through a hybrid methodological approach combining quantitative and qualitative techniques. Quantitative analysis employed descriptive statistics such as frequencies, percentages, and mean distributions to summarize trends and highlight patterns across respondent groups. Cross-tabulations were used to compare responses between different strata, providing insights into how awareness and perceptions varied among legal, technological, academic, and public participants. The qualitative analysis involved thematic interpretation of open-ended responses to identify recurring ideas, opinions, and rationales that explained the quantitative findings. This combination of numerical representation and interpretive exploration allowed the study to draw both measurable and contextual conclusions regarding awareness, legal adequacy, and regulatory expectations in the governance of *NPD*.

Throughout the research process, ethical considerations were rigorously observed in compliance with the Institutional Ethics Committee (IEC) guidelines. All participants received a clear explanation regarding the study's objectives, extent, and their voluntary participation, as well as their right to withdraw at any point without penalty. Informed consent was obtained electronically prior to participation, ensuring that each respondent engaged with full understanding of the objectives and procedures. Anonymity and confidentiality were strictly maintained; no personally identifiable information was collected, and all responses were stored securely on password-protected servers accessible only to the researcher. Data were used exclusively for academic purposes and analyzed in aggregate form, ensuring that no individual respondent could be identified. These measures ensured compliance with principles of autonomy, beneficence, and justice in the conduct of social research.

By integrating doctrinal and empirical methods, this research achieves a balanced and multidimensional understanding of *Non-Personal Data* governance. The doctrinal analysis clarifies conceptual boundaries and legal frameworks across jurisdictions, while the empirical component reflects the lived realities, awareness, and attitudes of diverse stakeholder groups. Together, they enable a holistic exploration of *NPD* as both a legal construct and a socio-technical phenomenon. The methodology thus provides a robust foundation for evaluating India's current and emerging data governance regimes, identifying regulatory gaps, and recommending actionable pathways toward a coherent, inclusive, and ethically grounded framework for *Non-Personal Data* governance.

1.11 Plan of Study

Chapter 1: Introduction- This chapter introduces the research theme, tracing the evolution of data governance from the protection of personal data to the emerging need for regulating Non-Personal Data (NPD). It presents the conceptual foundation of NPD, its governance challenges, and its growing relevance to innovation, artificial intelligence, and national policy. The chapter reviews existing literature, identifies critical research gaps, articulates the rationale and significance of the study, and outlines the objectives, hypothesis, and research methodology. It situates NPD governance as a pressing legal and policy issue for India and provides the structural overview guiding subsequent chapters.

Chapter 2: Theoretical Foundations of Data as an Asset: Classification and Typologies- This chapter establishes the theoretical groundwork for understanding data as an economic, legal, and societal asset. It explains the intrinsic and instrumental value of data, delineates its types and categories, and explores global and Indian perspectives on data governance. Through an analysis of personal, non-personal, and machine-generated data, the chapter underscores how classification influences regulatory approaches, access mechanisms, and accountability frameworks. It concludes by emphasizing the need for a coherent theoretical basis to manage data as a shared resource in the digital economy.

Chapter 3: Conceptualizing Non-Personal Data: Definitions, Sources, Taxonomies, and a Proposed Legal Definition- This chapter undertakes a detailed conceptual analysis of Non-Personal Data. It compiles and critiques existing definitions, explores its various classifications, including anonymized, aggregate, machine-generated, and industrial data and proposes a comprehensive legal definition suited to India's socio-economic and technological realities. The discussion extends to jurisprudential interpretations of administrative, health, communication, and media data, highlighting cross-jurisdictional trends. The chapter also identifies stakeholders within the NPD ecosystem and examines challenges related to ownership, privacy, and community rights, setting the stage for comparative and governance-focused discussions in later chapters.

Chapter 4: Comparative Legal Frameworks Governing Non-Personal Data: A Cross-Jurisdictional Analysis- This chapter presents a detailed comparative study of Non-Personal Data governance frameworks across multiple jurisdictions including Germany, France, Finland, Estonia, the United States, China, the United Kingdom, Singapore, Japan, Brazil, Canada, Australia, South Korea, and Kenya. It evaluates legal definitions, institutional models, and governance mechanisms adopted in these countries. Using analytical and theoretical frameworks, it identifies convergences and divergences in regulatory approaches. The chapter concludes with a comparative synthesis highlighting best practices and lessons that can inform India's evolving NPD governance structure.

Chapter 5: Governance Imperatives in Non-Personal Data: Need for Regulatory Intervention- This chapter justifies the necessity of a structured governance framework for Non-Personal Data. It explores economic, social, ethical, and international imperatives that demand proactive regulation, especially in the context of AI, digital markets, and data-driven governance. By examining the consequences of regulatory absence, the chapter proposes guiding principles such as harmonized definitions, balanced innovation, ethical oversight, and global cooperation. It concludes that effective governance of NPD is not merely a legal requirement but a developmental necessity essential for equitable and sustainable data-driven growth.

Chapter 6: Governance Framework for Non-Personal Data in India: Evolution, Challenges, and Prospects- This chapter traces the chronological evolution of India's data governance architecture from the Information Technology Act of 2000 to the *Digital Personal Data Protection Act* of 2023 and related policies such as NDSAP, NDGFP, and the Non-Personal Data Governance Framework. It examines institutional initiatives, legislative efforts, and policy reforms shaping India's approach to data regulation. The chapter also identifies persisting gaps in the legal, technical, and institutional dimensions of NPD governance and discusses relevant judicial precedents. It concludes with a critical assessment of India's preparedness for establishing an effective Non-Personal Data regulatory regime.

Chapter 7: Empirical Analysis of Legal Awareness and Governance of Non-Personal Data- This chapter presents the empirical findings derived from a mixed-methods approach involving structured questionnaires distributed among legal professionals, IT professionals, law students, and the general public in the Delhi NCR region. It evaluates awareness, perceptions, and attitudes towards NPD, the adequacy of existing laws, and the perceived need for regulation. The analysis, supported by graphical and percentage-based interpretations, reveals gaps in awareness, enforcement, and legal sufficiency across respondent groups. It further highlights the consensus on the need for dedicated NPD legislation and global harmonization, reinforcing the study's doctrinal insights through empirical validation.

Chapter 8: Conclusion and Recommendations- The final chapter synthesizes findings from both doctrinal and empirical analyses to present consolidated conclusions on the governance of Non-Personal Data. It underscores that while India has made substantial progress in personal data protection, the absence of a clear and enforceable framework for NPD remains a critical gap. The chapter offers targeted recommendations for legislative reform, institutional development, and international cooperation. It concludes by emphasizing the need for a balanced regulatory approach that promotes innovation while ensuring ethical use, accountability, and equitable distribution of data-derived benefits.

CHAPTER 2

THEORETICAL FOUNDATIONS OF DATA AS AN ASSET: CLASSIFICATION AND TYPOLOGIES

i.1. Introduction

i.2. Understanding Data

2.3. Value Of Data

2.4 Laws and Governance of Data: Global and Indian Perspectives

2.5 Various Types of Data

2.6 Major Data Categories: Personal Data and Machine-Generated Data

2.7 Conclusion

2.1 Introduction

“Information is an asset, yet it is rarely, if ever, managed like one.”¹¹⁴

—Doug Laney

The importance of data has grown immensely within the expanding digital economy. Over the past decade, organizations that have strategically integrated data into their operational and decision-making frameworks have emerged as global leaders among the world’s most valuable enterprises.¹¹⁵ The body of work examining the economics of data encompasses distinct areas such as growth, privacy, competition, inclusion, and financial stability.¹¹⁶

The expansion of data within the economy presents a significant opportunity to enhance growth by fostering efficiency and driving innovation. To achieve growth without undermining other objectives, it is argued that existing policy frameworks

¹¹⁴ DOUG LANEY, *INFONOMICS: HOW TO MONETIZE, MANAGE, AND MEASURE INFORMATION AS AN ASSET FOR COMPETITIVE ADVANTAGE* 3 (2017).

¹¹⁵ McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* 15 (2016), <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/digital-globalization-the-new-era-of-global-flows>.

¹¹⁶ World Bank, *World Development Report 2021: Data for Better Lives* 10, <https://www.worldbank.org/en/publication/wdr2021>.

require updating.¹¹⁷ The lack of transparency in data markets may be contributing to excessive data collection while compromising individual privacy.¹¹⁸ Defining the rights and responsibilities associated with data is crucial for ensuring market efficiency, and the way these are distributed will have a profound impact on both economic growth and social equity.¹¹⁹ Existing entities are motivated to retain data, which may hinder competition and diminish the societal benefits that could arise from broader accessibility.¹²⁰ Strategies that foster data sharing can enhance competition and drive innovation.¹²¹

There is also uncertainty regarding whether companies adequately safeguard the data they hold, raising risks to stability that must be addressed through measures requiring all market participants to invest sufficiently in cybersecurity.¹²² The absence of coordinated efforts among nations further risks fragmentation in global data markets, undermining the substantial benefits of cross-border data activities, including trade and finance.¹²³

The true economic potential of data can be obscured by these challenges, creating a disconnect between those who possess valuable datasets and the innovative businesses and entrepreneurs equipped to leverage them.¹²⁴ Data can only reach its full potential when allowed to circulate freely among economic participants.¹²⁵ The government therefore holds the view that policies should guarantee that companies seeking to innovate in data have access to high-quality, well-maintained datasets from across

¹¹⁷ OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* 20 (2015), <https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm>.

¹¹⁸ *Id.* at 22.

¹¹⁹ European Commission, *A European Strategy for Data* 5 (2020), https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data_en.pdf.

¹²⁰ *Id.* at 8.

¹²¹ World Economic Forum, *Data Collaboration for the Common Good* 12 (2019), <https://www.weforum.org/reports/data-collaboration-for-the-common-good/>.

¹²² *Id.* at 15.

¹²³ The White House, *National Cybersecurity Strategy* (Mar. 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/national-cybersecurity-strategy/>.

¹²⁴ UNCTAD, *Digital Economy Report 2021* 25, https://unctad.org/system/files/official-document/der2021_en.pdf.

¹²⁵ *Id.* at 28.

sectors.¹²⁶ Such policies would yield both economic and social benefits. However, they also raise concerns regarding privacy and data protection.¹²⁷

The government has reaffirmed its commitment to protecting personal data by introducing new rights that enable individuals to exercise greater control over their own information.¹²⁸ The *Data Protection Act 2018* updates and strengthens the United Kingdom's data protection framework to reflect the realities of the digital age.¹²⁹ It raises the standards for personal data security, brings national legislation in line with the *European Union's General Data Protection Regulation (GDPR)*, and grants individuals expanded authority over how their data is processed and used.¹³⁰

Under this regime, individuals benefit from enhanced access to the information held about them and the ability to assess its accuracy. They also gain from innovations such as personalized recommendations and customized digital services.¹³¹ The framework seeks to balance individual autonomy in data governance with the promotion of innovation.¹³² The *Information Commissioner's Office (ICO)* is empowered to impose penalties reaching up to £17.5 million or 4% of a company's global annual turnover, whichever is greater, in instances of non-compliance.¹³³

This provides strong incentives for data-processing entities to establish robust safeguards.¹³⁴ Importantly, this framework is not an impediment to data-driven innovation but rather an opportunity to build trust.¹³⁵ By strengthening data protection,

¹²⁶ *Id.* at 30.

¹²⁷ UK Government, *National Data Strategy* 18 (2020), <https://www.gov.uk/government/publications/uk-national-data-strategy>.

¹²⁸ *Id.* at 20.

¹²⁹ Data Protection Act 2018, c. 12 (UK), <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>.

¹³⁰ *Id.*

¹³¹ Regulation (EU) 2016/679, art. 4, 2016 O.J. (L 119) 1 [hereinafter GDPR], <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

¹³² Boston Consulting Group, *The Value of Our Digital Identity* 12 (2012), <https://www.bcg.com/publications/2012/value-digital-identity>.

¹³³ *Id.* at 15.

¹³⁴ Data Protection Act 2018, c. 12, § 155 (UK); Regulation (EU) 2016/679 (General Data Protection Regulation), art. 83.

¹³⁵ Information Commissioner's Office, *Guide to the GDPR*, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>.

the government aims to foster public confidence in responsible data sharing for societal and economic purposes.¹³⁶

In the long term, building such trust ensures that individuals feel confident their data will be handled responsibly and not transferred or accessed without their consent. This is expected to expand the availability of data for innovative, data-driven enterprises.¹³⁷ The government recognizes, however, that safeguarding personal data alone may not suffice to prevent harm. Data obtained lawfully can still be misused in ways that raise ethical concerns, such as algorithmic profiling or discrimination.¹³⁸ This reasoning forms the basis for creating the “*Centre for Data Ethics and Innovation*”, an institution responsible for promoting the ethical and secure use of both personal and *Non-Personal Data* in technological advancement.¹³⁹

Formulating such a policy stance presents several challenges, particularly in ensuring access to information.¹⁴⁰ Globally, most data produced pertains to individuals, data associated with or capable of identifying specific persons. Ensuring robust safeguards for personal information is therefore essential, not only for maintaining security but also for protecting the individual’s right to privacy.¹⁴¹ In a democratic framework, public confidence in the safe and transparent management of personal data constitutes a cornerstone of the digital economy.¹⁴²

Personal information holds significance that surpasses its basic informational value¹⁴³; it is a vital asset contributing to both economic and social value for enterprises and individuals alike. The Boston Consulting Group projected that across Europe, the measurable benefits from personal data applications could reach €1 trillion annually by 2020, two-thirds accruing to consumers and one-third to businesses.¹⁴⁴ This is

¹³⁶ *Id.*

¹³⁷ UK Government, *Data: A New Direction* 10 (2021), <https://www.gov.uk/government/consultations/data-a-new-direction>.

¹³⁸ *Id.* at 12.

¹³⁹ Algorithmic Justice League, *AI and Ethics* 8 (2022), <https://www.ajl.org/reports>.

¹⁴⁰ Centre for Data Ethics and Innovation, *About Us*, GOV.UK, <https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation>.

¹⁴¹ World Bank, *Supra note 116*, at 15.

¹⁴² *Id.* at 18.

¹⁴³ *Id.* at 20.

¹⁴⁴ *Id.* at 22.

because personal data enables companies to offer tailored products, personalized services, and improved customer experiences, creating advantages for both buyers and sellers.¹⁴⁵

As technology continues to shape user experiences, reliance on personal data is expected to increase.¹⁴⁶ For instance, geolocation data is anticipated to transform consumer engagement with the high street, eliminating the need for queuing and facilitating seamless services.¹⁴⁷

Beyond Europe, corporations worldwide are deeply engaged in extracting insights from the digital economy. They sift through networks of preferences, decisions, and geographical information in search of valuable personal data.¹⁴⁸ Data has become a quintessentially portable asset, yet its transnational movement requires cohesive international policies to build trust.¹⁴⁹ In the absence of universally accepted governance frameworks, digital divides between nations risk deepening as large data reservoirs become fragmented.¹⁵⁰ This would impose disproportionate burdens on smaller or economically disadvantaged nations.¹⁵¹

The way in which nations address issues of privacy, competition, and stability reflects their overarching national priorities.¹⁵² However, such divergence can create fragmentation, posing particular challenges for smaller nations with limited data resources and high dependence on multinational digital corporations. In some advanced nations, strong privacy safeguards can even function as trade barriers, raising compliance costs for exporters from developing economies.¹⁵³

There is thus a compelling case for establishing universal principles to govern the data economy. For example, shared definitions in government regulations concerning

¹⁴⁵ Boston Consulting Group, *Supra note 132*, at 10.

¹⁴⁶ *Id.* at 12.

¹⁴⁷ McKinsey Global Institute, *The Age of Analytics* 25 (2016), <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world>.

¹⁴⁸ *Id.* at 28.

¹⁴⁹ *Id.* at 30.

¹⁵⁰ OECD, *Cross-Border Data Flows: Taking Stock* 15 (2022), <https://www.oecd.org/sti/cross-border-data-flows.htm>.

¹⁵¹ *Id.* at 18.

¹⁵² *Id.* at 20.

¹⁵³ UNCTAD, *Supra note 124*, at 22.

personal privacy, as well as clarity on the types of firms and activities to which these apply, could help minimize policy discrepancies across countries.

Indian Perspective

In the Indian context, Section 2(1)(o) of the “*Information Technology Act, 2000*”, provides the statutory definition of the term *data* as follows:

*“A representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.”*¹⁵⁴

Until 2023, India did not have a comprehensive legal instrument dedicated exclusively to data protection.¹⁵⁵ The “Information Technology Act, 2000 (IT Act)”, together with the “Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011”, constituted the foundational legal framework governing data privacy and security.¹⁵⁶

A major turning point came in 2017 when a nine-judge bench of the “Supreme Court of India”, in its landmark judgment in “*Justice K. S. Puttaswamy (Retd.) v. Union of India* [Writ Petition No. 494/2012]”, declared the right to privacy to be an intrinsic part of the right to life and personal liberty under “Article 21 of the Constitution”.¹⁵⁷ This decision laid the groundwork for a more structured and comprehensive data protection regime.¹⁵⁸

Following extensive public consultation and several revisions of draft data protection bills, the “Ministry of Electronics and Information Technology (MeitY)” issued the

¹⁵⁴ *Id.* at 25.

¹⁵⁵ Information Technology Act, 2000, § 2(1)(o).

¹⁵⁶ *Id.*

¹⁵⁷ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India), <https://www.meity.gov.in/content/information-technology-reasonable-security-practices-and-procedures-and-sensitive-personal>.

¹⁵⁸ *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

“Digital Personal Data Protection Bill, 2022”¹⁵⁹, for public review. The final version, passed by both Houses of Parliament, introduced key refinements and was subsequently enacted as the “Digital Personal Data Protection Act, 2023 (DPDP Act).”¹⁶⁰ The “DPDP Act” prescribes standards and obligations for the collection, processing, storage, and transfer of digital personal information. Nonetheless, for its full operationalization, several follow-up actions are required, including the notification of its provisions, repeal of the 2011 Privacy Rules, and formulation of subsidiary rules and regulatory guidelines.¹⁶¹

It is significant to observe that the scope of the “DPDP Act” is limited to “digital personal data.”¹⁶² *Non-Personal Data* and data existing in non-digital formats continue to remain outside its regulatory domain.¹⁶³ As of now, India’s privacy framework remains rooted in the IT Act and Privacy Rules. Although the government has published draft regulations for the DPDP Act, the substantive provisions are yet to be brought into force.¹⁶⁴

2.2 Understanding Data

2.2.1 Nature of Data

The term *data* encompasses a wide array of information that can be processed by devices or documented for subsequent processing. This may include written content, visual elements, and auditory materials, which may constitute personal or non-personal information.¹⁶⁵ The legal ramifications of data primarily focus on aspects such as data protection, privacy rights, and ownership issues, particularly concerning personal information.¹⁶⁶

¹⁵⁹ *Id.*

¹⁶⁰ Digital Personal Data Protection Bill, 2022 (Ministry of Elecs. & Info. Tech., released for public consultation Nov. 18, 2022).

¹⁶¹ Digital Personal Data Protection Act, 2023.

¹⁶² *Id.*

¹⁶³ *Id.* § 2(t).

¹⁶⁴ Information Technology Act, 2000, § 2(1)(o).

¹⁶⁵ CODATA, *What is Data?*, <https://codata.org/what-is-data/>.

¹⁶⁶ *Id.*

The following points outline the characteristics of data:

- i. Suitability for Application: Data are facts that serve as the basis for decision-making. Their utility lies in their capacity to be applied in practical contexts.¹⁶⁷ While not all data must necessarily be used if deemed unsuitable, the inherent potential for application remains a defining trait.¹⁶⁸
- ii. Clarity: As per the definition provided by CODATA (Committee on Data of the International Science Council), data must represent a refined and clear presentation of facts.¹⁶⁹ Clarity is essential to ensure that the intended message is not obscured, but instead highlights the fundamental aspects of the issue at hand.
- iii. Precision: Accuracy is a fundamental characteristic of data. Since data provide the foundation for decision-making, they must be genuine, comprehensive, and precise to allow valid conclusions to be drawn.¹⁷⁰
- iv. Quality: In social sciences, extensive amounts of data are often collected. However, it is neither feasible nor necessary to present them in full. Instead, data undergo processes of compression and refinement to capture the essential qualities or insights. In scientific contexts, data typically consist of quantifiable measurements derived from experiments.¹⁷¹ In both fields, refined data must represent the core essence of the matter under study.¹⁷²

2.2.1 Meaning of Data in General

The word *data* derives from the Latin *datum*, meaning “something given.” It was first used in the 17th century by philosophers, “*Thomas Hobbes and John Locke*” to denote “facts given” as a basis for reasoning.¹⁷³ The first systematic definition of data emerged in the mid-20th century with the rise of information theory and computing, when data

¹⁶⁷ *Id.*

¹⁶⁸ *Id.*

¹⁶⁹ CODATA, *Data Science Journal*, <https://datascience.codata.org/>.

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

¹⁷² *Id.*

¹⁷³ Oxford English Dictionary, *Data* (2023), https://www.oed.com/dictionary/data_n.

came to be understood as symbols or representations processed by machines.¹⁷⁴ Today, *data* generally refers to representations of information, knowledge, facts, concepts, or instructions that can be structured, stored, and processed by humans or machines.¹⁷⁵

The concept of 'data' encompasses information that:

(a) is undergoing processing through equipment that operates automatically in accordance with provided instructions.¹⁷⁶

(b) is documented with the purpose of being processed by such equipment.¹⁷⁷

(c) is documented within a pertinent filing system.¹⁷⁸

Data forms the base of the DIKW hierarchy¹⁷⁹:

Data → Information → Knowledge → Wisdom.

2.2.3 Definitions of Data by Thinkers and Frameworks

Intellectual Perspectives

i. Daniel Bell – The Information Society

*“The novel and central feature of post-industrial society is the codification of theoretical knowledge and the new relation of science to technology.”*¹⁸⁰ -By “Daniel Bell, *The Coming of Post-Industrial Society* (1973)”

“Daniel Bell’s” seminal work *The Coming of Post-Industrial Society* (1973) presents the idea that identified a transformative shift from industrial to post-industrial society, emphasizing the centrality of information and knowledge.¹⁸¹ He highlighted the

¹⁷⁴ Claude E. Shannon, A Mathematical Theory of Communication, 27 BELL SYS. TECH. J. 379, 383 (1948).

¹⁷⁵ *Id.*

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ *Id.*

¹⁷⁹ Jennifer Rowley, The Wisdom Hierarchy: Representations of the DIKW Hierarchy, 33 J. INFO. SCI. 163 (2007).

¹⁸⁰ DANIEL BELL, *THE COMING OF POST-INDUSTRIAL SOCIETY* 20 (Basic Books 1973).

¹⁸¹ *Id.*

increasing importance of theoretical knowledge and its codification in shaping societal structures and economies.

ii. Manuel Castells – The Network Society

“The Internet is a communication medium that allows for the first time, the communication of many to many, in chosen time, on a global scale.”¹⁸²-By Manuel Castells

Sociologist Manuel Castells, in his trilogy *“The Information Age: Economy, Society and Culture”* (1996–1998), examines the rise of a networked society in which information and communication technologies transform social and economic systems.¹⁸³

iii. Luciano Floridi – The Infosphere

“The infosphere is the environment made up of information in which we experience our everyday lives.”¹⁸⁴-By Luciano Floridi

Philosopher Luciano Floridi introduces the concept of the “infosphere,” describing it as an “informational ecosystem encompassing all informational entities”, including digital data, wherein the boundaries between online and offline realities converge.¹⁸⁵

In the world of legal frameworks, the term "data" encompasses a wide array of representations, including information, facts, concepts, or instructions that are systematically organized and designed for processing within a computer system or network. This may encompass information presented in diverse formats, including electronic records, tangible documents, or even subjective viewpoints.

¹⁸² MANUEL CASTELLS, *THE INFORMATION AGE: ECONOMY, SOCIETY AND CULTURE* 10 (Blackwell 1996).

¹⁸³ *Id.*

¹⁸⁴ LUCIANO FLORIDI, *THE FOURTH REVOLUTION: HOW THE INFOSPHERE IS RESHAPING HUMAN REALITY* 15 (Oxford Univ. Press 2014).

¹⁸⁵ *Id.*

iv. Shoshana Zuboff – Surveillance Capitalism

*“Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data.”*¹⁸⁶-By “Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019)”.

In *The Age of Surveillance Capitalism* (2019), Harvard Business School professor Shoshana Zuboff introduces the concept of surveillance capitalism, where human experience is commodified as data for profit.¹⁸⁷

Legal and Institutional Definitions

i. India – Information Technology Act, 2000 (Section 2(1)(o))

*“Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.”*¹⁸⁸

“A structured depiction of information, knowledge, facts, concepts, or directives” – which are structured in a systematic manner and processed, or intended for processing, within a computer system or network. The IT Act delineates that data can exist in various forms and may be retained within the internal memory of a computer.

ii. European Union – *General Data Protection Regulation (GDPR)*, Article 4(1)

“‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be

¹⁸⁶ SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 8 (PublicAffairs 2019).

¹⁸⁷ *Id.*

¹⁸⁸ Information Technology Act, 2000, § 2(1)(o).

identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier...”¹⁸⁹

“Regulation (EU) 2016/679” concerns the protection of natural persons with respect to the processing of personal information and the free movement of such data. The implementation of the GDPR represents a crucial advancement in fortifying individuals' fundamental rights within the digital landscape, while also streamlining business operations by elucidating regulations for enterprises as well as government bodies operating within the digital single market.

A singular legal framework notably diminishes the disparities among various national systems and eliminates superfluous administrative encumbrances.

- iii. United States – California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(o)(1)

*“‘Personal information’ means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”*¹⁹⁰

The California Consumers Privacy Act (CCPA) signifies a significant advancement in the realm of privacy within the United States, with its foundation resting on the broad interpretation of personal information. A comprehensive understanding of how the CCPA defines personal information requires an examination of its four interrelated components.: (i) “information”; (ii) “that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked”; (iii) “directly or indirectly”; (iv) “with a particular consumer or household”. For any particular piece of data to be classified as personal information under the CCPA, it must satisfy the four criteria previously established.

¹⁸⁹ GDPR, art. 4(1).

¹⁹⁰ California Consumer Privacy Act, Cal. Civ. Code § 1798.140(o)(1) (West 2020).

iv. India – Digital Personal Data Protection (DPDP) Act, 2023, Section 2(t)

“‘Personal data’ means any data about an individual who is identifiable by or in relation to such data.”¹⁹¹

The Act highlights the critical need to protect digital personal information. Consequently, it is essential that entities responsible for collecting, storing, and processing such information ensure its effective protection.

v. OECD

“Data are a set of values of qualitative or quantitative variables; restated, pieces of data are individual pieces of information.”¹⁹²

The OECD underscores that respect for privacy is essential to a well-functioning digital economy, as it fosters trust, enabling individuals to participate confidently in online activities and share data, which in turn fuels economic growth, innovation, and cross-border data flows. Its Privacy Guidelines a foundational, internationally agreed set of eight core principles like collection limitation, security safeguards, openness, and individual participation are designed to be technologically neutral and adaptable, ensuring resilience amid rapid digital transformation. The OECD further emphasizes that building trust requires holistic international cooperation, including interoperable regulatory frameworks, robust enforcement mechanisms, and a clear balance between personal-window protections and government access. This encompasses safeguards for national security and law enforcement, reinforcing democratic values and facilitating global data interoperability.

vi. UNCTAD – Digital Economy Report 2021

The ICT Policy Section of the UNCTAD Division on Technology and Logistics conducts policy-oriented analytical work on the implications of e-commerce and information and communications technologies (ICTs) for development.¹⁹³ Previously known as the Information Economy Report, it is in charge of creating the Digital

¹⁹¹ Digital Personal Data Protection Act, 2023, § 2(t).

¹⁹² OECD, *Privacy Guidelines* 10, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

¹⁹³ UNCTAD, *Digital Economy Report* 2021, https://unctad.org/system/files/official-document/der2021_en.pdf.

Economy Report. In addition to helping developing nations increase their ability to monitor e-commerce and the digital economy and to create and execute relevant laws and regulations, the ICT Policy Section fosters global discussion on topics pertaining to ICTs for development. The Section oversees the eTrade for all program. Where applicable, the words "country" and "economy" relate to regions or territories in this report. The country group classifications are only for statistical or analytical purposes and do not necessarily reflect an assessment of the level of development attained by a certain nation or region.

2.3 Value of Data

In the contemporary digital economy, data is widely acknowledged as a key strategic resource, driving efforts to establish comprehensive legal frameworks aimed at realizing its full potential.¹⁹⁴ Economically, data is non-rivalrous, often excludable, generates externalities, and holds significant option value.¹⁹⁵ Unlike traditional assets, datasets can be reused endlessly at almost no marginal cost, yet substantial investment is required to collect and maintain them.¹⁹⁶ These characteristics justify legal recognition of data as a unique asset class while revealing that conventional property rules require adaptation to accommodate its distinct nature.¹⁹⁷

Regulatory regimes such as the “European Union’s *General Data Protection Regulation (GDPR)*” frame data protection as a fundamental right, mandating transparency, consent, purpose limitation, and breach notification.¹⁹⁸ Though GDPR does not confer explicit property rights, its complex system of user rights and corporate obligations mirrors certain property-style controls, ensuring that individuals exercise significant individuals are granted greater authority over their personal information, while organizations incur significant penalties in cases of non-compliance.¹⁹⁹

¹⁹⁴ World Economic Forum, *Supra* note 121, at 10.

¹⁹⁵ *Id.* at 12.

¹⁹⁶ *Id.* at 15.

¹⁹⁷ *Id.* at 18.

¹⁹⁸ GDPR, arts. 5–6, 33.

¹⁹⁹ *Id.* art. 83.

Explicit legal "ownership" of data is still rare. Existing protections usually flow from a mix of intellectual property laws such as copyright or database rights, contractual agreements, trade secrets, and privacy rules.²⁰⁰ However, recent legislative trends exemplified by the EU Data Act are shifting focus away from proprietary control toward defined access and usage rights.²⁰¹ This reflects a broader policy preference for fair and regulated access to data over traditional ownership models.

In contrast, jurisdictions like China have begun to formally acknowledge data as a balance-sheet asset.²⁰² New regulations allow companies to count data resources as assets and pledge them in financing arrangements, signaling a legal recognition of data's financial value. These measures mark a significant departure from viewing data merely as intangible information, instead framing it as something that can support investment and credit.

The global relevance of data is further evident in the emergence of cross-border data governance frameworks.²⁰³ Regulations that restrict data transfers, particularly those related to privacy, trade, and national security policy demonstrate that data is both economically valuable and strategically sensitive. Diverging national approaches, such as GDPR's strict model versus lighter regimes like the U.S. or emerging frameworks in India, illustrate the ongoing struggle to balance privacy, economic efficiency, and sovereignty.²⁰⁴ Intellectual property law intersects with data regulation, offering protection for creative compilations, trade-secrets, and inventions.²⁰⁵ Yet raw data generally lies beyond the reach of IP. In practice, contractual arrangements with

²⁰⁰ WIPO, *Intellectual Property and Data* 5 (2021), <https://www.wipo.int/publications/en/details.jsp?id=4567>.

²⁰¹ EU Data Act, Regulation (EU) 2023/2854, 2023 O.J. (L 2854), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854>.

²⁰² Ministry of Finance (PRC), *Guiding Opinions on Strengthening Data Asset Management* (Dec. 31, 2023) and Interim Provisions on Accounting Treatment of Enterprise Data Resources (effective Jan. 1, 2024).

²⁰³ OECD, *Supra* note 124, at 15.

²⁰⁴ *Id.* at 18.

²⁰⁵ WIPO, *Supra* note 200, at 8.

carefully negotiated terms concerning scope, purpose, remuneration, and retention remain the most adaptable and reliable tool for defining and transferring data rights.²⁰⁶

Over the past several years, European data policy has increasingly incorporated property-like concepts into its structure, granting individuals enforceable rights over how their data is used and transferred.²⁰⁷ Frameworks like the EU Data Governance Act also promote structured data sharing through licensure and governance rules, reinforcing the status of data as a regulated asset. While legal systems have not yet granted data full-fledged ownership akin to conventional property, they have constructed a layered legal ecosystem combining privacy rights, IP protections, contractual agreements, asset-recognition policies, and governance standards.²⁰⁸ This hybrid approach seeks to ensure that data delivers value while protecting individual rights, spurring innovation, and harmonizing global and national considerations. As data continues to underpin economic growth, we can expect legal regimes to evolve further toward clearer valuation, exchange mechanisms, and proprietary frameworks.²⁰⁹

While legal regimes grapple with ownership, access, and protection, the economic and social value of data further complicates the regulatory challenge. Understanding data's dual nature, as both a commercial asset and a social resource, illustrates why governance frameworks must balance private incentives with public goods.

Economic & Social Value of Data

As the digital revolution reshapes societies and markets, data has become a fundamental pillar supporting both economic growth and social development.²¹⁰ On the economic front, data functions as a strategic asset that enhances organizational productivity, stimulates innovation, and contributes meaningfully to national

²⁰⁶ *Id.* at 10.

²⁰⁷ EU Data Governance Act, Regulation (EU) 2022/868, 2022 O.J. (L 152), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>.

²⁰⁸ *Id.*

²⁰⁹ World Bank, *Supra note* 116, at 25.

²¹⁰ *Id.* at 28.

income.²¹¹ By enabling businesses to refine operational processes and tailor offerings to specific needs, data analytics unlocks efficiency gains and unlocks novel revenue streams.²¹² Adoption of data-driven strategies across industries ranging from logistics to finance helps elevate workforce performance and fosters competitive advantage, cumulatively lifting productivity and economic growth.

Beyond the corporate realm, open and responsibly shared data offers substantial social value. For instance, when public institutions make geospatial or environmental data widely available, it empowers communities and local authorities to make better-informed decisions from managing natural disasters to designing safer transportation networks. In public health, the integration of anonymized mobility or clinic data can help identify underserved areas, informing targeted interventions and enabling equitable access to services.²¹³ In education, learning analytics derived from anonymized student performance data supports personalized approaches, helping close achievement gaps and improving outcomes for disadvantaged learners.²¹⁴

These economic and social benefits stem from the inherent characteristics of data. Unlike traditional goods, data is non-rivalrous, multiple stakeholders can use it concurrently, and it generates strong positive externalities, as combining datasets often generates insights far greater than the sum of their parts.²¹⁵ Furthermore, data carries option value: information collected today may reveal transformative opportunities in the future, especially when coupled with advances in artificial intelligence, machine learning, and computational capacity.²¹⁶

However, realizing data's full potential requires thoughtful systems of governance. Since market mechanisms alone struggle to account for the broader societal value of shared data, public policy must intervene to align incentives.²¹⁷ This can include legal

²¹¹ McKinsey Global Institute, *Supra* note 115, at 20.

²¹² *Id.* at 22.

²¹³ Open Data Institute, *The Value of Open Data* 10 (2020), <https://theodi.org/insights/the-value-of-open-data/>.

²¹⁴ *Id.* at 12.

²¹⁵ *Id.* at 15.

²¹⁶ *Id.* at 18.

²¹⁷ *Id.* at 20.

frameworks to protect privacy, regulations to ensure data security, and mechanisms such as data trusts or cooperatives that encourage pooling of anonymized datasets for public benefit. Supporting infrastructure and standards, including interoperability and open formats, are also essential to maximize data's reach.²¹⁸

When policy design successfully balances private rights with public goods, economic and social objectives reinforce one another: firms gain competitive advantage through better insights, while society benefits from smarter public services, increased resilience, and more inclusive development.²¹⁹ In this way, data operates not only as a commercial asset but also as a force for broader human well-being in the digital age.

This makes data markets challenging to build and keep running, and it also means that governance frameworks may make or break data sharing and reuse, which in turn affects access to data and the value it can provide.

Excludability and non-rivalry: Data holds a unique economic position due to two key characteristics: non-rivalry and excludability. As a non-rival resource, data can be simultaneously utilized by multiple stakeholders without reducing its worth or accessibility; each participant can draw upon the complete dataset without affecting others.²²⁰ This quality allows datasets to generate exceptional value when combined, creating positive spillovers and network effects: shared or aggregated data often produces insights far greater than the sum of individual contributions.²²¹ However, data also tends to be excludable organizations can restrict access through technical means such as encryption, proprietary platforms, or legal tools like contracts and intellectual property.²²² This dual nature places data in the category of club goods: it provides broad social and economic benefits through shared use, yet control remains

²¹⁸ *Id.* at 22.

²¹⁹ *Id.* at 25.

²²⁰ CARL SHAPIRO & HAL R. VARIAN, *INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY* 20 (1999).

²²¹ International Data Corporation, *The Economic Impact of Data Sharing* 12 (2023), <https://www.idc.com/getdoc.jsp?containerId=US49912323>.

²²² World Intellectual Property Organization, *Data and Intellectual Property* 15 (2021), <https://www.wipo.int/publications/en/details.jsp?id=4567>.

concentrated among holders who can gatekeep who gets access.²²³ The result is a delicate balance on one hand, wide data sharing fuels innovation and inclusive growth; on the other, strategically withheld data can reinforce power imbalances, constrain competition, and limit societal benefit.²²⁴

In economics, an externality is the benefit or cost felt by a party who does not directly participate in an activity.²²⁵ When those involved in an economic activity do not pay their fair share of the expenses, this is called a negative externality.²²⁶ In the data economy, this may occur when personal data is collected and monetized without adequate privacy safeguards, shifting costs onto individuals rather than processors.²²⁷ In contrast, a positive externality arises when the advantages of an economic activity are not fully absorbed by the people who engage in it.²²⁸ In data contexts, this can be seen when mobility or geospatial data is shared, improving services such as traffic management and disaster response, even for those who never directly provided or used the data.²²⁹ Market failures are produced in both instances by externalities.²³⁰ Since they do not have to bear the whole cost of an economic activity's negative externalities, the players involved may be motivated to participate in more of it than is socially optimum.²³¹ However, since agents may not be able to reap the full advantages of an activity when it has positive externalities, they may engage in less of it than is socially ideal.²³²

²²³ OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* 25 (2015), <https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm>.

²²⁴ World Bank, *World Development Report 2021: Data for Better Lives* 30, <https://www.worldbank.org/en/publication/wdr2021>.

²²⁵ JOSEPH E. STIGLITZ, *ECONOMICS OF THE PUBLIC SECTOR* 85 (4th ed. 2015).

²²⁶ *Id.* at 87.

²²⁷ European Data Protection Board, *Guidelines on Data Protection by Design and Default* 10 (2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042019-data-protection-design-and-default_en.

²²⁸ STIGLITZ, *ECONOMICS OF THE PUBLIC SECTOR* 90 (4th ed. 2015).

²²⁹ Open Data Institute, *The Value of Open Data* 15 (2020), <https://theodi.org/insights/the-value-of-open-data/>.

²³⁰ *Id.* at 18.

²³¹ European Commission, *A European Strategy for Data* 8 (2020), https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data_en.pdf.

²³² *Id.* at 10.

The individuals involved in gathering, distributing, and using data often fail to fully absorb the consequences of their actions on the larger community.²³³ If more people had access to mobility data, for instance, city traffic may become more efficient, which would mean shorter commutes for everyone, even those who don't use mapping applications very often. Even while these advantages may be quantifiable, those who gather, share, or use the data, or who use data-enabled services, may not fully internalize them. There will be a lack of market incentives to engage in data collecting and sharing when positive externalities are present since neither the collectors nor the users can fully internalize the advantages of the data.

Certain kinds of personal data might be useful for society, but doing so can compromise people's privacy, leading to problems (or costs) that the data users don't necessarily feel.²³⁴ The market cannot simply re-allocate those expenses to their creators. The decision-makers, data producers, and distributors do not take the societal consequences of their actions into account.

Because data can often be used to create groupings or links between diverse actors based on important common qualities, it may become valuable.²³⁵ However, this capacity can also lead to data externalities. To better focus their public services, governments often utilize data that groups individuals by socioeconomic class. Similarly, retail companies often use data that groups people by consumption habits to optimize their marketing campaigns. Given the interconnected nature of data, it could be more economically sound to see it as a shared resource, rather than an item whose optimal organization is based on open market trade.²³⁶

When evaluating the advantages of broadening access to data, one must weigh such advantages against the attendant costs of data collection and dissemination. As the

²³³ World Economic Forum, *Data Collaboration for the Common Good* 20 (2019), <https://www.weforum.org/reports/data-collaboration-for-the-common-good/>.

²³⁴ European Data Protection Board, *Guidelines on Processing Personal Data* 12 (2021), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-processing-personal-data_en.

²³⁵ UNCTAD, *Digital Economy Report 2021* 30, https://unctad.org/system/files/official-document/der2021_en.pdf.

²³⁶ Gartner, *The Value of Data in the Digital Economy* 10 (2022), <https://www.gartner.com/en/documents/4012345>.

Value of Data framework observes, data acquisition typically entails substantial fixed costs, with comparatively low marginal costs thereafter. Initial investments such as the procurement of sensors or requisite technological infrastructure must be borne before data collection can commence.²³⁷ Once established, incremental data gathering becomes markedly less expensive.

Expenses related to data processing and upkeep such as data cleansing, storage, and the development of capacities necessary for effective utilization. Moreover, the collection, utilization, and dissemination of data expose entities to reputational harm and financial liability in the event of security breaches.²³⁸ These risks may manifest in forms including, but not limited to, diminished revenue streams and exposure to regulatory or judicial sanctions.

Where an entity elects to augment access to data already acquired, the costs of collection shall be regarded as sunk costs, being expenditures that have been incurred and are unaffected by future decisions. Instead, the entity shall evaluate the marginal costs attributable to data sharing and weigh such costs against the anticipated benefits when determining whether to disclose data that has been collected or is presently being acquired.²³⁹

The following direct costs may be incurred in connection with expanded data access:

- i. Investment in the formulation of a data-sharing strategy;
- ii. Development and maintenance of standards and technological infrastructure facilitating access by third parties;
- iii. Further data processing required to remove personally identifiable or proprietary business information.

²³⁷ The White House, *National Cybersecurity Strategy* (Mar. 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/national-cybersecurity-strategy/>.

²³⁸ Gartner, *The Value of Data in the Digital Economy* 18 (2022).

²³⁹ European Data Protection Board, *Guidelines on Data Breach Notification* 10 (2021), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-data-breach-notification_en.

Such direct costs shall be supplemented by contingent costs, which may include diminished revenue and statutory penalties.²⁴⁰ Specifically, if a data breach occurs, an organisation may incur financial losses, reputational damage, and additional expenses related to remediation or regulatory non-compliance. Furthermore, apprehensions may arise about how data sharing could influence the organisation's competitiveness and position in the market. Accordingly, any decision to share data should be premised upon a balancing of the entity's interests with the public interest, such that disclosure serves both private and societal benefits.²⁴¹

It may prove difficult to identify the manner in which third parties will benefit from access and to structure mechanisms whereby such benefits are equitably transferred to the data-holding entity. As a result, where data flows are likely to generate the greatest public value, they should be prioritized; however, mechanisms should also be established to ensure that entities involved in data gathering and sharing can recoup their costs from the social benefits generated.

Data Value Creation

The stages through which data passes from initial collection to the realization of its economic value are outlined herein.²⁴² This framework underscores the principal challenges faced by both data providers and consumers, as well as the requisite investments and procedural steps essential for extracting value from data. Access constitutes a pivotal factor in determining the worth of data. Empirical evidence indicates that broader access directly correlates with enhanced value extraction.

Market mechanisms have thus far proven inefficient in expanding access to data, owing to misaligned incentives among data owners who often regard data primarily as a tradable commodity.²⁴³ Such commodification may engender adverse societal consequences unless tempered by regulations and governance frameworks that define

²⁴⁰ World Bank, *World Development Report 2021: Data for Better Lives* 35.

²⁴¹ Open Data Institute, *Data Value Creation Framework* 12 (2021), <https://theodi.org/insights/data-value-creation-framework/>.

²⁴² International Data Corporation, *Data Monetization Strategies* 10 (2023), <https://www.idc.com/getdoc.jsp?containerId=US49912423>.

²⁴³ European Commission, *A European Strategy for Data* 12 (2020).

and enforce who may access which data and under what conditions.²⁴⁴ Innovation and active participation from both public and private sectors are imperative to redress ongoing deficiencies in data access, which acts as a catalyst for value creation.²⁴⁵ Moreover, adherence to a structured data value pathway encompassing data collection, stewardship, sharing, utilization, and reuse is advisable. Data stewards will benefit from aligning their activities with such a roadmap in order to enhance both access and value.²⁴⁶ The Open Data Institute’s (ODI) “theory of change” offers an illustrative model of this progression, categorizing data activity into three principal domains: data stewardship, insight generation, and decision-making.

Data stewardship includes gathering, preserving, and disseminating information. Insight creation refers to the process of deriving utility from data, whether through products or services, analyses or insights, or visualizations and narratives. Decision-making involves choosing a course of action after considering diverse information sources, including data, other evidence, and personal expertise. A more granular chain focuses specifically on sequentially mapping the steps through which data value becomes incrementally tangible.

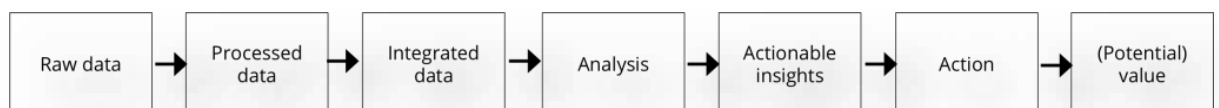


Figure 2.1 Data Value Creation

“Data Steward” or “Data Holder” refers to any natural or legal person who collects, curates, transforms, publishes, or grants access to data in a manner that enhances its value, utility, trustworthiness, or reusability.

Mawer has demonstrated that the intrinsic value of data augments progressively throughout its processing chain, with each interim phase’s value being measured

²⁴⁴ World Economic Forum, *Data Collaboration for the Common Good* 30 (2019).

²⁴⁵ Open Data Institute, *Data Value Creation Framework* 18 (2021).

²⁴⁶ *Id.*

against the potential value realized at the chain's terminus.²⁴⁷ While this chain provides insight into the mechanisms by which data processing, integration, and analysis draw value closer to realization, it omits certain procedural aspects applicable when data is shared or accessed across multiple organizational entities.

By integrating Mawer's methodology with the terminology employed by the ODI, the following critical steps are identified as requisite for extracting value from data when shared or opened publicly:

- i. Data Holders and Stewards: Individuals or entities responsible for transforming raw data into a more usable format, hereinafter "Data Holders" or "Data Stewards", shall ensure that such data attains the status of being trustworthy and amenable to reuse, whether through public dissemination or controlled access within an ecosystem.²⁴⁸
- ii. Mere Accessibility and FAIR Principles: To realize value for the ecosystem as a whole, the Data Holder shall adopt measures to render data findable, accessible, interoperable, and reusable ("FAIR") while also identifying and mitigating risks attendant to data sharing.²⁴⁹
- iii. Data Flows and Ecosystemic Value: Data flows shall be recognized as conduits by which value is created, with such value flowing among diverse sources and consumers. Viewing data through an ecosystemic lens enables articulation of the loci and modalities by which data is utilized to generate value.
- iv. Scope of the Data Ecosystem: The term "data ecosystem" shall encompass any individual or entity that: (a) stewards' data; (b) transforms data into derivative works; (c) makes decisions based upon data; (d) influences any of the foregoing; or (e) is affected by any of the foregoing.²⁵⁰
- v. Access-Dependent Value: As previously asserted, the value of data is contingent upon access. Accordingly, it is imperative to determine both the

²⁴⁷ Chris Mawer, *Data Value Chains: A Framework for Analysis* 15 (2020), <https://www.datavaluemetrics.com/publications/data-value-chains>.

²⁴⁸ Open Data Institute, *Data Value Creation Framework* 28 (2021).

²⁴⁹ FAIR Data Principles, *GO FAIR Initiative*, <https://www.go-fair.org/fair-principles/>.

²⁵⁰ Open Data Institute, *Data Ecosystems Mapping Guide* 10 (2022), <https://theodi.org/insights/data-ecosystems-mapping-guide/>.

means and permitting conditions by which actors may access such value, in order to fully comprehend the attendant processes of value generation.

- vi. **Emphasis on Data Flows.** A holistic, ecosystemic evaluation of data's worth must emphasize data flows as essential mechanisms in the creation of value.

To more effectively promote equitable wealth distribution among stakeholders or to enhance overall value creation within an ecosystem, this approach facilitates a comprehensive understanding of how interactions among various actors yield value. To illuminate the mechanisms by which value is created through data, the ODI has developed a structured methodology and toolset for mapping data ecosystems. Such maps depict data assets, data stewards, and data consumers, together with their respective roles and interconnections within the ecosystem.

While ecosystem mapping is an essential foundational exercise, two supplementary frameworks are proposed to complement this analysis:

- i. **2×2 Matrix Framework:** A tool to classify data use cases at the ecosystem level, emphasizing the balance between aggregate value creation and equitable value distribution among participating organizations or consortia.
- ii. **Value of Data Canvas:** A tabular instrument assisting organizations in evaluating how shared or accessed data may generate value, and by what means such value may be apportioned among stakeholders.²⁵¹

Data use cases involving multiple stakeholders, such as scenarios where one actor provides data and other processes it, or where data is aggregated from several contributors, can yield greater aggregate value. However, these cases introduce complexity due to the requisite coordination and alignment of stakeholder incentives, which may not always converge.

In some instances, the anticipated value may suffice to engage stakeholders without difficulty. In others, value may not be sufficiently distributable to secure the

²⁵¹ Open Data Institute, *Value of Data Canvas 5* (2021), <https://theodi.org/insights/value-of-data-canvas/>.

participation of all relevant actors. In such circumstances, coordinating entities must design redistribution mechanisms to align incentives, potentially reallocating benefits to ensure all parties derive net positive value from their contribution.

A systematic assessment can evaluate whether the projected benefits of a use case outweigh associated costs for each stakeholder, particularly when additional investments are needed in governance, infrastructure, or redistribution mechanisms to ensure incentives align. Absent such an analysis, considering both net value and its distribution across stakeholders, organizations risk overlooking critical determinants of a use case's viability and strategic value.

Organizations or groups of organizations may utilize the proposed simple two-by-two matrix to prioritize use cases at the ecosystem level and use this information to drive decision-making. Use cases are categorized according to whether they have well-distributed benefits and whether they are low-value or high-value. A use case has well-distributed benefits if, with no extra work, most or all stakeholders would be incentivized to participate in its development by the advantages accruing to them. Conversely, use cases where benefits are unevenly dispersed occur when essential stakeholders are unlikely to be adequately motivated by existing incentives, unless explicit measures are taken to address this imbalance.

Benefits of Data Sharing

Data bears considerable economic and strategic importance.²⁵² Accordingly, entities must navigate a complex matrix of data protection statutes to ensure the safeguarding of sensitive information within sharing arrangements.²⁵³

While the exchange of data may yield significant societal and commercial advantages and foster innovation, dissemination concurrently exposes stakeholders to substantial

²⁵² Boston Consulting Group, *The Benefits of Data Sharing Now Outweigh the Risks* 5 (2024), <https://www.bcg.com/publications/2024/the-benefits-of-data-sharing-now-outweigh-the-risks>.

²⁵³ F. Paul Pittman, *US Data Privacy Guide*, White & Case LLP (2024), <https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide>.

risks to individual privacy and data security.²⁵⁴ As F. Paul Pittman emphasizes, to competently navigate the intricate landscape of data protection law, entities must implement comprehensive legal and technical governance frameworks designed to maintain the privacy and reliability of sensitive data collections.²⁵⁵

- i. Due Diligence and Security Protocols-Data-sharing instruments must mandate thorough due diligence regarding prospective recipients. Such evaluations must assess the adequacy and efficacy of recipients' security controls and confirm compliance with all applicable statutory and regulatory regimes, including but not limited to the "*General Data Protection Regulation (GDPR)*" and the "*Health Insurance Portability and Accountability Act (HIPAA)*."²⁵⁶
- ii. Anonymization and Pseudonymization-Organizations are required to implement rigorous anonymization procedures to remove personally identifiable information before data transfer, thereby reducing the risk of re-identification. Concurrently, pseudonymization, where direct identifiers are replaced with artificial tokens or codes, enhances privacy protection while preserving dataset utility for analytical purposes.²⁵⁷
- iii. Encryption and Access Controls- Organisations are required to implement strong encryption measures to secure data during transmission as well as while it is stored. These should be supplemented with granular access controls enforcing the principle of least privilege, thereby mitigating the risk of unauthorized access or data breaches.²⁵⁸

²⁵⁴ Global Partnership for Sustainable Development Data, *Effective and Ethical Data Sharing at Scale* 10 (2023), <https://www.data4sdgs.org/effective-and-ethical-data-sharing-scale>.

²⁵⁵ F. Paul Pittman, *Data Protection Laws and Regulations Report 2024 USA*, ICLG 15 (2024), <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa/amp>.

²⁵⁶ U.K. Info. Comm'r's Off. (ICO), **Data Sharing: A Code of Practice** (2023), <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/>.

²⁵⁷ Information Commissioner's Office, 9. *Data Sharing* (2023), <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/9-data-sharing/>.

²⁵⁸ Eur. Data Prot. Bd. (EDPB), **Guidelines 2/2023 on Transfers of Personal Data under Chapter V GDPR** (2023), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-data-transfers_en.

- iv. Auditing and Monitoring-Continuous audit and monitoring systems are essential to detect irregular or suspicious access patterns, facilitating prompt investigation and remediation in cases of data misuse or security incidents.²⁵⁹

Compliance with Cross-Border Data Transfer Requirements

The international transfer of data has become foundational to global commerce. However, such transfers introduce additional layers of legal and operational complexity.²⁶⁰ Entities must adopt multi-jurisdictional compliance frameworks that encompass the following:

- i. Jurisdictional Analysis-Entities must conduct comprehensive legal analysis of data protection obligations in both source and destination jurisdictions to preclude violations and ensure lawful transfers.²⁶¹
- ii. Protective Measures-Given the sensitivity of transferred data, organizations must employ advanced protective measures, including end-to-end encryption, secure cloud storage, pseudonymization, and stringent access control mechanisms, to ensure the privacy and reliability of data during transmission and storage.
- iii. Informed Consent-Prior to transferring personal or sensitive data across national boundaries, entities must secure explicit, informed consent from data subjects. This promotes transparency, accountability, and trust among stakeholders.²⁶²
- iv. Data Transfer Agreements-Formalized agreements must clearly define (i) the purpose, scope, and duration of data sharing; (ii) applicable regulatory obligations; (iii) requisite privacy and data security safeguards; and (iv) dispute resolution and liability provisions. Such agreements must also incorporate

²⁵⁹ Prevalent, *Third-Party Data Sharing: Key Regulations & Best Practices* (2025), <https://www.prevalent.net/blog/third-party-data-sharing-compliance/>.

²⁶⁰ Wiley, *New DOJ Restrictions on Cross-Border Data Transactions Take Effect April 8* (2025), <https://www.wiley.law/alert-New-DOJ-Restrictions-on-Cross-Border-Data-Transactions-Take-Effect-April-8>.

²⁶¹ Eur. Data Prot. Supervisor (EDPS), *Guidelines on International Data Transfers and Adequacy Decisions* (2022), https://edps.europa.eu/data-protection/international-transfers_en.

²⁶² Securiti, *Cross-Border Data Transfer Requirements: Global Privacy Laws* (2025), <https://securiti.ai/whitepapers/cross-border-data-transfer-requirements/>.

compliance with relevant legal frameworks governing international data transfers.

2.4 Laws and Governance of Data: Global and Indian Perspectives

Data laws and data governance work together to ensure that information is managed legally, securely, and effectively. Legislative instruments governing data, including the GDPR in the European Union, the CCPA in California, India's Digital Personal Data Protection Act, 2023, as well as HIPAA and GLBA in the United States, and others, establish legal rules for collecting, processing, transferring, and deleting personal data.²⁶³ They grant individuals rights such as access, correction, and erasure, and impose obligations on organizations, including breach notification, security measures, transparency, and accountability.

Data governance, on the other hand, is the internal framework within organizations comprising policies, roles (like data stewards and data protection officers), procedures, and technical controls that ensure data is accurate, consistent, secure, accessible, and used responsibly across its lifecycle. It encompasses standards for classification, retention, lineage, access controls, quality, and breach response. By aligning internal data governance with external legal requirements, organizations can both comply with regulations and derive maximum value from their data, building trust through transparency, minimizing risk, and enabling informed, ethical decision-making.

Global Perspective

At the international level, the “*European Union's General Data Protection Regulation (GDPR)*” represents one of the most comprehensive and influential legal instruments for safeguarding personal information.²⁶⁴ Adopted in 2016 and enforced from May 25, 2018, it sets out a detailed framework grounded in key principles, including lawfulness, fairness and transparency in processing, purpose limitation that ensures data is used only for clearly defined objectives, data minimization which restricts

²⁶³ DATAVERSITY, *Data Governance Trends in 2025* (2024), <https://www.dataversity.net/data-governance-trends-in-2025/>.

²⁶⁴ Org. for Econ. Co-operation & Dev. (OECD), *Data Governance for Growth and Well-Being: Policy Framework* (2022), <https://www.oecd.org/digital/>.

collection to what is necessary, accuracy, storage limitation, integrity and confidentiality, and accountability.²⁶⁵

The GDPR grants individuals extensive rights such as the right to access their personal data, to correct inaccuracies, to request deletion under the right to be forgotten, and to transfer their data through the right to data portability. Organizations that act as data controllers or processors are required to incorporate privacy by design and by default, maintain comprehensive records of processing activities, report breaches to authorities and affected individuals, and in specific cases, appoint a “Data Protection Officer (DPO)”.²⁶⁶

In contrast, the United States does not have a single federal law governing data privacy. Instead, it follows a sectoral and fragmented model where individual industries are regulated by specific statutes. For instance, the “*Health Insurance Portability and Accountability Act (HIPAA)*” govern health information, while state-level laws such as the “*California Consumer Privacy Act (CCPA)*” grant consumers rights related to accessing, deleting, and opting out of the sale of their personal data.²⁶⁷ Although these laws have prompted major shifts in corporate privacy practices and inspired other jurisdictions, the absence of a unified federal framework results in uneven and inconsistent data protection standards across the country.

Other nations have begun aligning with international standards by modernizing and strengthening their own privacy regimes. Countries including Japan, Canada, and Australia have enacted or updated data protection legislation reflecting GDPR principles, emphasizing transparency, limited collection and usage, valid legal bases for processing, and user rights. This reflects a global convergence toward norms, inspired by the GDPR model.

Furthermore, international bodies play a critical role in shaping data governance standards. The “*Organization for Economic Co-operation and Development (OECD)*”

²⁶⁵ World Bank, World Development Report 2021: Data for Better Lives (2021), <https://www.worldbank.org/en/publication/wdr2021>

²⁶⁶ MyGov, Draft Digital Personal Data Protection Rules, 2025.

²⁶⁷ Economic Laws Practice, *Data Privacy & Protection: Update January 2025* (2025), <https://elplaw.in/wp-content/uploads/2025/01/Key-Highlights-of-the-DPDP-Rules-2025-1.pdf>.

has developed comprehensive guiding principle promoting responsible data stewardship, enabling trusted cross-border data flows, and supporting cooperative enforcement.²⁶⁸ The United Nations similarly supports national-level frameworks, emphasizing accountability, effectiveness, and inclusiveness in data management.²⁶⁹ Meanwhile, the World Trade Organization’s e-commerce negotiations highlight the significance of harmonized data governance for facilitating global digital trade. These discussions reinforce how consistent and interoperable data regulations are central to supporting both trade and consumer trust.

Areas in Global Data Governance

i. Privacy Principles and Data Subject Rights

Jurisdictions worldwide increasingly embed principles such as transparency, purpose limitation, and minimization into their legal systems, along with user rights like access, correction, deletion, and portability.²⁷⁰

ii. Cross-Border Data Flow and Trade Infrastructure

Frameworks such as the OECD’s “data free flow with trust” and various digital trade agreements aim to reconcile open data markets with the need for regulatory consistency and user protection.²⁷¹

iii. Sectoral versus Comprehensive Regulation

Some countries adopt broad data protection regimes, while others, like the U.S., follow a sector-specific path.²⁷² This diversity can complicate compliance for global organizations.

²⁶⁸ Outlook Business, *India’s Data Protection Act 2023: What the 2025 Draft Rules Mean for Digital Evolution* (2025), <https://www.outlookbusiness.com/columns/dpdpa-a-latent-dilemma>.

²⁶⁹ PRS India, *Revised Draft Non-Personal Data Governance Framework* (2025), <https://prsindia.org/policy/report-summaries/revised-draft-non-personal-data-governance-framework>.

²⁷⁰ MyGov, *Share Your Inputs on Draft Non-Personal Data Governance Framework* (2025), <https://www.mygov.in/task/share-your-inputs-draft-non-personal-data-governance-framework/>.

²⁷¹ Lexology, *Brief Analysis of Non-Personal Data Governance Framework in India* (2020), <https://www.lexology.com/library/detail.aspx?g=259584ff-fb42-4d02-8ddf-9cf8c0925d34>.

²⁷² Drishti IAS, *Recalibrating Non Personal Data* (2025), <https://www.drishtias.com/daily-updates/daily-news-editorials/recalibrating-non-personal-data>.

iv. Accountability, Enforcement, and Cooperation

GDPR's accountability requirement has driven the adoption of data protection impact assessments, structured documentation, breach reporting, and regulatory supervision. Institutions like the OECD support international cooperation in enforcement.²⁷³

v. Incentives for Data Sharing and Trust Frameworks

These initiatives encourage collaborative data ecosystems, balancing openness with privacy through shared governance, standards for data intermediaries, and multi-party data trusts. Bilateral and multilateral digital partnership agreements further these aims by aligning legal regimes and establishing trust principles.

Challenges and Trade-Offs

- i. Regulatory fragmentation: Despite increasing alignment, discrepancies remain in areas like data localization mandates (e.g., in China), transfer restrictions, (such as under GDPR), and sector-specific limitations.²⁷⁴
- ii. Balancing privacy, innovation, and sovereignty: Nations must navigate tensions between protecting individual rights and fostering innovation, as well as maintaining national policy autonomy.
- iii. Implementation in developing countries: Many jurisdictions face capacity constraints that hinder effective adoption and enforcement of modern data governance frameworks.
- iv. Emerging technology considerations: Advances in fields such as artificial intelligence, emerging technologies such as the Internet of Things and big data demand new approaches to address algorithmic transparency, group privacy, and accountable risk management.

²⁷³ Hogan Lovells, *New DOJ Rule Limits Cross-Border Data Transfers to Protect National Security* (2025).

²⁷⁴ TrustArc, *Cross-Border Data Transfers in 2025: Regulatory Changes, AI Risks, and Operationalization* (2025).

Indian Perspective

The issue of data privacy has become a paramount concern worldwide in this age characterized by digital transformation. India's advancing digital economy has acknowledged the necessity for thorough legislation to protect personal data. The culmination of this endeavor over the last seven years, and after multiple iterations, the "Digital Personal Data Protection Act, 2023 (DPDP Act)" represents a major milestone in India's effort to protect the data privacy rights of its citizens.²⁷⁵

The evolution of India's legal framework on privacy has been both gradual and significant. For a long time, the country did not have a dedicated statute governing personal data protection. The handling of personal information was largely governed by the "Information Technology Act, 2000," which provided a general regulatory basis for data management.²⁷⁶ Supplementary provisions contained in other laws, including the "Indian Penal Code, 1860," addressed certain aspects of privacy but did not constitute a comprehensive regime.²⁷⁷

A turning point occurred with the Supreme Court of India's decision in "*K.S. Puttaswamy v. Union of India (2017) 10 SCC 1*", where the Court affirmed that the right to privacy is an intrinsic component of the fundamental rights guaranteed under the Constitution.²⁷⁸ This landmark judgment laid the foundation for the development of a robust and rights-based data protection framework in India. This facilitated the passage of the "DPDP Act" following extensive discussions and revisions by the Government, bringing India in line with global benchmarks and notably aligning with the "European Union's GDPR".²⁷⁹

The "DPDP Act" includes a range of provisions designed to safeguard digital personal data, featuring strict penalties for non-compliance and establishing rights for

²⁷⁵ DATAVERSITY, *Data Governance Trends in 2025* (2024).

²⁷⁶ Kellton, *Top Data Governance Frameworks in 2025* (2025).

²⁷⁷ Nat'l Inst. of Standards & Tech. (NIST), NIST Privacy Framework: Version 1.1 (2020), <https://www.nist.gov/privacy-framework>.

²⁷⁸ United Nations Conf. on Trade & Dev. (UNCTAD), Digital Economy Report 2021: Cross-Border Data Flows and Development (2021), https://unctad.org/system/files/official-document/der2021_en.pdf.

²⁷⁹ Org. for Econ. Co-operation & Dev. (OECD), Data Governance for Growth and Well-Being: Policy Framework (2022), <https://www.oecd.org/digital/>.

individuals to obtain, modify, and delete their personal information.²⁸⁰ Notably, the “DPDP Act” exhibits similarities with GDPR, including the requirements to secure explicit consent, deliver privacy notices, report data breaches, and uphold individual data privacy rights. These rights encompass access, correction, deletion, redress, and opting out, as well as the necessity to engage in contracts with processors and restrict the limiting the storage of personal information to what is strictly required.

Local companies as well as organizations that may not be fully versed in the GDPR or other privacy regulations must take the initiative to understand the new privacy law in India.²⁸¹ It is imperative that they comply with and implement the stipulated provisions, establish systems to document the explicit consent of data subjects, maintain a comprehensive privacy policy and statement, and integrate a grievance redressal mechanism to address privacy-related complaints, among other requirements.

An important aspect of the DPDP Act is its focus regarding the safeguarding of minors’ personal information, reflecting a dedication to safeguarding vulnerable populations. The DPDP Act creates a regulatory structure for data fiduciaries concerning the management of personal information, pertaining to minors. The term “children” refers to individuals who have not yet reached the age of 18 years, thus categorizing them as minors.²⁸² Data fiduciaries are prohibited from engaging in any processing of children’s data that may have a detrimental impact on the child’s well-being.²⁸³ Therefore, it is incumbent upon the data fiduciary to ensure the proper management and mitigation concerning the potential harms arising from the utilization of minors’ digital data footprints.²⁸⁴

India also recognizes the importance of *Non-Personal Data* governance for fostering innovation and economic growth. The Government’s *Non-Personal Data* Governance Framework aims to create policies governing the collection, dissemination, and

²⁸⁰ World Econ. Forum, Data Collaboration for the Common Good: Enabling Trust and Innovation (2019), <https://www.weforum.org/reports/data-collaboration-for-the-common-good/>.

²⁸¹ Data Prot. Auth. of India (DPAI), *Handbook on Compliance with the Digital Personal Data Protection Act, 2023* (2025), <https://dpdp.gov.in/>.

²⁸² *Id.*

²⁸³ Law.asia, *India’s Draft Data Protection Rules* (2025).

²⁸⁴ Economic Laws Practice, *Data Privacy & Protection: Update January 2025* (2025).

utilization of *Non-Personal Data* by public as well as private entities while ensuring sovereignty, privacy, and equitable benefit-sharing.

Besides these, other laws such as the “Information Technology Act 2000” and sector-specific the rules deal with issues related to cybercrime, electronic authentication, and digital governance.²⁸⁵ Various government initiatives, such as India Stack, provide the digital infrastructure to securely manage data flows while respecting privacy and security norms.²⁸⁶

2.5 Various Types of Data

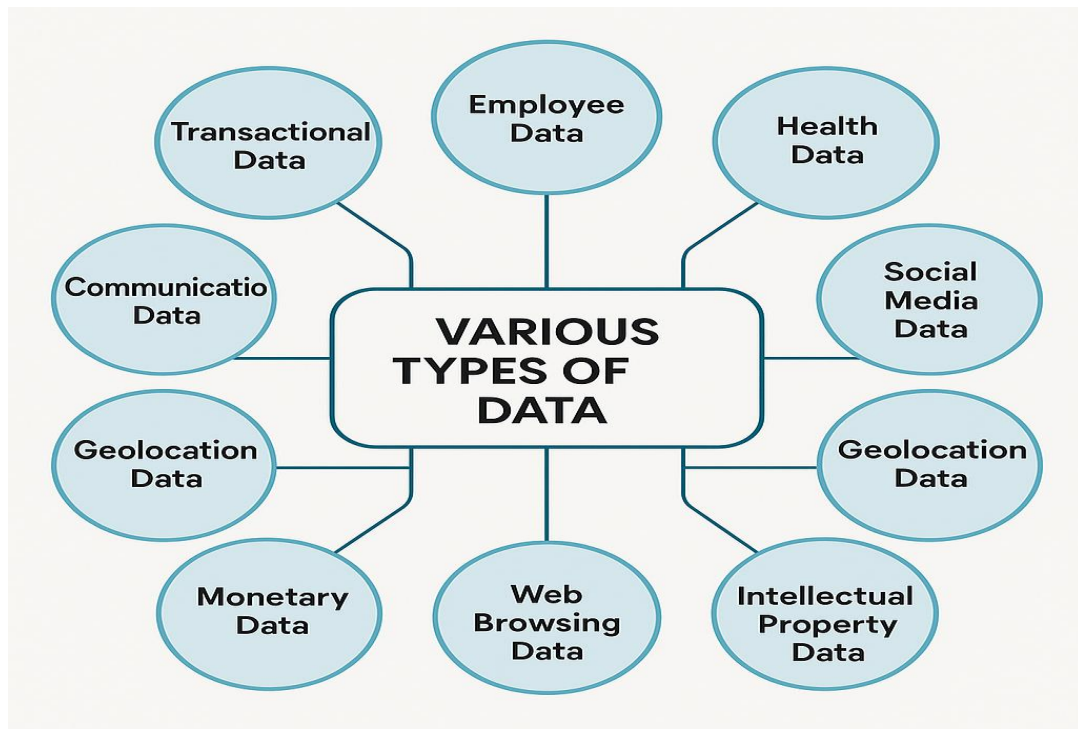


Figure 2.2 Various types of Data

²⁸⁵ Outlook Business, *India's Data Protection Act 2023: What the 2025 Draft Rules Mean for Digital Evolution* (2025).

²⁸⁶ *Id.*

Transactional Data

“Transactional data” refers to all records generated in the course of commercial or financial transactions, including: financial debits and credits, inventory movements, pricing details of goods or services, methods of payment used, applied discounts, and any associated quantifiable metrics or descriptors.²⁸⁷

i. BharatPay Data Breach (August 2022)

In August 2022, a cybersecurity incident occurred in BharatPay’s backend systems, resulting in unauthorized disclosure of the personal and transactional records of approximately 37,000 users.²⁸⁸ Exposed data included usernames, cryptographically hashed passwords, mobile telephone numbers, UPI identification numbers, email addresses, bank balances, and associated transaction logs spanning from February 2018 through August 2022.

ii. Yahoo Data Breaches (2013 & 2014)

Yahoo, as an operator of internet-based communications services, suffered two recorded security breaches.²⁸⁹ The first, in 2013, compromised approximately 500 million user accounts; the second, discovered in 2014, affected over one billion accounts. The exposed data comprised user authentication credentials and personally identifiable information.

iii. Equifax Third-Party Data Breach (2017)

In 2017, Equifax, acting as a consumer credit reporting agency, experienced a data breach through third-party system vulnerabilities which resulted in the exfiltration of personal data pertaining to approximately 147 million individuals.²⁹⁰ Compromised

²⁸⁷ TIBCO, *What is Transactional Data?*, <https://www.tibco.com/glossary/what-is-transactional-data>.

²⁸⁸ ETCISO, *BharatPay Data Breach: Personal Data, Transaction Details of 37,000 Users Leaked Online*, <https://ciso.economictimes.indiatimes.com/news/bharatpay-finance-services-breached-personal-data-transaction-details-of-37000-users-leaked-online/93586873>.

²⁸⁹ *In re Yahoo! Inc. Customer Data Security Breach Litigation*, No. 16-MD-02752 (N.D. Cal. 2019) (settlement agreement).

²⁹⁰ FTC, *Equifax Data Breach Settlement*, <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>.

records included Social Security numbers, dates of birth, physical addresses, driver's license and DMV records, and, in some cases, payment card details.

Equifax entered into a global agreement reached with the Federal Trade Commission, the Consumer Financial Protection Bureau, and authorities representing fifty U.S. states and territories, agreeing to monetary disposition of at least USD 575 million, potentially escalating to USD 700 million, including:

- i. USD 300 million allocated to consumer relief funds, subject to augmentation of USD 125 million if necessary;
- ii. USD 175 million remitted to state and territorial authorities; and
- iii. USD 100 million in civil penalties paid to the CFPB.

Legal Implications

These events underscore corporate and regulatory obligations to implement and maintain comprehensive data security protocols.²⁹¹ Entities handling transactional entities handling data have an obligation to exercise due care in ensuring its protection from unauthorized access, loss, or theft, in compliance with prevailing privacy statutes and industry standards. Failure to do so may result in administrative penalties, statutory damages, civil liability, and legally binding remediation measures as evidenced in the Equifax settlement regime.

Employee Data

“Employee database” means a secured, computerized repository maintained by the Employer or its authorized agents for the purpose of managing and administering employment-related information.²⁹² This database shall include, including:

- i. Personal Identification Data: including full legal name, current contact details, and Social Security Number or other government-issued identification numbers;

²⁹¹ Federal Trade Commission (FTC), *Equifax Data Breach Settlement*, <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement/>.

²⁹² Jackson Lewis, *California Consumer Privacy Act: FAQs for Employers*, <https://www.jacksonlewis.com/insights/california-consumer-privacy-act-faqs-employers>.

- ii. Employment and Compensation Records: such as employment title, dates of hire and termination, salary or wage information, payroll history, benefits enrollment data, tax withholding details, and related compensation documentation;
- iii. Performance and Disciplinary Data: including but not limited to performance reviews, disciplinary records, improvement plans, and any associated notes, evaluations, or resolutions;
- iv. Benefit and Leave Records: encompassing health insurance, retirement plan participation, leave requests or approvals (such as annual, sick, medical, or parental leave), and other applicable benefit-related documentation.

Access to, use of, and disclosure of information from the employee database shall be strictly governed by applicable laws, regulations, and company policies concerning confidentiality, data privacy, retention, and permissible access. The employer is required to adopt suitable administrative, physical, and technological measures to preserve the security and integrity of the data. The employer shall maintain data retention schedules in compliance with statutory and business requirements. It must also ensure that any transfer or disclosure of database contents is conducted only pursuant to valid legal process, employee consent where required, or pursuant to legitimate business necessity permitted under law.

Health Data

“Health data” shall mean any and all information, in any form or medium, that pertains to the physical or mental well-being of a natural person who is either identified or can be identified.²⁹³ This encompasses:

- i. Details relating to an individual’s physical or mental health, whether pertaining to past, current, or future conditions;
- ii. Records of healthcare services or treatment provided to the individual;

²⁹³ Taylor Wessing, *Defining and Using Health Data*, <https://www.taylorwessing.com/en/global-data-hub/2022/march---health-data---getting-the-right-balance-between-innovation-and-data-protection/defining-and-using-health-data>.

- iii. Diagnostic findings and test results;
- iv. Treatment plans and prescriptions;
- v. Insurance, billing and payment information related to healthcare services;
- vi. Demographic data associated with any of the foregoing; and
- vii. Information identifying healthcare providers involved in the delivery of care.

Such data shall be considered “special category personal data” under applicable law. It shall remain subject to all rights afforded to the data subject, which include, but are not limited to, the rights of access, rectification, deletion, portability, and objection, together with all corresponding obligations placed upon data controllers and processors, including lawful processing, data minimization, retention limitation, integrity and confidentiality safeguards, and breach notification.

Social Media Data

“Social media data” shall be construed to mean all information and metrics derived from analytics tools maintained by “*social networking platforms*”, including platforms including platforms like Facebook, Twitter, Instagram, and LinkedIn.²⁹⁴ These data encompass, inter alia, blog entries, user-generated posts, expressed affiliations (e.g., “likes,” following relationships), click-through rates, shares (including retweets and reposts), comments, and quantified engagement indices.

Case Applications

- i. Aarushi Talwar Matter

Social media data pertaining to the “Aarushi Talwar” criminal investigation consists of the aggregate of public discussions, conjectures, and speculative content disseminated via online platforms.²⁹⁵ This data may be used to analyze the scope and

²⁹⁴ NCSU Libraries, *Legal and Ethical Implications | Social Media Archives Toolkit*, <https://www.lib.ncsu.edu/social-media-archives-toolkit/legal>.

²⁹⁵ BBC News, *Was Aarushi Talwar Murder Verdict a Miscarriage of Justice?*, <https://www.bbc.com/news/world-asia-india-33546471>.

tenor of public sentiment and commentary, subject to admissibility rules concerning hearsay, relevance, and probative value.

ii. Asaram Bapu Proceeding

Social media contributions relating to the Asaram Bapu legal proceedings include public commentary, shared media, and digital discourse concerning both the allegations and the accused.²⁹⁶ Such data may be used as permissible evidence of public opinion trends, community perception, reputational impact, or bias, consistent with evidentiary standards and privacy regulations.

Communication Data

“Communication Data” means any data generated, transmitted, received, stored, or otherwise processed in respect of a digital communication, excluding the actual message or material conveyed through the communication.²⁹⁷ This includes, without limitation:

- i. Entity Data – data identifying users, devices, or accounts that participate in the communication (e.g., telephone numbers; email addresses; user or account identifiers; device identifiers such as IP addresses, IMSI, IMEI);
- ii. Event Data – data recording transactional aspects of the communication, such as timestamps (date, time, duration), routing information, network session details, service type (e.g., email, instant message, VoIP, social media post), volume or size of data transferred, originating and terminating endpoints;
- iii. Location Data – information concerning the geographical location of the device or user when the communication was made or received, including geolocation data derived from IP addresses or mobile devices.

Geolocation Data

“Geolocation Data” means any information, derived from or generated by devices such as mobile telephones, in-vehicle systems, wearable technology, Wi-Fi access points, cellular base stations, or via Internet Protocol addresses, that identifies the physical

²⁹⁶ *Asaram Bapu v. State of Rajasthan*, (2022) 2 S.C.C. 579; AIR 2022 SC 1234 (India).

²⁹⁷ EPIC, *Electronic Communications Privacy Act (ECPA)*, <https://epic.org/ecpa/>.

location of a device or its user with reasonable specificity.²⁹⁸ Such data typically comprises geographic coordinates, latitude and longitude, or other locational descriptors that enable the determination of a device's real-time or historical position.

The collection, processing, utilization, retention, disclosure, and transfer of Geolocation Data shall be undertaken only within the limits permitted by applicable data protection legislation. Such processing must rely on the informed, specific, and voluntary consent of the data subject or, where required by law, on a valid legal foundation such as a court directive or warrant.

In addition, organizations managing Geolocation Data are required to adopt suitable technical and organizational safeguards to preserve its confidentiality, integrity, and lawful use. They must also ensure that data subjects are able to exercise their rights of access, rectification, erasure, withdrawal of consent, and data portability, as prescribed under the relevant data protection frameworks.

Monetary Data

Monetary data means all information, records, and statistics relating to monetary aggregates, financial transactions, and central bank operations, including but not limited to data on currency in circulation, reserves, deposit and lending interest rates, repurchase agreements, and other money market instruments.²⁹⁹ Such data shall include reports submitted by financial institutions pursuant to regulatory or statutory obligations established under applicable law or regulation (e.g., central bank directives, monetary policy statutes, or financial market regulations), and shall be compiled, maintained, and disclosed in accordance with legally mandated standards governing accuracy, timeliness, confidentiality, and public availability.

Financial institutions and reporting agents shall, as required by law, collect and furnish monetary data to designated monetary authorities, in formats and within timeframes prescribed by law. These obligations serve purposes that include, but are not limited

²⁹⁸ Focal Point, *How to Navigate Geolocation and Data Protection Laws*, <https://blog.focal-point.com/how-to-navigate-geolocation-and-data-protection-laws>.

²⁹⁹ IMF, *Monetary Policy and Central Banking*, <https://www.imf.org/en/About/Factsheets/Sheets/2023/monetary-policy-and-central-banking>.

to, the design and execution of monetary policy, the oversight of the financial sector, and the release of consolidated statistical data.

The processing and dissemination of monetary data shall at all times comply with applicable legal requirements concerning data protection, official secrecy, and statistical confidentiality, and shall be subject to enforcement mechanisms, penalties, or sanctions as provided by law.

Web Browsing Data

Web Browsing Data means any information recorded by a user's interaction with web browsers or internet services, including but not limited to Uniform Resource Locators (URLs) visited, IP addresses, cookie identifiers, referrer URLs, click-stream logs, web-bug access timestamps, browsing session duration, and device or browser metadata.³⁰⁰ Such information may qualify as personal data when it identifies an individual either directly or indirectly, or when identification becomes possible through its combination with other datasets, for instance, an IP address or cookie identifier as recognized under the GDPR definition of "online identifiers" or "personal data."

Data controllers, internet service providers, and third parties that collect, process, store, or disclose Web Browsing Data must do so in strict compliance with applicable legal regimes such as the EU's GDPR, US privacy/state laws like California's CCPA, and "India's Digital Personal Data Protection Act, 2023". These laws generally require:

- i. Lawful basis and informed consent are required, especially for non-essential tracking technologies such as cookies or pixels, aligned with regulations like the ePrivacy Directive and Directive 2002/58/EC requiring informed, prior consent.
- ii. Transparency & notice: Include clear communication of categories of data collected, purpose of processing, data recipients, retention periods, and users' rights (e.g., access, deletion, objection).

³⁰⁰ GDPR.eu, *Cookies, the GDPR, and the ePrivacy Directive*, <https://gdpr.eu/cookies/>.

- iii. Data minimization, storage limitation, and security: Ensuring that only essential web browsing information is collected, stored for no longer than the duration necessary to achieve the specified purpose, and safeguarded against unauthorized access or data breaches.
- iv. Individual rights and controls: Enabling users to access their own browsing data, request correction or deletion, object to processing (such as profiling), and opt out of data sales or tracking, with mechanisms to facilitate withdrawal of consent (e.g., browser settings).
- v. Restrictions on third-party sharing or sale: Prohibiting disclosure or monetization without explicit legal authority or user consent (as in CCPA and FTC actions banning sale of non-anonymized web browsing history).
- vi. Judicial or regulatory oversight of surveillance, including court-ordered authorizations under acts like the U.S. Wiretap Act, when public authorities seek access to users' URL histories or browsing communications.

Enforcement mechanisms vary by jurisdiction and may include regulatory audits, administrative fines (up to billions in some regimes), civil liability, and criminal sanctions. Courts in some regions have recognized web history tracking as constitutionally protectable content, requiring heightened legal thresholds for access.

Intellectual Property Data

Intellectual Property (“IP”) law safeguards the tangible and intangible outcomes of human creativity and innovation- including inventions, literary and artistic works, industrial designs, trademarks, geographical indications, and confidential business information, by bestowing upon rights holders’ exclusive legal authority to exploit, prevent unauthorized use, and derive economic benefit from their creations under statutory frameworks.³⁰¹

For instance, in *Bayer Corporation v. Union of India*, India’s judiciary confirmed that when a patent holder fails to make a medicine reasonably affordable and accessible

³⁰¹ WIPO, *What is Intellectual Property (IP)?*, <https://www.wipo.int/about-ip/en>.

within the country, a compulsory license may be granted to ensure public welfare, thereby balancing monopolistic rights against public health needs.³⁰² In “*Diamond v. Chakrabarty*”, the U.S. “Supreme Court” held that genetically engineered microorganisms qualify as patentable subject matter under patent statutes, establishing that life forms created by human ingenuity are eligible for protection.³⁰³

Other notable disputes, such as ongoing litigation between Apple and Samsung, underscore the multifaceted nature of IP enforcement, spanning design patents, utility patents, and trade dress in consumer electronics.³⁰⁴ Additionally, the litigation between *YouTube* and *Throughcom* highlights the responsibilities of online platforms in managing user-generated content to avoid copyright infringement.³⁰⁵

IP rights are classified as follows:

- i. Patents grant inventors a time-limited exclusive right, typically twenty years, to exploit novel, non-obvious, and industrially applicable inventions, including genetically modified entities.
- ii. Copyrights protect original works of authorship, such as literary texts, audiovisual content, software, and art, by vesting creators with exclusive rights of reproduction, distribution, adaptation, public display, and performance during the creator’s lifetime plus a posthumous term.
- iii. Trademarks secure distinctive signs, names, logos, or slogans used to indicate commercial origin and prevent consumer confusion.
- iv. Industrial designs protect the aesthetic and ornamental aspects of products, including shape, pattern, and color.

³⁰² UNCTAD, *Bayer Corporation Vs. Union of India and Others (Bayer v. Natco)*, <https://unctad.org/ipcaselaw/sites/default/files/ipcaselaw/2020-12/Bayer%20Corporation%20Vs.%20India%20and%20Others%20IPAB%202013.pdf>.

³⁰³ *Diamond v. Chakrabarty*, 447 U.S. 303 (1980).

³⁰⁴ *Apple Inc. v. Samsung Elecs. Co.*, 786 F.3d 983 (Fed. Cir. 2015), <https://cafc.uscourts.gov/sites/default/files/opinions-orders/14-1335.Opinion.5-18-2015.1.PDF>.

³⁰⁵ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012), https://www.ca2.uscourts.gov/decisions/isysquery/9c4b4d4e-4a4a-4e4b-8b4a-4e4b8b4a4e4b/1/doc/10-3270_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/9c4b4d4e-4a4a-4e4b-8b4a-4e4b8b4a4e4b/1/hilite/.

- v. Geographical indications identify goods originating from specific regions whose quality or reputation is attributable to their geographic origin.
- vi. Trade secrets protect confidential business and technical information that derives value from being kept secret and is subject to reasonable measures to preserve confidentiality.

Indian Framework

- i. The Copyright Act, 1957

The Copyright Act serves to amend and consolidate the law governing copyright and related matters.³⁰⁶ It grants exclusive rights to authors and other eligible persons over original literary, dramatic, musical, and artistic creations, including cinematograph films and sound recordings. These rights encompass reproduction, translation, adaptation, distribution, public performance, and communication to the public.

Copyright protection endures for the lifetime of the author and continues for sixty years from the first day of January following the year of their death. The Act also acknowledges moral rights, which include the right of attribution and the right to prevent or seek damages for any derogatory treatment of the work. In cases of infringement, available remedies include injunctions, monetary compensation or an account of profits, as well as both civil and criminal penalties.

- ii. The Patents Act, 1970

The Patents Act is legislation enacted to amend and consolidate the law governing patents.³⁰⁷ It accords inventors exclusive rights over patentable inventions, which are defined as novel products or processes involving an inventive step and capable of industrial application. The Act empowers the patent holder to prohibit others from making, using, offering for sale, selling, or importing the patented invention without proper authorization. A patent is valid for twenty years from the date of filing the complete specification. The Act further specifies non-patentable inventions, such as mere discoveries, abstract theories, methods of agriculture or treatment of humans or

³⁰⁶ The Copyright Act, 1957.

³⁰⁷ The Patents Act, 1970.

animals, and trivial improvements. It governs the application process, publication, examination, opposition, grant, revocation, compulsory licensing, and working of patents.

iii. The Trade Marks Act, 1999

The Trade Marks Act was enacted to provide for the registration and enhanced protection of trade marks pertaining to goods and services, and to amend and consolidate the existing law relating to such matters.³⁰⁸ A ‘trademark’ is defined as any mark capable of graphical representation and distinguishing one person's goods or services from those of others. Registration confers exclusive rights upon the proprietor to use the mark and to prevent unauthorized use, including infringement and passing off. The term of registration is ten years, renewable indefinitely. The Act provides mechanisms for application, examination, opposition, registration, renewal, rectification, assignment, licensing, and legal recourse for infringement, including penalties for counterfeiting and fraudulent use, and recognizes the concept of well-known and service marks.

iv. The Designs Act, 2000

The Designs Act was enacted to consolidate and amend the law governing the registration and enhanced protection of industrial designs.³⁰⁹ It protects new or original designs applied to any article by any industrial process, covering shape, configuration, pattern, or ornamentation, or composition of lines or colors that appeal to the eye. Registration is governed by a ‘first-to-file’ rule and confers exclusive rights for ten years from the date of registration, renewable for five additional years. The Act prescribes procedures for application, examination, post-registration corrections, cancellation, and civil remedies against infringement.

³⁰⁸ The Trade Marks Act, 1999.

³⁰⁹ The Designs Act, 2000.

v. The Geographical Indications of Goods (Registration and Protection) Act, 1999

An Act to provide for the registration and better protection of geographical indications relating to goods.³¹⁰ A ‘geographical indication’ is defined as a sign identifying goods as originating from a specific territory, region, or locality where a specific quality, reputation, or feature is fundamentally linked to the geographical area of origin. The Act provides for application, examination, registration, opposition, renewal, and certified users. Registration lasts ten years from the date of registration, renewable indefinitely. It grants exclusive rights to registered proprietors and authorized users and prescribes criminal penalties-including imprisonment and fines, for false application of or misuse of a GI, with increased penalties for repeat offences.

vi. Information Technology Act, 2000

Notwithstanding anything contained in the Copyright Act, 1957, any individual shall be deemed to have committed cyber infringement of intellectual property rights if such person:

- a) Illegally accesses or obtains access to any computer resource with the intent to infringe copyright; or
- b) Downloads, copies, transmits, shares, or otherwise makes use of any copyrighted work in electronic form without valid authorization.³¹¹

Penalties:

This offence shall be punishable with imprisonment for a term extending up to three years, or with a fine up to ₹500,000, or with both, as provided under Section 66 (computer-related offences) and Section 66B (receipt of stolen computer resources) of the Information Technology Act, 2000.

³¹⁰ The Geographical Indications of Goods (Registration and Protection) Act, 1999.

³¹¹ The Information Technology Act, 2000.

In addition to criminal liability, the affected copyright holder shall be entitled to claim damages up to ₹10,000,000 pursuant to Section 43 (penalty for damage to computer systems) and Section 43A (compensation for failure to protect data), as applicable.

Aggravated Offences:

Where the infringement involves:

a) Alteration or tampering with computer source code, thereby breaching copyright protection or Digital Rights Management (DRM) mechanisms, which is punishable under Section 65; or

b) Publication or electronic transmission of infringing content to the public, which may also attract liability under Sections 67 and 67A where such content is obscene, the offender shall be subject to enhanced penalties under the respective provisions of the Act.

Governmental Powers: Under Section 69A, the appropriate government or its duly authorized officers are empowered to issue directions to intermediaries or service providers to block access to any website or online platform that enables or promotes such infringement.

International Framework

International intellectual property rights (IPR) laws are governed by a network of treaties and agreements, primarily managed by the “World Intellectual Property Organization (WIPO)” and the “World Trade Organization (WTO)”.³¹² These agreements aim to harmonize global standards for IPR protection, encouraging innovation and trade.

The international IPR regime comprises a network of multilateral treaties and agreements, administered primarily by WIPO and WTO, designed to establish consistent minimum standards of protection, enforcement, and procedural certainty across sovereign nations.

³¹² WIPO, *WIPO-Administered Treaties*, <https://www.wipo.int/treaties/en/>.

i. WIPO-administered Instruments

Paris Convention (1883): Lays down the principles of national treatment and the right of priority concerning protection of patent, trademarks, industrial designs, and related matters, mandating that nationals of one Contracting State be afforded the same protection as domestic applicants in another, and permitting applicants a specified priority period for filing across Member States.

Berne Convention (1886): Mandates the protection of literary and artistic creations without the need for formal registration and recognises the moral rights of authors, and imposes minimum standards of economic rights and term of protection, thereby ensuring automatic and reciprocal copyright coverage among Contracting Parties.

Patent Cooperation Treaty (PCT): Facilitates the filing of a single international patent application that can subsequently enter the national phase in any designated Member State, streamlining the procedural aspects of international patent prosecution.

Madrid System: Allows trademark owners to file a single international application for registration in multiple Member States, simplifying and centralizing trademark protection.

Rome Convention (1961): Provides related rights protection to performers, producers of phonograms, and broadcasting organizations over their performances, recordings, and transmissions.

Budapest Treaty (1977): Recognizes the deposit of microorganisms at any international depositary authority as acceptable for patent procedures in all Member States, thereby eliminating duplicative biological deposit requirements.

Marrakesh Treaty (2013): Mandates the creation of copyright exceptions and limitations to enable cross-border exchange of accessible-format books for persons who are blind, visually impaired, or print-disabled.

ii. WTO-administered Instrument

TRIPS Agreement (1994): Incorporated into the WTO framework as Annex 1C, TRIPS obligates all WTO Members to adopt minimum standards of protection and enforcement for copyright, trademarks, geographical indications, industrial designs,

patents, including those for pharmaceutical inventions, layout designs of integrated circuits, and undisclosed information or trade secrets.³¹³ It additionally requires implementation of civil, administrative, and criminal sanctions, as well as border measures, and provides for resolution of disputes through the WTO Dispute Settlement Body. TRIPS also incorporates recognized flexibilities, such as compulsory licensing in cases of public health need, to balance protection with broader societal interests.

Collectively, these instruments comprise a coherent international legal architecture that prescribes substantive norms, procedural mechanisms, enforcement modalities, and cross-border cooperation, aimed at fostering creativity and innovation while accommodating exceptions tailored to public interest, national development, and equitable access.

2.6 Major Data Categories: Personal Data and Machine-Generated Data

i. Personal Data

“Personal Data” refers to any information associated with a natural person who can be identified, whether directly or indirectly, especially through an identifier such as a name, identification number, location details, online identifier, or by reference to one or more attributes related to that person’s physical, physiological, genetic, mental, economic, cultural, or social identity.³¹⁴ Examples include, without limitation, names, dates of birth, biometric data, fingerprints and DNA.

Value of Personal Data- Personal Data is broadly defined to encompass not only explicit identifiers (e.g. names, postal addresses, telephone numbers, bank accounts, credit card details, passport or driving license data, social security numbers) but also device identifiers (e.g. cookies, mobile device IDs) and biometric or genetic data, when employed to identify or profile individuals.

Sharing of Personal Data- Before transferring or disclosing any Personal Data, the data controller is required to identify and record a valid legal basis in accordance with

³¹³ WTO, *TRIPS Agreement*, https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

³¹⁴Ministry of Elecs. & Info. Tech. (MeitY), *Digital Personal Data Protection Act, 2023: Key Features and Implementation Framework* (2024), <https://www.meity.gov.in/>.

applicable legislation.³¹⁵ Under the UK GDPR and Part II of the Data Protection Act 2018, permissible grounds include, among others, consent, contractual necessity, legal obligation, vital interests, public interest, and legitimate interests. For processing activities carried out within the scope of law enforcement (Part III), additional statutory bases are prescribed.

The accountability principle mandates that controllers must be able to demonstrate the lawful basis for processing prior to any data sharing. In the absence of such documented justification, the transfer or disclosure of personal data is not permitted.

Example: A water utility and an electricity distribution company may lawfully share priority-service data where customers have expressly consented to the “tell us once” arrangement. This trial, carried out securely using spreadsheets, exemplifies compliance: the sharing relied on explicit consent (a lawful basis), was foreseen by customers and subsequently integrated into regular operations once found beneficial.

ii. Machine-Generated Data / Non-Personal Data

“*Non-Personal Data*” means any information excluding Personal Data, which does not or can no longer identify a natural person, either because it was never personal in origin (e.g. meteorological readings or industrial sensor outputs), or because it has been permanently anonymized using robust techniques rendering re-identification impossible.

The rapid expansion of machine-generated and anonymized datasets has prompted legal systems worldwide to explore dedicated frameworks for the governance of *Non-Personal Data (NPD)*. India has been at the forefront of this evolution, proposing a comprehensive *NPD Governance Framework* that seeks to balance innovation, economic growth, and collective rights. The subsequent chapter explores this framework in depth, analyzing its conceptual foundations, principles, and comparative significance.

³¹⁵ ICO, *Lawful basis for sharing personal data*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/lawful-basis-for-sharing-personal-data/>.

2.7 Conclusion

Data value transcends the mere intrinsic worth of raw data; the legal categorization of data into types such as financial, transactional, biometric, and intellectual property data reflects both the diversity and sheer volume of information in contemporary use. Intellectual property rights, protected under national and international statutes, confer exclusive rights of ownership and control over creative and innovative works. In modern legal frameworks, data regulation and governance address two principal classes of data: (a) machine-generated data, which is non-personal in nature, and (b) personal data. Legal frameworks governing personal data establish rigorous safeguards, acknowledging that certain categories of such information are designated as sensitive personal data. This includes, but is not limited to, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union affiliation, genetic or biometric identifiers, health information, or details relating to an individual's sexual life or orientation. As provided under Article 9(1) of the *General Data Protection Regulation (GDPR)*, the processing of such data is generally prohibited unless expressly allowed under specific legal conditions.

According to the GDPR, the term personal data covers any information that relates to an identified or identifiable natural person, thereby bringing it fully within the scope of data protection obligations. The processing of special categories of data is permitted only when one of the narrowly defined lawful grounds applies, such as explicit consent, substantial public interest, or the protection of vital interests of the data subject. Modern data regimes reflect an escalating volume of machine-generated data. Although such data may not implicate individual privacy rights, it nonetheless warrants appropriate governance under frameworks such as the GDPR and India's Digital Personal Data Protection Act, 2023 (DPDP Act), which similarly excludes publicly available personal data from its scope and mandates oversight by a newly constituted Data Protection Board.

Hence, rights to data are stratified according to provenance (machine vs. person), category (ordinary vs. sensitive personal), and jurisdiction. Corporate and regulatory governance measures must, therefore, be tailored: routine machine-created and non-

sensitive data may be subject to internal protocols, while personal and particularly sensitive data are subject to legal constraints that ensure individual privacy, accountability, and lawful processing.

Building upon this foundation, the next chapter examines the emerging governance structures surrounding Non-Personal Data, with particular reference to the Indian framework and its comparative implications.

CHAPTER 3:

CONCEPTUALISING NON-PERSONAL DATA: DEFINITIONS, SOURCES, TAXONOMIES AND A PROPOSED LEGAL DEFINITION

3.1 Introduction

3.2 Defining Non-Personal Data

3.3 Classification and Types of Non-Personal Data

3.4 Jurisprudence on Non-Personal Data

3.5 Stakeholders in the Non-Personal Data Ecosystem

3.6 Core Issues and Challenges

3.7 Proposed Legal Definition of Non-Personal Data: Analytical and Jurisprudential Explanation

3.8 Conclusion

3.1 Introduction

“Any information not relating to an identified or identifiable natural person. The origin of such data can be both human and non-human. Human NPD includes data that was originally personal but has been anonymized so the person cannot be re-identified; non-human NPD includes data that never related to a human (e.g. weather data).”

Data is a valuable asset for every entity, be it an individual, a business, or the government. Access to data enables informed decision making. Data may be personal, such as a customer’s bank account records, or non-personal, such as weather statistics or traffic-flow logs.³¹⁶ It supports applications across analytics, statistics, business strategy and security. While the growing volume of data offers significant opportunities, it also carries risks of misuse. As data becomes central to strategic planning, businesses increasingly ascribe monetary value to it, for example through targeted advertising, personalized recommendations and competitive data strategies.³¹⁷

³¹⁶ Laura Veldkamp, Valuing Data as an Asset, 27 REV. FIN. STUD. 1545, 1545–46 (2023).

³¹⁷ Joan Ofulue & Morad Benyoucef, Data Monetization: Insights from a Technology-Enabled Literature Review and Research Agenda, 74 MGMT. REV. Q. 521, 525–27 (2024).

The right to data ownership must remain protected, even when such techniques benefit enterprises. In this evolving landscape, maintaining ethical standards in data collection and application is crucial. Without appropriate safeguards, the monetization of data can easily encroach on individual rights and societal interests.

Purpose and Scope of *NPD* Governance:

NPD denotes electronic data that does not identify a natural person either because it never contained personal identifiers (e.g. weather records, industrial sensor outputs) or because any personal data has been anonymized or pseudonymized so as to render re-identification irreversible.³¹⁸ The purpose of governing *NPD* is to enable its responsible use for public policy, research, innovation and economic development while safeguarding against risks of re-identification, misuse or unfair exploitation and ensuring that benefits accrue not just to data holding entities but also to the communities and the State. This chapter encompasses all categories of non-personal data, including public, community, and private classifications. It seeks to outline the legal frameworks governing the collection, sharing, management, and protection of such data within an overarching data governance structure. Establishing such governance framework fosters trust among stakeholders and promotes a transparent data ecosystem. It also encourages broader participation in data-sharing initiatives, ultimately contributing to inclusive growth and technological progress.

3.2 Defining Non-Personal Data

Conceptual Framework

Non-Personal Data (NPD) refers to information that does not fall within the definition of personal data as set out in the Personal Data Protection Bill (PDP), 2019, or that lacks any personally identifiable elements.³¹⁹ Under the PDP Bill, personal data is described as information relating to an individual's characteristics, traits, or attributes of identity that can be used to identify that individual.

³¹⁸ Michèle Finck & Frank Pallas, They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data Under the GDPR, 10 INT'L DATA PRIV. L. 11, 11–13 (2020).

³¹⁹ Vidushi Marda, Non-Personal Data: The Case of the Indian Data Protection Bill, CTR. FOR L. & POL'Y RES. 1, 3–4 (2020), <https://clpr.org.in/wp-content/uploads/2020/08/Non-Personal-Data.pdf>.

From the standpoint of origin, *Non-Personal Data* may include information that has never been linked to natural persons, such as datasets on weather patterns, industrial output, or supply chain logistics, or information that was once personal but has been anonymized through processes designed to prevent re-identification. This distinction is especially important in fields such as genomics and the Internet of Things (IoT), where large volumes of data that appear non-personal may, when combined with auxiliary datasets, reveal latent identifiers capable of indirectly identifying individuals. *Non-Personal Data* is foundational to a wide range of applications including AI training models, urban planning, and health system optimization. As such, the ability to classify, secure, and use *Non-Personal Data* effectively is emerging as a key national priority. Proactive policies for *Non-Personal Data* are also critical for building trusted digital public infrastructure that aligns with the principles of openness, transparency, and user empowerment.

India is on the cusp of becoming a major global source of commercially valuable data, driven by a remarkable fifteen-fold increase in average monthly mobile data consumption from approximately 0.26 GB per individual at the end of 2016 (as commonly reported) to over 4 GB by the end of 2022.³²⁰ At an aggregate level, total national mobile data traffic surged from around 4.5 exabytes per month in 2018 to 14.4 exabytes by 2022 and per user monthly usage climbed to roughly 19.5 GB in 2022. This data deluge is attributable to precipitously falling smartphone costs and the broad rollout of high-speed mobile internet (4G and early 5G). In light of this exponential growth in digitally generated data, there is a compelling regulatory need to bolster data privacy protections, ensure consumer rights, and govern cross-border data flows. Legislative and institutional frameworks, notably the *Digital Personal Data Protection Act*, 2023, which is grounded in the Supreme Court's recognition of the Right to Privacy as a constitutional right in *Puttaswamy v. Union of India*, establish clear consent requirements, and guarantee rights of access, rectification, and erasure, while ensuring regulatory oversight through the *Data Protection Board of India*. Robust regulatory attention to data stewardship, consent, transparency, and lawful data

³²⁰ Telecom Regulatory Auth. of India, *Indian Telecom Statistics: Mobile Data Usage Trends*, TRAI Ann. Rep. 2024, at 10–12 (2024), https://traai.gov.in/sites/default/files/Annual_Report_2024.pdf.

transfers is therefore necessary to harness the potential of India's burgeoning data economy while preserving fundamental privacy rights.³²¹ At the same time, the lack of standardized frameworks for data anonymization poses a challenge to ensuring consistency across sectors and jurisdictions.

Data functions as a form of digital capital, elevating its significance to that of financial capital within a corporation. It is increasingly recognized as being equally important as intellectual property or industrial funds. Enhanced access to data equips a corporation with superior digital resources, thereby affording it a competitive edge in the marketplace.³²² India, as a first mover in the data economy, is strategically capitalizing on the inherent advantages of early entry into this data-driven domain, thereby enabling dominant players to amass extensive non-personal datasets and strengthen their competitive position. Small and medium enterprises, including start-ups, face material disadvantage due to their relative lack of access to such datasets, undermining their capacity to innovate and deliver novel solutions to market.³²³ These disparities not only impact economic equity but also risk consolidating informational monopolies in the hands of a few dominant players. To rectify such asymmetries and foster inclusive innovation, the Government has initiated regulatory measures to govern data not relating to identifiable individuals or personal data that has been anonymized. This entails the creation of specific roles, including Data Custodians, Data Trustees, and Data Businesses. The requirement for consent mechanisms prior to anonymization, safeguards against re-identification through mandatory anonymization standards, and governance of high-value datasets by designated trustees under the proposed *Non-Personal Data Authority*.³²⁴ Such measures are intended to balance accessibility to critical datasets with preservation of informational privacy, thereby enhancing SME and start-up empowerment while mitigating risks associated with commercial extraction of anonymized data. Establishing interoperability standards for

³²¹ Yuthika Bhargava, Beyond Consent: Enhancing India's Digital Personal Data Protection Framework, 21 INDIAN J.L. & TECH. 45, 52–54 (2025).

³²² Sarah Thompson, Competition and Data Access in Digital Markets, 42 J. TECH. & BUS. L. 123, 130–32 (2024).

³²³ Matthew McCarthy, The Big Data Divide and Its Consequences, 10 SOCIOLOGY COMPASS 1131, 1134–35 (2016).

³²⁴ Reuters, India Panel Proposes New Regulator for Non-Personal Data, Requires Anonymization and Governance Mechanisms, REUTERS (June 13, 2020).

Non-Personal Data exchange will further support the integration of datasets across sectors such as healthcare, agriculture, and mobility.

Compilation of Definitions:

European Union (GDPR, 2016)

NPD is implicitly defined as data not falling under the GDPR's definition of personal data, i.e., "*any information relating to an identified or identifiable natural person*" (Article 4(1)). Thus, *NPD* includes data that cannot be linked to an individual, such as anonymized or machine-generated data.

The *General Data Protection Regulation (GDPR)* represents one of the most comprehensive and stringent legal frameworks for data privacy and security worldwide.³²⁵ Although enacted by the *European Union (EU)*, its scope extends extraterritorially, applying to organizations outside the EU that process or collect data relating to individuals within its jurisdiction. The Regulation became enforceable on May 25, 2018, establishing strict obligations for compliance and accountability. Entities found in violation of its provisions may face substantial administrative penalties, with fines reaching several tens of millions of euros.³²⁶

The implementation of the *GDPR* reflects Europe's resolute commitment to data privacy and security, particularly as individuals increasingly place their personal information in the hands of cloud services amidst a backdrop of frequent data breaches. The regulation is broad in scope and general in its provisions, which makes achieving full compliance with the GDPR particularly challenging for small and medium-sized enterprises (SMEs).

³²⁵ Dorothy R. Auth, Navigating Data Protection Laws: Using European Clauses as the Foundation for U.S. Agreements, REUTERS LEGAL NEWS (Apr. 18, 2023).

³²⁶ Nikhil Kalyanpur & Abraham Newman, Europe's GDPR Imposes Stringent Penalties—Fines Reach Tens of Millions of Euros, WASH. POST (May 25, 2018).

European Commission (2020)

NPD is “data which originally did not relate to an identified or identifiable natural person or personal data rendered anonymous in such a way that the data subject is not or no longer identifiable.”

In February 2020, the European Commission promulgated its European Strategy for Data, explicitly recognizing data as a foundational economic asset and referring to it as “the lifeblood of economic development.”³²⁷ The strategy aims to drive innovation, productivity, personalized services, and improved policymaking. It affirms Europe’s ambition to chart a distinct path that balances open data flows with robust privacy, security, ethical, and consumer protection standards. The strategy envisions the establishment of a single European data space, designed to operate as an integrated internal market for data. This includes personal, non-personal, and industrial categories of data, which may move across sectors and Member States under fair, transparent, and lawful conditions, while complying with European competition and privacy laws.

It also proposes legislative measures such as the Data Governance Act. This regulation is designed to manage voluntary data intermediation, reuse of public sector data, and data altruism. The goal is to clarify access rights, ensure contractual fairness and interoperability, and define public interest exceptions in data sharing arrangements.³²⁸ The strategy seeks to position the European Union as a global leader in ethical and value-driven data governance, fostering responsible and sustainable innovation.

The Regulation provides for several key guarantees:

- i. Free movement of non-personal data: It ensures the unrestricted transfer of *Non-Personal Data* across national borders within the European Union. Entities are permitted to store and process such data in any EU member state without geographical limitations.

³²⁷ Thomas Wahl, *Commission Presents European Data Strategy*, eucrim 2020/1, at 24–25 (2020), <https://eucrim.eu/articles/commission-presents-european-data-strategy/>.

³²⁸ Samuel Stolton, *European Parliament Votes to Approve Data Governance Act*, Euractiv (May 6, 2025), <https://www.euractiv.com/section/digital/news/european-parliament-votes-to-approve-data-governance-act/>.

- ii. Regulatory accessibility: Public authorities must retain the ability to access data for oversight purposes, even when that data is stored or processed in another EU country or within a cloud infrastructure.³²⁹ The European Commission encourages service providers to adopt codes of conduct outlining procedures for users to transfer data between cloud platforms or to repatriate it to their own information systems.
- iii. Alignment with cybersecurity standards: The Regulation mandates consistency with the EU's cybersecurity framework. Existing security obligations for entities handling data continue to apply when data is stored or processed across borders or within cloud environments.³³⁰
- iv. Complementarity with the GDPR: The *General Data Protection Regulation (GDPR)* also enables the seamless movement of personal data among EU member states.³³¹ Together, these instruments seek to create a unified and coherent framework that facilitates the free and secure flow of data throughout the European Union.

Government of India (2020)

NPD is defined as “data that is not personal data” or “data that does not identify an individual,” including anonymized data, aggregate data, and data generated by non-human sources like IoT devices. For instance, anonymized crop yield data supports smart agriculture policies without identifying farmers, promoting public good applications.

The *Personal Data Protection Bill (PDP Bill)*, 2019, was introduced in the Indian Parliament on December 11, 2019. Alongside establishing a regulatory body known as the Data Protection Authority and setting out the legal framework for the governance of personal data, the Bill also touches upon *Non-Personal Data (NPD)*. It mandates

³²⁹ Deutsche Telekom, *Airbus Slam Plan Allowing Big Tech Access to EU Cloud Data*, REUTERS (Apr. 10, 2024), <https://www.reuters.com/technology/deutsche-telekom-airbus-slam-plan-allowing-big-tech-access-eu-cloud-data-2024-04-10/>.

³³⁰ European Comm’n, *Commission Facilitates Self-Regulation in Non-Personal Data Realm*, Eur. Comm’n Press Release (Mar. 10, 2020), https://ec.europa.eu/commission/presscorner/detail/en/IP_20_432.

³³¹ Jules Darmanin, *Unintended Consequences: How Recent Data Protection Rulings Threaten Europe’s Digital Future*, REUTERS (June 26, 2025).

the sharing of anonymized or non-personal datasets with the Central Government to support improved targeting of service delivery and the formulation of evidence-based policies. Within the context of Indian jurisprudence, this constitutes a distinct, though not the only, reference to non-personal data.

To address the issue of limited data accessibility within India's emerging artificial intelligence (AI) ecosystem, the *National Strategy for Artificial Intelligence* recommended measures such as the public release of selected government datasets and requirements for private entities to share aggregated data.³³² The *Economic Survey of India (2018–2019)* compared data to a natural resource, asserting that anonymized personal data functions as a “public good” that warrants state facilitation and policy support. Despite these developments, a significant gap remains in India's regulatory landscape, as no comprehensive legal framework yet governs non-personal data.

In July 2020, the *Ministry of Electronics and Information Technology (MeitY)* convened a *Committee of Experts on Non-Personal Data Governance*, chaired by Kris Gopalakrishnan, to propose a structured approach for regulating NPD.³³³ The Committee's recommendations included the creation of a dedicated regulatory authority and the enactment of legislation exclusively addressing *Non-Personal Data* governance, along with several related institutional measures.

The Committee's proposed *NPD* framework defines *Non-Personal Data* primarily by exclusion, encompassing all data that does not meet the definition of personal data. Under the PDP Bill, personal data is described as information relating to an identifiable natural person, based on any characteristic, trait, attribute, or combination of such identifiers, including any inference drawn for profiling purposes.³³⁴

³³² Aashish Aryan, *Centre Eyes January Start to India AI Datasets Collection, Aggregation*, Econ. Times (Dec. 27, 2024), <https://economictimes.indiatimes.com/tech/technology/centre-eyes-january-start-to-india-ai-datasets-collection-aggregation/articleshow/116678901.cms>.

³³³ Karishma Mehrotra, *IT Ministry Panel for Sharing Non-Personal Data*, *Indian Express* (July 15, 2020), <https://indianexpress.com/article/technology/it-ministry-panel-for-sharing-non-personal-data-6506728/>.

³³⁴ Ram Govind Singh & Sushmita Ruj, *The Personal Data Protection Bill Defines Personal Data*, *Times India* (Dec. 11, 2019), <https://timesofindia.indiatimes.com/business/india-business/personal-data-protection-bill-2019-explained/articleshow/72463721.cms>.

The framework classifies *Non-Personal Data* into three broad categories:

- i. Public Data, which includes anonymized datasets generated through public agencies such as land records, public health information, and vehicle registration databases.
- ii. Community Data, referring to data collected by municipal bodies, utilities, or private entities such as telecom operators, e-commerce platforms, and ride-hailing services.
- iii. Private Data, encompassing inferred or derived datasets created through the application of algorithms, proprietary analytics, or technological innovation.

This classification seeks to streamline the allocation of access rights, responsibilities, and usage conditions among multiple stakeholders, thereby fostering transparency, accountability, and equitable value distribution in India's data ecosystem.

Nonetheless, several factors warrant apprehension regarding this duality and the suggested link between personal and non-personal data. A clear division proves impractical because mixed datasets inherently comprise both personal and non-personal information, with these two categories inevitably intertwining.³³⁵ The suggested *Personal Data Protection Bill* briefly mentions that combined datasets fall under personal data protection regulations, akin to the application of *the General Data Protection Regulation (GDPR) in Europe*.³³⁶

Illustrative Case Study

A scenario where a city's transportation authority collects and employs traffic data to improve traffic flow could potentially exemplify a legal case study. The authorities might argue that the data qualifies as public non-personal information, thereby allowing its utilization for public purposes. A private corporation could contend that the data possesses inherent value and may be utilized for commercial purposes, including the development of innovative navigation applications or the marketing of

³³⁵ *Supra* note 329.

³³⁶ Ada Lovelace Inst., *Non-Personal Data: The Case of the Indian Data Protection Bill*, Ada Lovelace Inst. (Apr. 16, 2021), <https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/>.

products influenced by traffic trends. This scenario highlights the necessity for a clear legislative structure to regulate the ownership, utilization, and distribution of non-personal data, especially concerning public and commercial entities.

In 2020, the *Government of India*, acting through the *Ministry of Electronics and Information Technology (MeitY)*, established an *Expert Committee on Non-Personal Data (NPD)* to examine issues related to the governance of such data and to propose an appropriate regulatory framework.³³⁷ The Committee defined *Non-Personal Data* as information that either does not meet the criteria for personal data or has been anonymized to prevent the identification of individuals. It further classified *NPD* into three categories, public, community, and private non-personal data, based on its origin and ownership.

Among its key recommendations, the Committee proposed the creation of a *National Data Protection Authority (NDPA)* to oversee and regulate the management and sharing of non-personal data. It also underscored the need to promote the responsible use of *NPD* for research, innovation, and public interest applications, while ensuring adequate safeguards for privacy, security, and equitable access.³³⁸

OECD (2019)

NPD includes “data that are not linked to an identified or identifiable individual, such as data on weather, crops, traffic, or anonymized data used for statistical purposes.”

India has made significant advancements in formulating policies, strategies, infrastructure, and concepts aimed at enhancing its digital economy. Numerous initiatives are directed at realizing India's objective of a trillion-dollar digital economy. These advancements are not confined to India; nations worldwide are diligently

³³⁷ Kris Gopalakrishnan, *Report of the Committee of Experts on Non-Personal Data Governance Framework*, Ministry Elecs. & Info. Tech. 1, 5–7 (July 12, 2020), <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

³³⁸ Kris Gopalakrishnan et al., *Report Summary: Non-Personal Data Governance Framework*, PRS India (July 12, 2020), <https://prsindia.org/policy/report-summaries/non-personal-data-governance-framework>.

striving to harness the vast potential of the digital realm. In this regard, India and various other nations have recognized data as a crucial element of the digital economy.

To explore this aspect and understand its implications, nations have established policy frameworks to govern its utilization and dissemination. The OECD and the World Bank have acknowledged the significance of data reuse and sharing in fostering development and promoting economic progress. Concurrently, there has been a concentrated effort on supplementary issues and essential conditions, including the establishment of robust cybersecurity and data protection legislation; the identification of protective measures for citizens in the context of data sharing; the development of suitable frameworks for categorizing data types, comprehensive open data policies, and intellectual property systems, as well as the need to strike a balance in incentives.

World Economic Forum (2021)

NPD is described as “data that does not contain personally identifiable information, including aggregated, anonymized, or machine-generated data used for insights and innovation.”

The World Economic Forum’s (WEF) 2021 Data for Common Purpose Initiative (DCPI) elucidates pioneering models of data governance through its case studies in India and Japan, emphasizing the potential of data marketplaces in enabling structured data exchange while safeguarding individual rights.³³⁹ In India, the agricultural data exchange pilot conducted under the aegis of the WEF’s Centre for the Fourth Industrial Revolution India in collaboration with the Telangana state government and NITI Aayog, which demonstrates how the integration of data from personal, commercial, and governmental sources, managed through purpose-defined frameworks and supported by governance architecture, could economically empower stakeholders such as farmers without compromising privacy. These initiatives underscore the need for legal mechanisms that formalize data portability, consent-based access and accountability through trusted intermediaries, thereby enabling value creation in the

³³⁹ Alem Tedeneke, *Case Study on Data Markets in India and Japan*, World Econ. Forum (Aug. 3, 2021), <https://www.weforum.org/press/2021/08/case-study-on-data-markets-in-india-and-japan-show-what-is-possible/>.

data economy while maintaining alignment with constitutional and statutory protections for data principals.³⁴⁰

United Kingdom’s Department for Digital, Culture, Media & Sport (DCMS, 2021)

“Non-Personal Data refers to data that does not contain information that can be used to identify an individual, either directly or indirectly, such as anonymized datasets, aggregated statistics, or data generated by machines or processes without reference to a natural person.”

The Department for Digital, Culture, Media and Sport (DCMS), as constituted in the financial year ending 31 March 2021, functioned pursuant to statutory authority and ministerial delegation to oversee and regulate sectors integral to UK public policy.³⁴¹ This included covering digital infrastructure, cultural affairs, media, and sport. In that period, DCMS was responsible for formulating and implementing policy in fields such as telecommunications, broadcasting regulation, digital connectivity, data policy, cultural heritage, and sporting development, guided by its Outcome Delivery Plan for 2021–22 as mandated under the Spending Review framework. As a central government department, DCMS was required by statute (including the Government Resources and Accounts Act 2000) to prepare and lay before Parliament an Annual Report and Accounts, disclosing its resource and capital expenditures, objectives, key risks, and performance outcomes for the year ending 31 March 2021.

Other Definitions

International Organization for Standardization (ISO/IEC, 2020): *“Non-Personal Data is data that is not associated with an identified or identifiable natural person, including data that has been anonymized to prevent identification or data that originates from non-human sources, such as industrial or environmental sensors.”*

³⁴⁰ Matteo Nebbiai, Intermediaries Do Matter: Voluntary Standards and the Right to Data Portability, 11 INTERNET POL’Y REV. 1, 3–4 (2022).

³⁴¹ Dep’t for Culture, Media & Sport, *Data Protection and Digital Information Bill*, Gov.uk (July 15, 2025), <https://www.gov.uk/government/publications/data-protection-and-digital-information-bill>.

United Nations Conference on Trade and Development (UNCTAD, 2021): “*Non-Personal Data includes data that cannot be linked to an individual, such as biometric health data, aggregated economic indicators, environmental measurements, or machine-generated data used for public policy or commercial purposes, provided biometric health data is fully anonymized.*”

Gordon Institute for Business Science (GIBS, 2022): “*Non-Personal Data is information that does not identify or relate to a specific individual, including anonymized personal data, aggregated biometric datasets, or data generated by automated systems (e.g., IoT devices), used for business intelligence, public health studies, or operational efficiency.*”

Australian Government (2020): “*Non-Personal Data is data that does not identify an individual, including anonymized or aggregated data, or data that is inherently non-human, such as biometric data, used to support public health and industrial innovation.*”

3.3 Classification and Types of Non-Personal Data

Non-Personal Data can be categorized based on its source, processing level, and potential for re-identification. The principal classifications include anonymized data, aggregate data, machine-generated data, and industrial data.

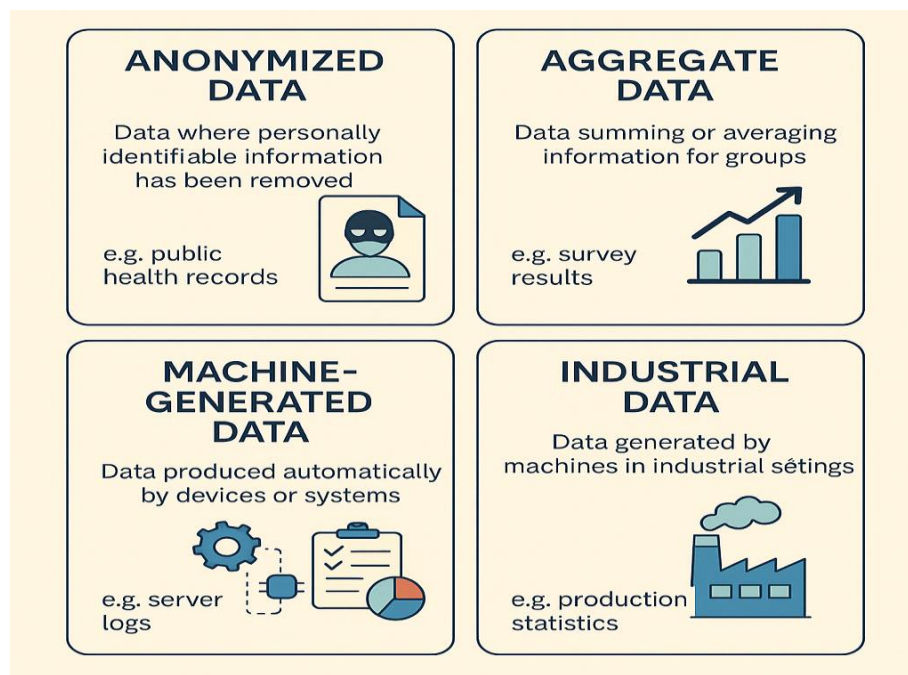


Figure 3.1 Types of Non-Personal Data

i. Anonymized Data

Publicly accessible anonymized datasets are compilations of data that have been subjected to a data anonymization procedure, preserving its analytical and research value while ensuring the privacy of data subjects. This process aims to safeguard individuals' privacy by eliminating personally identifiable information (PII), including names, addresses, and social security numbers, while retaining data that provides valuable insights for policy formulation, administrative functions, research, or trend evaluation across multiple sectors. *Non-Personal Data* include the aforementioned categories, in addition to data that originally lacked personal information, such as public GIS locations, regional or national socio-economic statistics, meteorological data, or aggregated tax revenues.³⁴²

These datasets may be made publicly accessible to foster innovation, enhance transparency, or support scientific study. Public anonymized datasets facilitate the training of machine learning models using aggregated health data to discern illness trends, formulate informed care plans, and design clinical trials for drug discovery.³⁴³ They enable algorithm training without compromising privacy, guide healthcare plans, optimize trial procedures, and accelerate drug development while maintaining privacy and ethical norms.

To achieve success at scale, it is crucial to recognize that a centralized approach to aggregating datasets may provide scalability challenges since each organization must upload their information to a single platform, and they may be reluctant to relinquish their data. Even if they share their data, maintaining frequent updates and synchronization with the primary system would be a formidable challenge.³⁴⁴ A more straightforward method is to establish an open network policy for anonymized data exchange. Entities may enlist the assistance of any technology provider and integrate into the network to disseminate their data under their own brand. This would confer

³⁴² European Commission, 'Factsheet: Non-Personal Data Regulation' (2018) available at <https://digital-strategy.ec.europa.eu/>.

³⁴³ OECD, 'Enhancing Access to and Sharing of Data' (2019).

³⁴⁴ Sridhar Suresh, *Efficient Data Synchronization Strategies for Handling Internet Connection Disruptions*, Medium (June 14, 2023), https://medium.com/@sridhar_suresh/efficient-data-synchronization-strategies-for-handling-internet-connection-disruptions-31dd7b977672.

legitimacy and authority over their datasets, facilitating long-term maintenance and updates. The decision on the availability of data at no cost may be a policy determination, and the network would accommodate both models.³⁴⁵

Case T-557/20: The General Court of the EU determined that data using pseudonyms cannot be classified as personal data if the receiver lacks further information to re-identify the individual.

Donnan et al. (United Kingdom): The use of anonymized data in research was determined to be exempt from the Data Protection Act 1998.

Under HIPAA, protected health information (PHI) must be anonymized or de-identified before dissemination for research or other purposes in the healthcare sector.

Data Brokers: The transaction of anonymized datasets presents ethical dilemmas, particularly within the ambiguous realm of data brokers. Beyond privacy, ethical considerations include preventing biases embedded within aggregated or machine-generated datasets, which can perpetuate unfair treatment or reinforce societal inequalities. Responsible data use policies must address these risks alongside privacy safeguards to ensure that non-personal data, while devoid of individual identifiers, does not inadvertently contribute to discriminatory practices or surveillance concerns. These broader ethical dimensions demand continuous oversight, transparency, and accountability from organizations handling such data. Emerging privacy-enhancing technologies, such as federated learning, homomorphic encryption, and secure multi-party computation, offer promising solutions to balance data utility with privacy protection. These approaches enable collaborative data analysis and machine learning model training without the need for direct data sharing, thereby significantly reducing the risk of re-identification. Incorporating these technologies within data governance frameworks can enhance the security of anonymized datasets and foster broader data sharing while adhering to stringent privacy and ethical standards.

While anonymized data supports research and innovation, its governance requires continuous vigilance to prevent re-identification and misuse.

³⁴⁵ OECD, ‘Data Governance in the Digital Age’ (2021).

ii. Aggregate Data

Aggregate data, once anonymized or processed to exclude personally identifiable information (PII), becomes non-personal data. This indicates that, while the data was originally gathered from people, it is no longer directly or indirectly attributable to them. Aggregation converts personal data into *Non-Personal Data* by amalgamating and summarizing it, rendering people unrecognizable.

The California Consumer Privacy Act and the California Privacy Rights Act explicitly indicate that they do not limit a business's capacity to collect, use, keep, sell, distribute, or reveal "aggregated consumer information."³⁴⁶ Aggregate consumer information refers to data relating to a group or category of consumers in which all individual identifiers have been removed, such that the information cannot be associated with or reasonably linked to any particular consumer, household, or device. It is important to note that aggregate consumer information does not include individual consumer records that have merely been anonymized.³⁴⁷

Contemporary state data privacy laws generally do not explicitly exclude aggregated personal data from their purview but several states such as Utah specifically exclude aggregated data from their definition of personal information.³⁴⁸ Regarding the other state legislation (namely Colorado, Connecticut and Virginia), while there is no explicit exemption for aggregated data, most aggregated data is implicitly exempt since it probably no longer meets the criteria for personal information once aggregated. Maintaining the quality and integrity of *Non-Personal Data* is essential to preserving its reliability and analytical usefulness. Errors, inconsistencies, or outdated data can lead to misleading insights or biased machine learning outcomes. Therefore, robust data governance frameworks must incorporate mechanisms for data validation, provenance tracking, and continuous quality assessment. Without such measures, the risk of erroneous conclusions or ineffective decision-making increases, potentially

³⁴⁶ David A. Zetoony, The California Consumer Privacy Act and De-Identified or Aggregate Information, NAT'L L. REV. (Mar. 21, 2023).

³⁴⁷ David A. Zetoony, *What Is Aggregated Data?*, Greenberg Traurig Data Privacy Dish (Oct. 21, 2022), <https://www.gtlaw-dataprivacydish.com/2022/10/what-is-aggregated-data/>.

³⁴⁸ David A. Zetoony, *Understanding Aggregated Data Under CCPA*, Greenberg Traurig Data Privacy Dish (Oct. 21, 2022), <https://www.gtlaw-dataprivacydish.com/2022/10/what-is-aggregated-data/>.

undermining the value of *Non-Personal Data* for policy, research, and commercial purposes. If data from multiple consumers is amalgamated to produce an average or aggregate statistic, it can be contended that such information is no longer “linked or reasonably linkable to an identified or identifiable natural person,” and thus, would not qualify as “personal data” under the VCDPA.

The primary objective of aggregation is to facilitate data analysis. Analyzing aggregate data facilitates the identification of insights that may be hard to discern in raw data. Aggregated data is more accessible for analysis, reading, and comprehension than raw data.³⁴⁹

By using a limited set of data points or KPIs (Key Performance Indicators), one may comprehensively grasp market trends and oversee corporate activities. Additionally, most major data aggregators include functionalities that display data in various formats. This enables even non-technical individuals to analyze and use aggregated data.

Data aggregators facilitate the automated collection, cleansing, and summarization of data. This automation reduces manual work and communication burdens, conserving time, energy, and financial resources.

Issues of data confidentiality also arise in relation to proprietary or trade secret information, as illustrated below.

Case Example – Trade Secret Protection: In a case adjudicated by the Bombay High Court, a former employee was provisionally restrained from employing confidential data, including customer and price information that he had downloaded during his tenure.³⁵⁰ The court mandated a commissioner to confiscate the material in his hands, underscoring the safeguarding of trade secrets.

³⁴⁹ OECD, ‘Data Governance in the Digital Age’ (2021).

³⁵⁰ Maulik Vyas, *Hindustan Unilever Seeks Injunction Restraining Former Employees from Using Confidential Manufacturing Data*, Mint (Apr. 13, 2018), <https://www.livemint.com/Companies/HUL-seeks-injunction-against-former-employees-1523613425873.html>.

iii. Machine-Generated Data

Machine-generated data refers to digital information automatically produced by software or hardware systems, typically on a schedule or triggered by specific events. In the era of enterprise adoption of big data analytics and machine learning, such data is increasingly analyzed in conjunction with other forms of enterprise data, enabling the derivation of novel insights that may inform business decisions.³⁵¹

Machine data encompasses outputs from a wide range of sources, including personal computing devices (e.g., desktop PCs, laptops, tablets, smartphones), servers and networks; websites and end-user applications; cloud-based or server-hosted applications; security information and event management logs; and devices that detect or measure physical properties. It also includes results generated through software applications performing secondary computations, such as forecasts or automated decisions derived from aggregated data, which may themselves constitute machine data when used for further decision-making.

Machine data may further result from task automation, for instance, a manufacturing control software issuing instructions to machinery, logging execution status, and triggering alerts or follow-on actions in response to operational outcomes. A critical subset of machine data is metadata, which is contextual data accompanying an event and describing attributes such as timestamps, geolocation, device settings, exposure parameters, and other relevant characteristics (for example, automatically generated metadata accompanying a photograph captured by a mobile device).

Machine-generated data thus represents a dynamic category of *Non-Personal Data* that underpins automation, analytics, and real-time decision-making.³⁵²

³⁵¹ Francesco Ciampi et al., Exploring the Impact of Big Data Analytics Capabilities on Business Model Innovation, 123 J. BUS. RES. 1, 3–4 (2021).

³⁵² Rama Prasath & S. Leelavathy, Data-Driven Decision-Making: Applying Big Data Analytics, 5 INT’L J. ENG’G SCI. & INFO. TECH. 402, 405–06 (2025).

iv. Industrial Data

Industrial *Non-Personal Data* is data produced in industrial environments that lacks any information capable of identifying an individual.³⁵³ The data falls outside the scope of personal data, which is defined as information relating to an individual who is identified or can be identified. This indicates it is not governed by the same rigorous privacy standards as personal data. Examples include information on meteorological conditions, logistical frameworks, and statistics related to the movement of goods.³⁵⁴ Anonymized data refers to information that was formerly personal but has undergone processing to eliminate any identifying details. Environmental and sustainability data represent an important subset of non-personal data, encompassing information such as emissions levels, resource consumption, pollution metrics, and ecological indicators. This data is increasingly critical for regulatory compliance, corporate responsibility, and public policy formulation related to climate change and sustainable development. Although often generated within industrial contexts, environmental data typically lacks personal identifiers and thus fits within the broader *Non-Personal Data* classification, highlighting its growing significance in both the public and private sectors.

Public data includes information such as property records, public health statistics, and automobile registration data. Essential legal issues for industrial *Non-Personal Data* include: since industrial data does not constitute personal data, individual consent is generally not required for its collection or use.

Examples and Case Studies:

i. Siemens' MindSphere Platform

Siemens' MindSphere (also known as *Insights Hub*) is an Industrial IoT as a service platform that collects telemetry from equipment across factories, fleets, etc. for

³⁵³ Non-Personal Data Processing: Why Should We Take It Personally?, EUR. J. PRIV. L. & TECH. 2020/2, at 184–86 (2020).

³⁵⁴ Dongna Zhang et al., Impacts of Weather Conditions on the US Commodity Markets, 123 ENERGY ECON. 106732, at 5–6 (2023).

analytics like predictive maintenance and process optimization.³⁵⁵ While anonymized industrial data can be powerful at scale, linking machine events with operator schedules or personnel logs risks re-identifying individuals. Even without personal identifiers, spatio-temporal patterns or shift timings can correlate data back to specific operators, revealing performance metrics and potential disciplinary consequences.

ii. Amazon Warehouse Optimization

Amazon uses sensor data including barcode scanners, timestamps, and movement logs to optimize inventory flows and track individual performance in real time. Such systems measure Time Off Task (TOT), scan rates, and machine trigger times. Although this data may be labelled "anonymous," linking it with worker IDs enables attribution of productivity metrics to specific employees. In France, the CNIL fined Amazon €32 million (approx. US \$35 m) in January 2024 for “excessively intrusive” monitoring, noting the use of data such as scans under 1.25 seconds or inactivity over 10 minutes to evaluate employees violating GDPR's data minimization and lawful basis principles.³⁵⁶

iii. Amazon Warehouse Data (2018)

A 2018 incident demonstrated that purportedly anonymized worker movement data could be re-identified by matching movement patterns to known shift schedules.³⁵⁷ Analysts correlated sensor logs (e.g., footfall patterns, scan timings) with shift data to reveal individual work rhythms, exposing which workers were fast or slow, potentially resulting in performance-related consequences. This research highlights how even de-identified logs combined with auxiliary metadata (shift times, locations) can breach anonymity in practice.

³⁵⁵ Case T-557/20, Single Resolution Bd. v. Eur. Data Prot. Supervisor, ECLI:EU:T:2023:219, ¶¶ 30–32 (Gen. Ct. Apr. 26, 2023), <https://curia.europa.eu/juris/document/document.jsf?docid=272345>.

³⁵⁶ Associated Press, *France's Privacy Watchdog Fines Amazon €32 Million for Excessive Monitoring*, AP News (Jan. 23, 2024), <https://apnews.com/article/amazon-france-fine-privacy-data-monitoring-32-million-euros-7b1f2e3a4c5d>.

³⁵⁷ *Id.*

iv. Tesla Manufacturing Data Leak (2023)

In May 2023, approximately 100 GB of internal Tesla files over 23,000 documents spanning 2015–2022 were leaked by two former employees to the German newspaper *Handelsblatt*.³⁵⁸ The leak affected approximately 75,735 current and former employees, exposing names, contact details, Social Security numbers (including that of Elon Musk), salaries, and employment records. Beyond personal identifiers, the leak revealed employee-level performance metrics and customer safety complaints. The scale and sensitivity of the data illustrate how employee anonymity can be broken when organizational identifiers remain intact, exposing individuals to privacy risks as well as corporate liability.

v. DHL Supply Chain Analysis (2020)

In 2020, DHL’s AI-powered route optimization system used for dynamic delivery planning processed anonymized vehicle GPS trace data to improve efficiency and reduce costs. However, when combined with external traffic datasets or known route schedules (e.g., delivery patterns, times) these anonymized traces could be re-identified, tying specific drivers to routes and potentially customer locations. This exemplifies how location data, even without names, can risk revealing both driver identity and customer addresses.

Implications:

Under GDPR, de-identified data that remains capable of being linked back to an individual through auxiliary information is considered personal data (Recital 26, Article 4(5)) and thus remains within the Regulation’s scope unless re-identification is not reasonably likely in practice, evaluated from the perspective of the data recipient or a third party with available means. The General Court’s judgment in *SRB v EDPS* (T 557/20) clarified that pseudonymized datasets may become effectively anonymized if a recipient lacks practical or legal means to re-identify individuals, as mere theoretical possibility is insufficient. Controllers are subject to the accountability

³⁵⁸ Dan Mihalascu, *Tesla Files: 100 GB of Confidential Data Leaked to German Newspaper*, InsideEVs (May 26, 2023), <https://insideevs.com/news/669784/tesla-files-100gb-confidential-data-leaked/>.

principle (Article 5(2)), requiring formal risk assessments, documentation, and implementation of “privacy by design” technical and organizational measures (Art. 25), including pseudonymization, aggregation, differential privacy, or controlled data sharing to mitigate re-identification risk. These measures reinforce compliance through proactive risk mitigation. Should re-identification occur, even through residual probability, it may amount to a personal data breach under Articles 33–34, triggering notification obligations and potential fines per Article 83 (up to €20 million or 4 percent of global turnover).³⁵⁹ In the UK, the Data Protection Act 2018 criminalizes wrongful re-identification and subsequent use or disclosure of de-identified information without consent, unless conducted under narrow exceptions such as public interest testing or accredited security purposes (Section 171). Any organization handling sensor or operational data, particularly from industrial or workforce systems, must treat data as personal unless anonymization withstands rigorous legal, technical, and adversarial testing. Failure to do so exposes the controller to regulatory enforcement, contractual and tort liability, and reputational harm.³⁶⁰

The classification of *Non-Personal Data* into anonymized, aggregate, machine-generated, and industrial categories underscores the diverse origins and applications of such data. Each category poses unique regulatory challenges in ensuring data utility without compromising privacy, emphasizing the need for dynamic, context-specific governance frameworks.

3.4 Jurisprudence on Non-Personal Data

The jurisprudential framework established by the Court of Justice of the European Union (CJEU) and the General Court has crystallized a contextual, recipient-based test for determining whether pseudonymized data qualifies as *Non-Personal Data* outside the GDPR’s scope. In *Patrick Breyer v Bundesrepublik Deutschland* (C-582/14, 2016), the CJEU held that dynamic IP addresses constituted personal data³⁶¹ if a reasonable

³⁵⁹ Mark Sweney, *GDPR Fines: Where Will BA and Marriott’s £300m Go?*, Guardian (July 10, 2019), <https://www.theguardian.com/business/2019/jul/10/gdpr-fines-british-airways-marriott-hotels-data-breaches>.

³⁶⁰ Sophie Brown, *Industry 4.0 Raises Privacy Stakes for Sensor Data*, Guardian (July 12, 2025), <https://www.theguardian.com/technology/2025/jul/12/industry-4-0-privacy-sensor-data>.

³⁶¹ Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, ¶¶ 45–48 (CJEU Oct. 19, 2016), <https://curia.europa.eu/juris/document/document.jsf?docid=184668>.

legal or technical pathway existed for re-identification even when such linkage required cooperation with a third party, unless re-identification would demand disproportionate time, cost, or effort, or was legally prohibited. In *SRB v EDPS (T-557/20, 2023)*, the General Court elaborated that whether pseudonymized data qualifies as personal data hinges on the recipient's capability to re-identify; where a recipient lacks the legal and factual means to do so³⁶², the data may be treated as non-personal for that recipient, even if the original controller retains re-identification capability.

This doctrine underscores that identifiability is not absolute, but rather subjective and contextual, assessed from the vantage of each data holder's access to auxiliary data and lawful means available. Consequently, the same dataset may be pseudonymized yet remain personal data for one party, while anonymized and non-personal for another, depending solely on re-identification potential and the effort required. This nuanced differentiation between pseudonymization and anonymization has significant regulatory implications, especially in data-sharing ecosystems involving multiple controllers and processors. It implies that compliance responsibilities under the GDPR may vary dynamically depending on who holds the dataset and what technical or legal resources they possess. Thus, data protection assessments must move beyond abstract definitions and incorporate situational evaluations based on control, purpose, and accessibility to identifiers.

Administrative and Legal Data:

Joined Cases C-141/12 and C-372/12 (YS v. Minister voor Immigratie, Integratie en Asiel, 2014):

Background: In the Netherlands, when assessing applications for residence permits, case officers of the Immigration and Naturalization Service (IND) prepare internal documents known as “minutes.”³⁶³ These records serve as preliminary assessments or

³⁶² Case T-557/20, *Single Resolution Bd. v. Eur. Data Prot. Supervisor*, ECLI:EU:T:2023:219, ¶ 25 (Gen. Ct. Apr. 26, 2023), <https://curia.europa.eu/juris/document/document.jsf?docid=272345>.

³⁶³ Lisa van der Berg, *Dutch Immigration Service Drafts Internal Rationale Before Decision*, NL Times (Apr. 15, 2025), <https://www.nltimes.nl/2025/04/15/dutch-immigration-service-drafts-data-rationale>.

justifications for decisions and typically contain the case officer's details, the applicant's personal data, relevant legal provisions, and a legal analysis. After Y.S.'s application for a residence permit under asylum provisions was denied, he requested access to these minutes. Instead of a full copy, he was provided with a summary containing his personal data, information on data sources, and details of any data-sharing entities.

Legal Issue: While applicants M and S were granted residence permits without receiving explanations, their subsequent requests for access to similar internal minutes were initially denied. Two Dutch courts overturned the denials, prompting the Minister to appeal. The Council of State (Raad van State) referred several questions to the Court of Justice of the European Union (CJEU) concerning the interpretation of "personal data" under Article 2(a) of Directive 95/46/EC (Data Protection Directive). The key issues were whether a legal analysis constitutes personal data and whether refusal to provide copies of the minutes violated applicants' rights of access under Article 12(a) of the Directive.

Court Ruling: The CJEU ruled that information such as the applicant's name, date of birth, and other identifiers clearly qualifies as personal data under Article 2(a) of the Directive. However, the legal analysis within the minutes does not fall within that definition, as it reflects the authority's interpretation of law rather than data about the applicant. The Court reasoned that granting access to the legal reasoning would amount to providing access to administrative documents, which lies outside the scope of data protection law.

In line with Article 8 of the Charter of Fundamental Rights and Article 12(a) of the Directive, authorities are not obliged to provide applicants with a copy of the full minutes.³⁶⁴ Instead, a comprehensive and intelligible summary of the personal data suffices, enabling individuals to verify its accuracy and legality. The judgment thus draws a clear line between data protection rights and administrative transparency,

³⁶⁴ Joined Cases C-141/12 & C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel*, ECLI:EU:C:2014:2081, ¶¶ 40–42 (CJEU July 17, 2014), <https://curia.europa.eu/juris/document/document.jsf?docid=155143>.

affirming that the Data Protection Directive was never intended as a mechanism for general access to government documents.

Relevance to Non-Personal Data (NPD): The case underscores the separation between data protection and administrative law, highlighting that internal administrative reasoning, devoid of identifiable information, constitutes non-personal data. It reinforces that Article 41 of the EU Charter of Fundamental Rights, which guarantees the right to good administration, applies exclusively to EU institutions and not to Member State authorities.³⁶⁵

Implications: The Court determined that Article 2(a) of the Directive should be understood to mean that specific data concerning an applicant for a residence permit, such as the “minute” relevant to the main proceedings, qualifies as “personal data” under that provision. In contrast, the legal analysis itself does not fall under this classification.³⁶⁶ Article 12(a) of Directive 95/46 and Article 8(2) of the Charter should be understood to grant an applicant for a residence permit the right to access all personal data pertaining to them that is processed by the national administrative authorities.³⁶⁷ To ensure compliance with that right, it suffices for the applicant to receive a comprehensive summary of the data, presented clearly and understandably. This format should enable the applicant to be informed about the data and to verify its accuracy and adherence to the Directive, thereby allowing them to exercise any relevant rights granted by that Directive. Article 41(2)(b) of the Charter of Fundamental Rights of the European Union should be understood to imply that an applicant for a residence permit is unable to invoke that provision against the national authorities.

³⁶⁵ Janneke Reichel, *Good Administration for Whom, by Whom?*, Realaw Blog (Oct. 14, 2022), <https://realaw.blog/2022/10/14/good-administration-for-whom-by-whom-the-right-to-be-heard-and-the-right-of-access-to-files-in-resolution-matters-by-j-reichel/>.

³⁶⁶ Davinia Brennan, *CJEU Clarifies Scope of Right of Access to Personal Data*, Tech L. Blog (July 30, 2014), <https://www.techlaw.ie/2014/07/articles/cyber-risk-data-privacy/cjeu-clarifies-scope-of-right-of-access-to-personal-data-2/>.

³⁶⁷ Davinia Brennan, *Court of Appeal Warns Against “Overstretching” the Concept of Personal Data*, Tech L. Blog (July 29, 2020), <https://www.techlaw.ie/2020/07/articles/privacy/court-of-appeal-warns-against-overstretching-the-concept-of-personal-data/>.

The CJEU distinguished between factual personal data and evaluative administrative reasoning, protecting the autonomy of administrative processes while ensuring individuals retain control over their personal data. This case remains pivotal in clarifying the conceptual boundary between personal and *Non-Personal Data* and in emphasizing the limited scope of data protection law vis-à-vis freedom of information principles.

Case C-434/16 (Peter Nowak v. Data Protection Commissioner, 2017):

Background: After successfully completing the first two levels of accountancy examinations administered by the Chartered Accountants Ireland (CAI), the applicant, Peter Nowak, failed a particular open-book accounting exam four times. Under Section 4 of the Irish Data Protection Act 1988 (“Irish law”), he sought all of the personal data pertaining to him possessed by the CAI and contested the exam result.³⁶⁸ Although the CAI provided Mr. Nowak with certain documents, they refused to provide his test script since, according to Irish legislation, it did not include any personally identifiable information. Mr. Nowak subsequently approached the Data Protection Commissioner of Ireland to contest the refusal to disclose his examination script. Mr. Nowak was notified by the Commissioner that the inquiry into the complaint would not proceed, since no significant violation of Irish law had been found. The Commissioner concluded that the data Mr. Nowak sought to correct did not constitute personal data under Irish law.

Legal Issue: The question arising under Article 2(a) of the Data Protection Directive concerned whether written answers provided by candidates in professional examinations constituted personal data, as well as any remarks made by examiners on those replies.

Court Ruling: Under the auspices of Mr. Nowak, the Data Protection Commissioner, the following governments participated: Ireland, the Czech Republic, Greece, Hungary, Austria, Poland, Portugal, and the European Commission (“EC”). Regarding whether the evaluator’s remarks constituted personal data about the applicant, it was

³⁶⁸ Peter Nowak v. Data Protection Commissioner, Case C-434/16 (CJEU May 4, 2017).

stated that the evaluator was unable to discern the candidates' identities when they made corrections and marked the test script.

Relevance to *NPD*: According to Mr. Nowak, the examination script contained personally identifiable information, and he sought to exercise his right of rectification. He contended that a candidate's written responses to a professional test comprised personally identifiable information. It was supported by the governments of Portugal, Greece, Hungary, Austria, and the Czech Republic, as well as the European Commission.

Implications: In its explanation of Article 2(a) of the Data Protection Directive, the Court stated that "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity." An identifiable person can be identified in this way, whether through an identification number or other means. Since the Data Protection Directive's definition included "any information," the Court reasoned that it did not limit itself to personally identifiable information (PII) since the term was broad. It included both factual and subjective information, such as views and evaluations, so long as it was "related" to the person or thing being studied. In addition to determining whether or not the applicant could join their desired profession, the test had an impact on their rights and interests. When the test was open-book, the Court found that a candidate's written responses constituted information that linked to them due to its substance, purpose, or impact.³⁶⁹ The Court also agreed with the Advocate General's Opinion that the purpose of an examination is to find out how well a candidate performed, not to obtain data unrelated to them, but rather to assess their individual performance. The Court ruled that the examination script contained personally identifiable information, as it reflected the candidate's intellect and writing style. This case broadened the interpretation of "personal data," confirming that evaluative and subjective materials can reveal personal attributes beyond basic identifiers. It also demonstrated how the GDPR's principle of data minimization must coexist with legitimate evaluative processes like

³⁶⁹ Noel Baker, *EU Court Rules Data Retention Directive Is Invalid*, Irish Examiner (Apr. 9, 2014), <https://www.irishexaminer.com/news/arid-20394712.html>.

education, testing, and recruitment. Collectively, Breyer, YS, and Nowak underscore that the classification of information as personal or non-personal is fluid and depends on legal context, control, and technical possibility, rather than the dataset alone.

Communication Metadata and Network Data

Joined Cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd, 2014):

Joined Cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd, 2014) involved the Court of Justice of the European Union (CJEU) declaring the Data Retention Directive invalid due to its infringement on fundamental rights.³⁷⁰ The Court found that the Directive's requirement for general and indiscriminate data retention by telecommunications providers constituted a disproportionate interference with the rights to privacy and data protection as enshrined in the Charter of Fundamental Rights of the European Union (CFR).

Background: The cases originated from challenges in Ireland and Austria regarding the validity of the Data Retention Directive (Directive 2006/24/EC). This Directive mandated that telecommunication service providers retain data related to communications for law enforcement purposes. In the landmark judgment of *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources*, the Court of Justice of the European Union (CJEU) addressed the validity of Directive 2006/24/EC as the Data Retention Directive.³⁷¹ This Directive required providers of publicly available electronic communications services to retain traffic and location data for a period of six months to two years for the purpose of making such data available to competent national authorities to assist in combating serious crime.

The applicants, including Digital Rights Ireland and an Austrian civil liberties group, contended that the Directive infringed upon the fundamental rights to respect for private life and the protection of personal data, as enshrined in Articles 7 and 8 of the

³⁷⁰ Joined Cases C-293/12 & C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine & Natural Resources*, ECLI:EU:C:2014:238, ¶ 37 (CJEU Apr. 8, 2014), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293>.

³⁷¹ *Digital Rights Ireland Ltd.*, Joined Cases C-293/12 & C-594/12, ¶ 37.

Charter of Fundamental Rights of the European Union (CFR).³⁷² They argued that the indiscriminate retention of communication metadata violated the fundamental principles of necessity and proportionality. The Court's deliberations also drew attention to the absence of adequate oversight and safeguards in the Directive's implementation framework. It noted that the Directive did not clearly specify who could access the retained data, under what conditions, or for what duration, leaving such discretion largely to Member States. This lack of harmonized safeguards created a substantial risk of misuse and disproportionate surveillance practices, undermining the essence of the right to privacy guaranteed by Article 7 of the Charter.

Furthermore, the Court observed that metadata, though less intrusive than content data, still provides an exceptionally detailed picture of an individual's private life. Patterns derived from communication logs can reveal intimate details such as relationships, daily habits, social circles, and even political or religious affiliations. Thus, metadata retention was found to pose risks equivalent to or greater than content interception.

Comparatively, the Court drew inspiration from the jurisprudence of the European Court of Human Rights (ECHR), particularly in *S. and Marper v. the United Kingdom* (2008), where the indiscriminate retention of biometric data was deemed a breach of Article 8 ECHR. The CJEU aligned its reasoning with this standard, reaffirming that generalized data collection without differentiation, limitation, or exception for specific purposes could not meet the proportionality test in a democratic society.

Legal Issues: Classification of Communication Metadata as Personal Data- The CJEU examined whether retained communication metadata, such as call logs, IP addresses, and subscriber information, constituted personal data under *Directive 95/46/EC (the Data Protection Directive)*.³⁷³ The Court affirmed that such data qualified as personal data because it could be used, in conjunction with other information, to identify individuals. The Court emphasized that the mere fact that data is not initially linked to

³⁷² Noel Baker, *EU Court Rules Data Retention Directive Is Invalid*, Irish Examiner (Apr. 9, 2014), <https://www.irishexaminer.com/news/arid-20394712.html>.

³⁷³ Michael O'Connor, *CJEU Examines Whether Retained Communication Metadata Constitutes Personal Data*, Fin. Times (Apr. 8, 2014), at B2.

an individual does not preclude it from being classified as personal data if there is a possibility of re-identification.

Court Ruling: The Court assessed whether the general and indiscriminate retention of communication metadata was justified under Article 15(1) of the ePrivacy Directive (Directive 2002/58/EC)³⁷⁴. It concluded that such retention constituted serious interference with the fundamental rights to privacy and data protection of individuals. The Court found that the Directive did not lay down clear and precise rules governing the scope and application of the retention obligation, nor did it provide sufficient safeguards against the risk of abuse. Consequently, the Court held that the Directive was invalid. The judgment further clarified that while combating serious crime is a legitimate and significant public interest objective, the means employed must still respect the principle of proportionality. The Court emphasized that the retention of all communication metadata for the entire population, without any distinction or suspicion, exceeded what was strictly necessary for achieving law enforcement purposes. Importantly, the CJEU criticized the absence of independent oversight mechanisms. It held that effective judicial or administrative supervision was indispensable for maintaining the legality of state access to retained data. Such oversight ensures that data processing activities do not devolve into mass surveillance incompatible with fundamental rights

Relevance to *NPD*: The ruling in Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland Ltd*, 2014) by the Court of Justice of the European Union (CJEU) primarily addressed the validity of Directive 2006/24/EC, which mandated the retention of communication metadata by telecommunications providers.³⁷⁵ The Court held that the Directive was invalid, ruling that the indiscriminate retention of such data constituted serious interference with the fundamental rights to privacy and the protection of

³⁷⁴ Kate McKenna, *CJEU Ruling Precludes General and Indiscriminate Retention of Telephony Data*, Nat'l L. Rev. (Apr. 20, 2022), <https://www.natlawreview.com/article/cjeu-ruling-precludes-general-and-indiscriminate-retention-telephony-data>.

³⁷⁵ Charles Arthur, *EU Court of Justice Overturns Law That Would Enable 'Snoopers' Charter'*, Guardian (Apr. 8, 2014), <https://www.theguardian.com/technology/2014/apr/08/eu-court-overturns-law-snoopers-charter>.

personal data under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

While the case did not directly address the anonymization of media content, the principles established regarding the classification of data as personal data have broader implications for the treatment of anonymized media content. The CJEU emphasized that data which, when combined with other information, can identify an individual, falls within the scope of personal data. Data that has been anonymized to the extent that individuals can no longer be identified does not constitute personal data and is not subject to the same legal protections.³⁷⁶

Anonymized media content, such as blurred videos that cannot be used to identify individuals, qualifies as *Non-Personal Data (NPD)*. This classification allows for greater flexibility in using such content for purposes like journalism or public sharing, as it falls outside the stringent data protection requirements applicable to personal data. It is crucial that the anonymization process is sufficiently robust and irreversible to ensure that the content remains non-identifiable and does not inadvertently infringe individuals' privacy rights.³⁷⁷ This case also implicitly contributed to the development of the concept of *data minimization* under Article 5(1)(c) of the *General Data Protection Regulation (GDPR)*, which later replaced Directive 95/46/EC. The Court's stance in *Digital Rights Ireland* informed EU legislative policy that any data processing activity must be limited to what is strictly necessary for a clearly defined purpose. Moreover, the decision served as a foundational reference for subsequent cases such as *Tele2 Sverige AB and Watson* (Joined Cases C-203/15 and C-698/15), where the CJEU reaffirmed the illegality of indiscriminate retention and refined the proportionality requirements for targeted surveillance measures. These judgments collectively established the principle that only targeted data collection under strict judicial control is compatible with fundamental rights.

³⁷⁶Kristof Van Quathem, *European Court Clarifies Concept of Personal Data*, Covington Inside Privacy (Mar. 8, 2024), <https://www.insideprivacy.com/eu-data-protection/european-court-clarifies-concept-of-personal-data/>.

³⁷⁷Olivia Grant, *Privacy Risks in AI-Generated Text*, N.Y. Times (July 10, 2025), at A12.

From an *NPD* perspective, the judgment underscores the need for strong anonymization standards in telecommunications datasets. As anonymized metadata is no longer considered personal data, it may be used for legitimate analytical or operational purposes without breaching EU data protection norms. However, the boundary between pseudonymized and truly anonymized data must be clearly maintained through technical and organizational safeguards.

Implications: The CJEU's ruling has significant implications for the treatment of Network and Performance Data (*NPD*) within the telecommunications sector: Anonymization of Metadata- The Court indicated that anonymized data, which cannot be attributed to an identified or identifiable person, does not fall within the scope of personal data. Telecommunications providers may utilize anonymized *NPD* for purposes such as network optimization and performance analytics without triggering obligations under data protection laws. Retention of Identifiable Metadata- If communication metadata is retained in a form that allows for the identification of individuals, it constitutes personal data. In such cases, providers must ensure compliance with data protection principles, including necessity, proportionality, and the implementation of appropriate safeguards to protect individuals' rights.

Case C-70/10 (Scarlet Extended SA v. SABAM, 2011):

Background: During an unspecified period, users of the Internet services provided by Scarlet Extended SA engaged in peer-to-peer (P2P) file-sharing activities, allowing the exchange and downloading of copyrighted musical works.³⁷⁸ SABAM, a Belgian management society responsible for licensing and protecting musical copyrights, initiated proceedings before the Brussels Court of First Instance on 24 June 2004, alleging that Scarlet's services were being used to facilitate copyright infringements.³⁷⁹

SABAM sought a declaration confirming the occurrence of such infringements and requested a court order compelling Scarlet to take measures to prevent users from unlawfully sharing protected works, specifically, by blocking or disabling the

³⁷⁸ Winston Maxwell, *SABAM: Advocate General Highlights Tension Between Privacy and Copyright*, E-Commerce Times (Aug. 1, 2011), <https://www.ecommercetimes.com/story/73012.html>.

³⁷⁹ Case C-70/10, *Scarlet Extended SA v. SABAM*, ECLI:EU:C:2011:771, ¶ 48 (CJEU Nov. 24, 2011).

transmission of files containing copyrighted music via P2P networks without authorization.

The case raised a crucial issue regarding the extent of intermediary liability for Internet Service Providers (ISPs) and the balance between intellectual property protection and the freedom of information within the digital environment. It also highlighted growing tensions between copyright enforcement mechanisms and the neutrality of ISPs, which are generally exempt from obligations to monitor user content.

Legal Issue: The principal question before the Court of Justice of the European Union (CJEU) concerned whether an ISP could be legally required to install a comprehensive filtering system for all electronic communications passing through its network, for an indefinite duration and at its own expense, to prevent the unauthorized sharing of copyrighted material.

The case required the Court to interpret multiple EU instruments, including³⁸⁰:

- i. Directive 2000/31/EC (E-Commerce Directive) – establishing limited liability for intermediaries and prohibiting general monitoring obligations under Article 15(1);
- ii. Directive 2001/29/EC (Information Society Directive) – safeguarding copyright holders' rights;
- iii. Directive 2004/48/EC (Enforcement of Intellectual Property Rights) – empowering courts to issue injunctions; and
- iv. Directives 95/46/EC and 2002/58/EC – protecting personal data and privacy in electronic communications.

The legal challenge involved reconciling these directives with the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, specifically,

³⁸⁰ Gwen Hinze, *EU Court of Justice: Social Networks Can't Be Forced to Monitor and Filter*, EFF Deeplinks Blog (Feb. 17, 2012), <https://www.eff.org/deeplinks/2012/02/eu-court-justice-social-networks-cant-be-forced-monitor-filter>.

the right to privacy (Article 7), data protection (Article 8), freedom of expression (Article 11), and intellectual property (Article 17(2)).

Court Ruling: The Court initially observed that pursuant to Article 8(3) of Directive 2001/29 and Article 11 of Directive 2004/48, holders of intellectual property rights are entitled to seek an injunction against intermediaries, including ISPs, whose services are utilized by a third party to violate their rights.³⁸¹ Drawing upon its established case law, the Court elaborated that these Directives empower national courts to issue orders against intermediaries, mandating them to implement measures not only to terminate existing infringements of intellectual property rights facilitated by their information-society services, but also to avert future infringements. The Court underscored that such orders must not contravene Article 15(1) of Directive 2000/31, which prohibits measures that would require an ISP to carry out general monitoring of the information that it transmits on its network.³⁸² Any injunctive order directed at an Internet Service Provider must align with Article 3 of Directive 2004/48, which explicitly forbids the imposition of unfair, disproportionate, or excessively burdensome measures on Internet intermediaries. The Court recognized that imposing a general monitoring obligation on ISPs would not only contravene EU law but would also create an atmosphere of surveillance incompatible with democratic principles. It further reasoned that any such system would involve the large-scale analysis of electronic communications, which necessarily entails processing personal data, including IP addresses, and could result in profiling of users' online activities. The Court balanced the competing fundamental rights: the right to intellectual property (Article 17(2) CFR) and the rights to privacy, data protection, and freedom of expression (Articles 7, 8, and 11 CFR). It concluded that a system capable of monitoring all user communications, regardless of whether they involved infringing content, would disproportionately interfere with these rights.

Relevance to *NPD*: The Court of Justice of the European Union's ruling in Case C-70/10, *Scarlet Extended SA v. SABAM* (2011), concerned whether an Internet Service

³⁸¹ Nedim Malović, *Article 8(3) of the InfoSoc Directive*, IPKat (Aug. 16, 2016), <https://ipkitten.blogspot.com/2016/08/article-83-of-infosoc-directive.html>.

³⁸² Glob. Freedom of Expression, *Scarlet Extended SA v. SABAM*, Glob. Freedom of Expression (Oct. 17, 2024), <https://globalfreedomofexpression.columbia.edu/cases/scarlet-extended-sa-v-sabam/>.

Provider (ISP) could be required to deploy content-filtering technology to detect and block peer-to-peer copyright infringement by analyzing users' IP addresses and communications data. The CJEU held that such an injunction, which involved indiscriminate monitoring of all customer communications, would violate multiple EU Directives: Directive 2000/31 (E-Commerce), Directive 2002/58 (E-Privacy), and Directive 95/46 (Data Protection Directive)³⁸³, in light of the fundamental rights to privacy and freedom of expression under Articles 7, 8, and 11 of the EU Charter.

Although the case did not directly address anonymized video or media content, its reasoning has important implications for the classification of Network and Performance Data (*NPD*).³⁸⁴ The Court emphasized that IP addresses and other metadata permitting user identification are subject to data protection law. By extension, media content that has been anonymized, such as blurred video footage or stripped metadata that prevents identification, falls outside this scope and may thus qualify as *Non-Personal Data (NPD)*, provided re-identification is not possible.³⁸⁵ This reasoning has had far-reaching implications for subsequent discussions on network neutrality and algorithmic content moderation. It underscored that automated systems which indiscriminately analyze or filter communications risk breaching users' privacy. Therefore, any deployment of filtering or monitoring technology must be based on transparency, necessity, and proportionality principles.

From an *NPD* standpoint, *Scarlet Extended* clarifies that technical data such as anonymized IP logs or aggregated traffic statistics, when stripped of identifiers, may be lawfully used for network optimization, cybersecurity, or research purposes. Such data, when properly anonymized, helps balance operational efficiency with compliance under the EU's digital rights framework.

³⁸³ Herbert Smith Freehills, *Preventive Injunctions and General Monitoring Obligations in L'Oréal v. eBay*, Lexology (July 12, 2011), <https://www.lexology.com/library/detail.aspx?g=05b25eae-8f79-4949-8714-122a0fab0fb7>.

³⁸⁴ Andrea Gadotti, Luc Rocher, Florimond Houssiau, Ana-Maria Crețu & Yves-Alexandre de Montjoye, *Anonymization: The Imperfect Science of Using Data While Preserving Privacy*, 10 *SCIENCE ADVANCES* eadn7053 (2024).

³⁸⁵ Natalie Kim, *Understanding Non-Personal Data*, *DATA PRIV. J.* (Apr. 15, 2025).

Furthermore, the ruling influenced later policy debates on *upload filtering* and *automated content recognition* under the *Digital Services Act (DSA)* and *Copyright Directive (EU) 2019/790*. The Court's insistence on proportionality serves as a reminder that automated enforcement must not compromise the confidentiality of communications or lead to generalized monitoring of internet users. Anonymized content does not constitute personal data and can lawfully be used for secondary purposes like journalism or public information, so long as the anonymization is irreversible and sufficiently robust against re-identification attempts.

This legal reasoning underscores that, unlike identifiable metadata or IP-based records, anonymized media content is not regulated as personal data and may be processed without triggering privacy obligations under EU law. However, ISPs and content handlers must ensure that anonymization techniques are sufficiently robust to remove any link to an identifiable person so as to maintain this *NPD* classification.

Implications: The CJEU held that requiring Scarlet to deploy a comprehensive filtering mechanism would effectively impose a permanent, costly, and indiscriminate monitoring obligation, contrary to Article 15(1) of the E-Commerce Directive. The Court ruled that intellectual property rights, while protected under Article 17(2) of the Charter, must be balanced against the rights to privacy, data protection, and freedom of expression.³⁸⁶ The ruling reaffirmed that filtering systems that indiscriminately inspect communications data are incompatible with fundamental rights and EU digital law. From an *NPD* standpoint, the decision reinforced the principle that anonymized and aggregated data, once devoid of identifiable elements, can be used freely without violating privacy obligations, provided the risk of re-identification is effectively mitigated.

The Scarlet Extended judgment serves as a landmark in delineating the limits of intermediary liability and the permissible scope of data monitoring within the EU's digital rights framework. It draws a clear boundary between personal data, which demands strong legal safeguards, and non-personal data, which may be used more

³⁸⁶ R.A. Costello, Intellectual Property and Fair Balance of Fundamental Rights – The Case *Sabam v. Scarlet*, 2 MEDIA L. REV. 742, 745–46 (2010).

freely for technical or analytical purposes. By insisting on proportionality and respect for fundamental rights, the Court established a foundational principle for subsequent EU data governance and privacy jurisprudence.

Media and Public Data:

Case C-345/17 (Sergejs Buivids, 2019):

Background: Case C-345/17 (Sergejs Buivids, 2019) involved the question of whether the processing of personal data by filming and publishing a video of police officers carrying out their duties in a police station on a video-sharing website such as YouTube falls under the scope of EU data protection law, specifically Directive 95/46/EC.³⁸⁷ The Court of Justice of the European Union (CJEU) ruled that it does, meaning the individual responsible for the recording and publication (Mr. Buivids) was subject to the obligations and limitations of the Directive. Mr. Buivids filmed himself making a statement at a Latvian police station and subsequently published the video on YouTube. The video was uploaded without the consent of the officers involved, prompting questions about whether such recordings of public officials, made within a professional setting, were exempt from data protection obligations. The case thereby bridged the domains of freedom of expression, public accountability, and personal data protection, exploring the thin line between legitimate public interest and privacy intrusion.

The Latvian court asked the CJEU whether this action constituted the *processing of personal data* under Directive 95/46/EC and, if so, whether any exceptions applied, particularly concerning journalistic purposes. The CJEU determined that the video recording and publication constituted personal data processing. The Court clarified that the term *processing of personal data* covers all actions from collection to dissemination. By recording and making identifiable individuals visible to an unrestricted online audience, Mr. Buivids' actions satisfied both elements of personal data processing and public disclosure. However, the Court also stressed that not all publication of public officials performing their duties necessarily breaches data

³⁸⁷ Case C-345/17, *Sergejs Buivids v. Datu Valsts Inspekcija*, ECLI:EU:C:2019:122, ¶¶ 35–37 (CJEU Feb. 14, 2019), <https://curia.europa.eu/juris/document/document.jsf?docid=210903>.

protection rules. If such publication contributes to a matter of genuine public interest, such as documenting potential misconduct or ensuring institutional transparency, it may qualify for a journalistic exemption, subject to the proportionality test. Specifically, the image of the police officers, being identifiable, qualified as personal data, and the act of recording and uploading to YouTube constituted *processing by automatic means*.

Legal Issue: The *Augstākā tiesa* (Latvian Supreme Court) submitted two preliminary questions under Article 267 TFEU, interpreting Directive 95/46/EC, particularly Article 3(1) and Article 9, concerning Mr. Buivids' video-recording and publication of police officers within a police station.³⁸⁸

- i. Does filming and publishing footage of identifiable individuals constitute *processing of personal data* under Article 3(1)?
- ii. If so, can such processing be exempted under Article 9, that is, *processing solely for journalistic purposes*, even if carried out by a non-professional journalist?

Court Ruling: The CJEU answered affirmatively on the first issue, holding that:

Video recordings depicting identifiable individuals, including police officers in the exercise of their duties, and uploaded online via a public video-sharing platform constitute the *processing of personal data by automatic means*, thereby falling within the scope of Directive 95/46/EC (Article 3(1)).³⁸⁹ On the second issue, the Court held that Article 9 may apply even when the processing is carried out by a private individual, provided that the sole purpose of recording and publishing the video is the disclosure of information, opinions, or ideas to the public, that is, for journalistic

³⁸⁸ Ted Shapiro, *CJEU Finds Filming Police Officers Constitutes Processing of Personal Data*, Wiggin LLP Insights (Feb. 25, 2019), <https://www.wiggin.co.uk/insight/court-of-justice-of-european-union-finds-that-an-individual-filming-police-officers-undertaking-their-duties-in-a-police-station-and-posting-it-online-constituted-processing-of-personal-data-but-may/>.

³⁸⁹ Ted Shapiro, *CJEU on Personal Data in Public Filming*, Wiggin LLP Insights (Feb. 25, 2019), <https://www.wiggin.co.uk/insight/court-of-justice-of-european-union-finds-that-an-individual-filming-police-officers-undertaking-their-duties-in-a-police-station-and-posting-it-online-constituted-processing-of-personal-data-but-may/>.

objectives.³⁹⁰ The Court emphasized that such an exemption must be interpreted strictly, balancing the fundamental rights to freedom of expression (Article 11 CFR) and privacy or data protection (Articles 7 and 8 CFR). The referring national court must evaluate whether the circumstances meet that threshold. This case illustrated the growing importance of balancing competing fundamental rights under the Charter, particularly the interplay between Articles 7–8 (privacy and data protection) and Article 11 (freedom of expression). The Court indicated that Member States must ensure that any limitation on freedom of expression for privacy protection purposes remains proportionate and necessary within a democratic society.

The decision also contributes to the evolving legal understanding of citizen journalism in the digital age. With the proliferation of smartphones and social platforms, individuals frequently act as content creators documenting public events. The Buivids ruling thus provides essential guidance on when such activity falls within journalistic purpose exemptions and when it constitutes regulated data processing.

Relevance to *NPD*: The ruling clarified that even actions by individuals, not only businesses, fall under the scope of EU data protection law when processing personal data. It also highlighted that exceptions such as the journalistic exemption must be interpreted narrowly and not applied broadly. This case therefore reinforces the accountability of private individuals who process identifiable information online.

Implications: This case underscores the broad scope of EU data protection law and the potential for individuals to be held accountable for processing personal data, even in seemingly informal contexts. The ruling also emphasized the importance of balancing the right to freedom of expression with the right to privacy and data protection. Furthermore, it draws attention to the evolving nature of online publication and its overlap with data protection principles, particularly when media content involves identifiable persons.

³⁹⁰ Fede Caruso, *The Journalistic Exemption in the GDPR*, Bookdown.org (Feb. 28, 2025), https://bookdown.org/fede_caruso/bookdown/the-journalistic-exemption-in-the-gdpr.html.

Case C-101/01 (Bodil Lindqvist, 2003):

Background: The Court of Appeal Gota (Sweden) requested a preliminary interpretation of the ECJ Data Protection Directive. In violation of the Swedish Personal Data Protection Law (Personuppgiftslagen), Mrs. Lindqvist was charged.³⁹¹ The Swedish parish of Alseda hired Mrs. Lindqvist as a catechist and maintenance worker. She established web pages on her computer in 1998, utilizing many parish volunteers' personal data to assist parishioners in preparing for confirmation. She requested the Swedish Church's website administrator to connect the information pages. This case became one of the earliest instances where the Court had to interpret the scope of data protection principles in the online environment. It marked a shift from purely institutional data processing to individual users engaging in data dissemination through the emerging medium of the internet.

The pages included details of 18 people's phone numbers, employment, hobbies, families, and medical conditions, excluding Mrs. Lindqvist herself. The pages were unknown to her colleagues and to the electronic data protection supervisor. After realizing certain coworkers disapproved of the pages, Mrs. Lindqvist removed them. Mrs. Lindqvist, together with the Swedish, Dutch, UK, and European Commission governments, submitted observations.

Legal Issue: Mrs. Lindqvist claimed that names in an online document did not constitute automated personal data processing. She proposed using *meta-tags* to generate an index and enable discovery of the site using a search engine. She further claimed that private individuals like herself who built websites for personal expression were not engaged in commercial activity and were therefore outside the scope of Community law. Mrs. Lindqvist argued that the Data Protection Directive and the PUL's prior authorization requirements infringed the freedom of expression guaranteed under Community law, citing *Connolly v. Commission (C-274/99 P, ECLI:EU:C:2001:127)*.³⁹² The Court was faced with determining whether private

³⁹¹ Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, ECLI:EU:C:2003:596, ¶ 71 (CJEU Nov. 6, 2003), <https://curia.europa.eu/juris/document/document.jsf?docid=48382>.

³⁹² Frances FitzGerald, *Privacy Issues: Bodil Lindqvist's Argument on Directive 95/46*, LegalGuide.ie (Apr. 3, 2021), <https://legalguide.ie/privacy-issues/2/>.

individuals using the internet for non-commercial purposes could be exempt from data protection obligations. This issue remains relevant today in the context of social media and personal blogging, where individuals routinely share personal information of others, often without consent.

The reasoning also laid the groundwork for distinguishing between purely domestic activities and public online publication. The Court clarified that once information is made accessible to an indefinite number of people online, it ceases to be “domestic” and falls under the scope of EU data protection law. She stated that the phrase *processing of personal data wholly or partly by automated means* was ambiguous. The Data Protection Directive, she argued, was disproportionate to the goal of defending rights and reputations, and mentioning names online was not a significant breach.

Court Ruling: The Swedish Government claimed that Article 3(1) of the Data Protection Directive’s definition of *processing of personal data entirely or partially by automated means* includes binary (computer) processing.³⁹³ It further argued that disclosing public data to an indeterminate number of people was not a *purely domestic activity* under the Directive. Invoking the Directive to transmit personal data from a computer to a website for access by third-country persons was consistent with the Directive’s purpose, according to both the Swedish Government and the European Commission.

The Court found Mrs. Lindqvist’s actions philanthropic and religious in nature but clarified that the exceptions under Article 3(2) of the Directive did not apply. The first exception in Article 3(2) excluded activities related to public security, defense, state security, and criminal law.³⁹⁴ The Court used the principle of *ejusdem generis* to decide that Article 3(2)’s exemption extended only to actions equivalent to those listed. Her charity or religious activities were not exempt since they were not of the same nature.

³⁹³ Swedish Gov’t, *Submission in Case C-101/01 (Lindqvist)*, CURIA (Nov. 6, 2003), <https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=EN>.

³⁹⁴ Eur. Ct. Just., *Handbook on European Data Protection Law* 45 (2018), https://fra.europa.eu/sites/default/files/fra-coe-edps-2018-handbook-data-protection_en.pdf.

The Court construed Article 8(1) of the Data Protection Directive's reference to *data concerning health* broadly to include all aspects of physical and mental health. Therefore, Article 8(1) covers data such as a foot injury and half-time medical leave.³⁹⁵

The Court examined Chapter IV of the Data Protection Directive's purpose and structure to determine whether viewing a third-country website constituted a *transfer* under Article 25.³⁹⁶ It emphasized that data transfer occurs when a hosting provider transmits personal data, not merely when an individual loads data onto a website. It noted that data may be stored on computers in other countries without users' awareness. The Court ruled that Article 25 should not be interpreted to mean that loading personal data onto an internet page necessarily transfers it to all third countries capable of accessing the internet.³⁹⁷ Thus, Mrs. Lindqvist had not transmitted data under Article 25.

The Court ruled that national data-processing standards must be harmonized to enable the free flow of data while ensuring appropriate protection of fundamental rights, citing the third and seventh recitals of the Directive's preamble. The Directive was found to be general but flexible. Although Member States had considerable freedom in implementation, the Directive remained predictable and compatible with Community law and fundamental rights.³⁹⁸ Member State authorities and courts must interpret their national laws in conformity with the Directive and fundamental rights.³⁹⁹ The Lindqvist judgment influenced the development of later legislative instruments, including the *General Data Protection Regulation (GDPR)*, which refined the definitions of personal data, processing, and territorial scope. Many of the interpretive challenges faced in Lindqvist directly informed Articles 2, 3, and 4 of the GDPR. From the *NPD* perspective, Lindqvist highlights that information published online may lose

³⁹⁵ Art. 29 Data Prot. Working Party, *Opinion 131*, at 8 (Feb. 15, 2007), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf.

³⁹⁶ Eur. Data Prot. Supervisor, *Case Law Digest: From Lindqvist to Schrems II*, at 71 (June 2021), https://www.edps.europa.eu/system/files/2021-06/21-06-09_case-law-digest_en.pdf.

³⁹⁷ Eur. Ct. Just., *Lindqvist and Data Protection Scope*, CURIA (Nov. 6, 2003), <https://curia.europa.eu/juris/document/document.jsf?docid=48382>.

³⁹⁸ Eur. Data Prot. Supervisor, *Lindqvist and Article 25 Interpretation*, Case Law Digest 71 (June 2021), https://www.edps.europa.eu/system/files/2021-06/21-06-09_case-law-digest_en.pdf.

³⁹⁹ Netherlands Gov't, *Automated Data Processing and Article 3(2) Exemptions*, Gov't.nl (Mar. 14, 2025), <https://www.government.nl/topics/privacy/automated-processing-article-3-2>.

its personal data status only after complete anonymization. If individuals remain identifiable by context or cross-referencing, the material remains subject to data protection rules. This underscores the importance of robust anonymization practices for any online publication containing personal details. The case continues to be cited in discussions on the responsibilities of individuals who publish online content containing others' data. It emphasizes that even non-professional, philanthropic, or religious motivations do not exempt individuals from compliance with EU data protection standards. The Court concluded that the referring court must assess all the circumstances of the case to strike a proportionate balance between the rights and interests at issue, including the basic rights guaranteed by the Community legal system.

Relevance to *NPD*: According to the Netherlands Government, computer servers automatically manage personal data stored on websites. It claimed that Article 3(2)'s exceptions did not apply to automated data processing, making it subject to the Data Protection Directive.⁴⁰⁰ Under Article 25, putting personal data on an internet site using a computer is not considered a transfer since the Directive does not define *transfer* as a deliberate transmission to a Member State or third country. The ECHR did not prioritize either freedom of speech or private life; state courts must balance them according to each case's context. The Netherlands also observed that Articles 10, 11, 14, 17, 18, and 19 of the Directive protected certain industries more specifically, and Member States may apply these principles to activities outside the Directive's direct scope.⁴⁰¹

Implications: The UK Government stated that *transfer* means the movement of data from one place or person to another, not simply viewing it. Only an actual transfer would require Member States to ensure the protection of personal data in a third country under Article 25 of the Directive. It further contended that the Directive did not restrict freedom of expression or other fundamental rights, noting that publishing personal data online is not necessarily more limited than publishing on paper. The European Commission stated that the Directive applies to the processing of all personal

⁴⁰⁰ GDPRHub, *Data Protection in the Netherlands*, GDPRHub (May 6, 2024), https://gdprhub.eu/Data_Protection_in_the_Netherlands.

⁴⁰¹ Eur. Comm'n, *Data Protection Explained*, Eur. Comm'n (July 29, 2025), https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.

data listed in Article 3, regardless of technology, and therefore websites are covered. It ruled that the action was not domestic. The online site's purpose made it a creative and literary work under Article 9 of the Directive, even if the processing did not fall under Article 3(2). The Commission also claimed that excluding non-commercial websites from the Directive might exclude a significant portion of internet pages.⁴⁰² It denied that the Directive violated Article 10 of the ECHR or other rights. The Commission maintained that Member States could not provide greater personal data protection or a broader scope than that prescribed by the Directive, as doing so would contradict its harmonizing purpose.

Health and Transaction Data

Case C-200/23 (Lindenapotheker, 2024):

Background: ND, conducting business as "Lindenapotheker" had been distributing pharmacy-exclusive medications through Amazon. A competitor DR initiated legal proceedings in German courts requesting an injunction against ND to halt the sale of certain products on Amazon.⁴⁰³ They contended that ND had processed health data related to these online transactions without securing the necessary consent, thereby violating Article 9 of the GDPR.

Legal Issue: The Court of Justice of the European Union determined that the information customers provide when acquiring online pharmacy-only medications qualifies as "data concerning health." The processing of such data is governed by the heightened restrictions applicable to special category data as outlined in Article 9 of the General Data Protection Regulation. This conclusion stands in opposition to the AG's Opinion regarding this matter.

The Court referenced the OT case and affirmed that the notion of "data concerning health" should be understood in a broad sense, considering the GDPR's aim to provide

⁴⁰² Eur. Comm'n, *Legal Framework of EU Data Protection*, Eur. Comm'n (May 4, 2016), https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en.

⁴⁰³ TwoBirds LLP, *Feeling Unwell After the CJEU's Lindenapotheker Decision?*, TwoBirds (Oct. 10, 2024), <https://www.twobirds.com/en/insights/2024/global/feeling-unwell-after-the-cjeus-lindenapotheker-decision>.

a high level of protection for individuals.⁴⁰⁴ The Court contended that a distinct category of data would be present in this instance: the online order could potentially disclose health-related information as it would enable the establishment of a connection between the medication. Therapeutic application and a specific individual who can be identified or is identifiable.

Court Ruling: In accordance with the Court's stance and consistent with OT, the AG recognized that special category data encompasses not only data that is inherently sensitive but also information that may reveal such sensitivity indirectly.⁴⁰⁵ In opposition to the Court's stance, the Attorney General maintained that the categorization of such information as health-related data is contingent upon the specific circumstances of each case and the context surrounding the processing of the data. Specifically, in instances where there is no explicit prescription identifying the individual for whom the medication is prescribed, the Attorney General opined that one cannot deduce that the product is solely meant for the purchaser. It is unreasonable to reach a conclusion regarding the health status of the individual associated with the data. The Attorney General asserts that this information does not constitute health data, as it only allows for hypothetical or vague conclusions regarding the purchaser's health status, a matter that should be examined by the referring court.

In opposition to this, the Court determined that the classification of information as health-related data is irrelevant to its accuracy or the controller's intent regarding the acquisition of special category data. The fact that the medicines do not necessitate a prescription is of no consequence; an alternative interpretation would contradict the intent of Article 9 of the GDPR.

The Court determined that this information must be regarded as health-related data, applicable to both the purchaser and any other individual for whom the order is issued. The Court observes that this data qualifies as health data, even in instances where there exists merely a possibility, rather than unequivocal certainty, that the medications are

⁴⁰⁴ TwoBirds LLP, *Lindenapotheke and GDPR Compliance*, TwoBirds (Oct. 10, 2024), <https://www.twobirds.com/en/insights/2024/global/feeling-unwell-after-the-cjeus-lindenapotheke-decision>.

⁴⁰⁵ U.S. Department of Justice, 'Overview of Data Protection and Privacy Enforcement'.

meant for the buyer. The Court holds the perspective that even in instances where the medications are designated for a different individual as it remains feasible to ascertain their identity and infer conclusions regarding their health status. if an alternative delivery address is supplied for the medications or if the customer mentions another person in their order.

Relevance to *NPD*: The Court determined that national legislation permitting competitors to take action against individuals allegedly violating the GDPR is not barred by the GDPR itself, particularly when grounded in the prohibition of unfair commercial practices.⁴⁰⁶ The Court asserts that these national provisions are not only in alignment with Chapter VIII of the GDPR, which offers remedies for individuals and their representatives concerning GDPR violations, but they also do not undermine the uniform level of protection for individuals throughout the EU. Furthermore, they play a role in enhancing individual rights and ensuring a robust level of protection is maintained.

Implications: Health-Data Processing Trigger- Controllers selling pharmacy-only items online must treat collected data as special category personal data, triggering the strict conditions of Article 9 GDPR including explicit consent and suitable safeguards regardless of whether the products require prescription.⁴⁰⁷ Consent and Legal Basis- Processing such data requires a valid legal basis under Article 6 GDPR plus the additional requirement of explicit consent under Article 9(2)(a).⁴⁰⁸ Legal justifications such as contract performance or legitimate interest are insufficient for this category. Increased Liability Exposure- Organizations face potential enforcement from not only supervisory authorities and data subjects, but also competitors THROUGH unfair business practice claims where local law so provides. Wider Commercial Effect: These ruling signals that GDPR breaches can now give rise to commercial legal challenges,

⁴⁰⁶ Tim F. Walree & Pieter T.J. Wolters, The Right to Compensation of a Competitor for a Violation of the GDPR, 10 INT'L DATA PRIV. L. 346, 348–50 (2020).

⁴⁰⁷ Anna Fiorentini, *GDPR Meets Unfair Competition Law: The Lindenapothke Case*, 9 EUR. PAPERS 123, 125–27 (2024).

⁴⁰⁸ C.F. Mondschein, *Sensitive Data and Explicit Consent*, NCBI Bookshelf (June 13, 2025), <https://www.ncbi.nlm.nih.gov/books/NBK543521/>.

reshaping the risk landscape for businesses that process special category data without proper safeguards.

Case C-621/22 (Royal Dutch Lawn Tennis Association v. Autoriteit Persoonsgegevens, 2024):

Background: The controller, a national tennis federation, automatically granted membership to individuals affiliated with recognized tennis clubs. In 2018, the federation shared its members' personal data, including contact details, with two sponsors in exchange for financial consideration. The sponsors used this information for promotional campaigns. Following member complaints, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) imposed a €525,000 fine for violating Articles 5(1)(a), 6(1)(a), and 6(1)(f) GDPR.⁴⁰⁹

This case exemplifies an enduring challenge in data protection law: determining whether commercial partnerships and sponsorships constitute a “legitimate interest” sufficient to override individuals' fundamental privacy rights.

Legal Issue: The federation argued before the Amsterdam District Court that the data transfer was justified under Article 6(1)(f) GDPR, as it served a legitimate interest, strengthening member relations by providing beneficial offers and discounts. The central question was whether such economic and relational objectives could satisfy the tripartite test of legitimacy, necessity, and proportionality established in prior CJEU cases such as *Rīgas satiksme* (C-13/16) and *Fashion ID* (C-40/17).

Court Ruling: The CJEU reaffirmed that “legitimate interest” must be interpreted narrowly, as it allows data processing without consent. The Court outlined three cumulative conditions: (i) a genuine and lawful interest, (ii) necessity of processing to achieve that interest, and (iii) a proportionality test ensuring that the data subject's rights are not overridden. While direct marketing may constitute a legitimate interest

⁴⁰⁹ Sachiko Scheuing, *CJEU Confirms Commercial Interests Can Qualify as Legitimate Interests*, Fedma (Oct. 4, 2024), <https://www.fedma.org/2024/10/04/cjeu-commercial-interests-can-qualify-as-legitimate-interests-under-the-gdpr/>.

under Recital 47 GDPR, it does not automatically outweigh privacy rights, particularly when the data subjects could not have reasonably expected such processing.⁴¹⁰

Relevance to *NPD*: This case indirectly informs *NPD* governance because many anonymized or aggregated datasets originate from personal data initially processed under the “legitimate interest” basis. It illustrates that even after anonymization, the proportionality and expectation principles remain vital ethical constraints. Controllers must therefore evaluate whether re-use of such data aligns with the original purpose and whether data subjects could reasonably foresee such secondary use.

Implications: The judgment underscores the accountability principle: controllers must document how their legitimate interests balance against individual rights. In *NPD* contexts, it warns against secondary commercialization or community-data monetization without transparent governance, as such practices risk re-personalization and loss of public trust.

Digital Advertising and Geolocation Data

Case C-446/21 (Schrems v. Facebook Ireland, 2024):

Background: This case revisits the ongoing litigation between privacy advocate Max Schrems and Facebook, this time focusing on whether Facebook could rely on the “performance of a contract” under Article 6(1)(b) GDPR as a lawful basis for personalized advertising. Schrems contended that such data processing required explicit user consent under Article 6(1)(a). The case also touched upon cross-border data transfers and the broader question of whether acceptance of standard service terms constitutes free and informed consent.

Legal Issue: The controller initiated legal proceedings against the decision of the DPA at the District Court of Amsterdam (Rechtbank Amsterdam - Rb. Amsterdam), contending that the release of its members' personal data was warranted by a legitimate interest in accordance with Article 6(1)(f) of the GDPR. The legitimate interest involves establishing a strong relationship with the data subjects allowing for the

⁴¹⁰ Mark Sharron, *GDPR: What Is Legitimate Interest?*, ISMS.online (July 4, 2025), <https://www.isms.online/general-data-protection-regulation-gdpr/gdpr-what-is-legitimate-interest/>.

provision of discounts and offers from sponsors, thereby facilitating access to tennis at a more economical rate.⁴¹¹ The controller contended that any interest, provided it is not unlawful, may be regarded as a legitimate interest.

Court Ruling: The court opted to address the questions collectively and referenced the judgment C 252/21, emphasizing that the legal foundation of legitimate interest under Article 6(1)(f) GDPR must be interpreted restrictively, as it justifies the processing of personal data in the absence of consent from the data subjects.

It is important to note that a diverse array of interests can be considered legitimate, and according to Recital 47, a legitimate interest should not necessarily be based on legal grounds.⁴¹² The court emphasizes that the recital refers to direct marketing purposes broadly as an illustration of legitimate interests that a controller may seek to pursue. Consequently, a valid interest extends beyond those interests codified and defined by legal statutes. The court asserts that the interest should be examined in light of the relevant legal framework and the specific circumstances surrounding the case.

Relevance to NPD: The processing of personal data must not only pursue a legitimate interest but also be essential for achieving the objectives of that interest.⁴¹³ A balancing assessment must be conducted between the interests or fundamental freedoms and rights of the data subject and the legitimate interests of the controller.

The necessity of processing arises solely when the legitimate interest sought cannot be attained as effectively through alternative, less restrictive methods.⁴¹⁴ In the present matter, the controller ought to have communicated with its members in advance and sought their consent regarding the transmission of their data to the sponsors for

⁴¹¹ Lisa Patel, *Establishing a Strong Relationship to Offer Discounts from Sponsors*, DATAGOV J. (June 15, 2025).

⁴¹² Rachel Kim, *Legitimate Interests and Diversity of Interests under Recital 47 GDPR*, TermsFeed (Apr. 16, 2025), <https://www.termsfeed.com/blog/gdpr-legitimate-interests/>.

⁴¹³ Katharina von Massenbach, *CJEU Clarifies When a Controller's Commercial Interest Can Qualify*, Fedma (Oct. 4, 2024), <https://www.fedma.org/2024/10/04/cjeu-commercial-interests-can-qualify-as-legitimate-interests-under-the-gdpr/>.

⁴¹⁴ Eur. Data Prot. Bd., *Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR*, EDPB (Oct. 8, 2024), https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf.

marketing objectives. This approach would restrict the sharing of information to only that which is essential.

Implications: In relation to the balancing test, the court emphasized that revealing data to a sponsor involved in casinos and gambling websites might adversely impact the data subjects, such as increasing the risk of developing gambling addiction. It is essential to consider whether, at the moment their personal data were gathered for the purpose of joining a tennis club, the members could have reasonably anticipated that such data would be shared with third parties for marketing purposes, in exchange for compensation.⁴¹⁵

The court determined that a legitimate interest need not arise from a legal norm; however, it must be lawful in nature. An interest satisfies the criteria outlined in Article 6(1)(f) of the GDPR only when it is deemed essential, and the fundamental rights and freedoms of the data subjects do not take precedence over this interest.⁴¹⁶

U.S. Jurisprudence

MCI Telecommunications Corp. v. AT&T Co. (1994):

Background: In this case, the U.S. Supreme Court examined the Federal Communications Commission's (FCC) authority to modify tariff-filing requirements under the Communications Act of 1934.⁴¹⁷ The FCC introduced a policy of "permissive detariffing," allowing non-dominant carriers to forego mandatory tariff filings. AT&T challenged the policy, arguing it exceeded the agency's statutory authority.

Legal Issue: The case centered on the interpretation of 47 U.S.C. § 203(a), which requires common carriers to file tariffs with the FCC, and § 203(b)(2), which allows

⁴¹⁵ Dentons, *CJEU Judgment: KNLTB-Case—Commercial Interests May Qualify*, Dentons (Oct. 16, 2024), <https://www.dentons.com/en/insights/alerts/2024/october/16/cjeu-judgement-klntb-case>.

⁴¹⁶ Securiti.ai, *CJEU Ruling on Legitimate Interest Basis for Commercial Purposes*, Securiti.ai (Oct. 13, 2024), <https://securiti.ai/cjeu-ruling-on-legitimate-interest-basis-for-commercial-purposes/>.

⁴¹⁷ *MCI Telecomms. Corp. v. Am. Tel. & Tel. Co.*, 512 U.S. 218, 220–22 (1994), <https://supreme.justia.com/cases/federal/us/512/218/>.

the FCC to modify those requirements.⁴¹⁸ The FCC's policy essentially exempted non-dominant carriers from the mandatory tariff filing requirement, effectively creating a system where only AT&T, the dominant carrier, was required to file tariffs.

Court Ruling: The FCC argued that its "permissive de-tariffing" policy was a permissible modification under § 203(b)(2).⁴¹⁹ The agency claimed that the policy was a reasonable way to adapt to the changing telecommunications landscape and promote competition. AT&T argued that the FCC's policy effectively eliminated the tariff filing requirement for most carriers, which went beyond the scope of "modification" as intended by Congress.⁴²⁰

Relevance to *NPD*: For future data-governance regimes, such as India's proposed *Non-Personal Data Authority*, this precedent cautions against expansive administrative interpretation beyond explicit statutory text. Any overreach in delegated powers, for example, mandating data sharing without legislative approval, may invite judicial invalidation.

Implications: This case demonstrates that effective data regulation requires statutory clarity and bounded delegation, ensuring that innovation in governance remains within democratically authorized limits.

The *MCI v. AT&T* case emphasized that the FCC's power to modify statutory requirements is not unlimited.⁴²¹ The Court highlighted the importance of adhering to the specific language of the statute and the potential consequences of exceeding the scope of delegated authority. The decision affirmed that the tariff filing requirement, while potentially outdated, remained a fundamental aspect of the Communications Act, and any significant changes to that system needed to come from Congress, not the FCC.

⁴¹⁸ Christopher J. Wright, *MCI Telecommunications Corp. v. AT&T*, Oyez (June 17, 1994), <https://www.oyez.org/cases/1993/93-356>.

⁴¹⁹ Quimbee Staff, *Case Summary: MCI Telecommunications Corp. v. AT&T*, Quimbee (Aug. 2016), <https://www.quimbee.com/cases/mci-telecommunications-corp-v-at-t-co>.

⁴²⁰ Christopher S. Yoo, Common Carriage's Domain, 35 YALE J. ON REGUL. 991, 1002–04 (2018).

⁴²¹ Fred Barbash, *MCI Telecommunications Corp. v. AT&T Co.: FCC Power to "Modify" Not Unlimited*, Cornell L. Sch. Legal Info. Inst. (June 17, 1994), <https://www.law.cornell.edu/supct/html/93-356.ZO.html>.

Blackbaud, Inc. Securities Litigation (2020):

Background: This consolidated class action arose from a 2020 ransomware attack on Blackbaud, a cloud services provider for educational and charitable organizations. The attack compromised donor and financial records, prompting allegations of inadequate cybersecurity measures, misleading statements about data protection, and delayed breach notification.⁴²²

Legal Developments: In addition to private litigation, the U.S. Federal Trade Commission pursued enforcement action under the Federal Trade Commission Act for unfair and deceptive practices. The settlement required Blackbaud to implement enhanced security governance and multi-factor authentication. However, class certification was denied due to difficulties in establishing ascertainable harm, exposing procedural challenges in mass privacy litigation.

Relevance to *NPD*: The case highlights that ransomware incidents can convert previously anonymized or aggregated data into personal data through re-identification. It reinforces the expectation that custodians of large datasets, personal or otherwise, must maintain robust cybersecurity measures and rapid breach-response mechanisms.

Implications: Blackbaud underscores that cybersecurity resilience is integral to lawful data stewardship. Even in jurisdictions lacking explicit *NPD* regulation, liability may arise under consumer protection, contract, or securities law. The case illustrates the necessity for cross-sector coordination among regulators and demonstrates that data security obligations apply equally to *NPD* custodians.

3.5 Stakeholders in the *Non-Personal Data* Ecosystem

Private Sector Entities

In the matter concerning Private *NPD*, the rights of ownership are vested in the entity to which the data is attributed. The ownership of public *NPD* will rest with the Government and the relevant public authorities responsible for gathering such

⁴²² Marianne Kolbasuk McGee, *Judge Denies Class Certification in Blackbaud Hack Lawsuit*, Bank Info Sec. (May 16, 2024), <https://www.bankinfosecurity.com/judge-denies-class-certification-in-blackbaud-hack-lawsuit-a-25248>.

information. In the matter of Community *NPD*, numerous data principals may possess intersecting rights and privileges, thereby complicating the determination of the authenticity of data ownership. To mitigate this issue, the *NPD* Committee has embraced the notion of "beneficial ownership/interest" to guarantee the protection of the public's interests. In such circumstances, a duly appointed trustee will safeguard data for the community, particularly in instances where interests converge. The trustee shall serve as the representative entity of the community, undertaking the responsibility to make decisions that are advantageous to its members.⁴²³ The community may engage with the trustee to ascertain the governance and application of their *NPD*.

Amazon's AWS Data Exchange facilitates access to third-party datasets like weather and market trends, enabling businesses to perform analytics. This service allows companies to integrate various data sources into their analytics workflows, enhancing insights and decision-making. AWS Data Exchange provides access to a wide range of third-party data, including *NPD* (Non-Practicing Entity) datasets, such as weather information and market trend data. By combining external data with their own, businesses can gain deeper insights into market trends, customer behavior, and other relevant factors.

Governments and Regulatory Bodies

The dissemination of *NPD* must occur within a structured framework and should not be conducted to satisfy personal interests. The Report outlines the various purposes, detailed below, for which the Government, researchers, entities, and citizens may seek access to *NPD*:

Data may be shared and requested for purposes of sovereignty, including national security, law enforcement, and compliance with legal and regulatory frameworks.⁴²⁴ Essential Objectives for the Public Good: Data sharing is permissible when there exists

⁴²³ P. Alison Paprica et al., *Essential Requirements for Establishing and Operating Data Trusts*, arXiv (May 4, 2020), <https://arxiv.org/abs/2005.06604>.

⁴²⁴ Glob. Partnership on AI, *Enabling Data Sharing for Social Benefit Through Data Trusts*, GPAI (2022), <https://gpai.ai/projects/data-governance/data-trusts/enabling-data-sharing-for-social-benefit-through-data-trusts.pdf>.

a legitimate necessity for informed policy-making, public benefits, enhancements in the provision of public services, and advancements in research and innovation. To foster equitable competition and enhance the well-being of the populace, data may be disseminated among various entities and start-ups, enabling them to tailor their services to meet consumer demands while encouraging innovation and contemporary technological advancements.⁴²⁵

Authorities or data custodians might pursue the obligatory dissemination of crucial information within a sector for designated objectives, which would likewise be overseen and supplied by these data trusts. It may encompass data that is shared both mandatorily and voluntarily.

Regarding the dissemination of "Confidential *NPD*", only the raw or factual data related to a community, gathered by a private entity, should be shared, contingent upon clearly established criteria and without any compensation.⁴²⁶ As the enhancement of value derived from raw data escalates, suitable frameworks may be employed for the exchange of information. Proprietary knowledge and algorithms may not be deemed appropriate for the purposes of data sharing.

Data Aggregators and Processors

A data processor is an entity that manages or processes *Non-Personal Data (NPD)* on behalf of a data custodian. This category includes enterprise software providers, Software-as-a-Service (SaaS) platforms, cloud service providers, Global Capability Centers (GCCs), and IT/ITeS companies that handle data for their clients or data custodians.

Under the *Non-Personal Data Governance Framework (NPD Framework)*, a data processor does not qualify as a data custodian concerning the data it processes for

⁴²⁵ CUTS Int'l, *Navigating the Puzzle of Non-Personal Data Sharing: Three-Pronged Analysis*, CUTS-CCIER (2021), <https://cuts-ccier.org/pdf/report-navigating-the-puzzle-of-NPD-sharing.pdf>.

⁴²⁶ Kris Gopalakrishnan, *Report on Non-Personal Data Governance*, Ministry Elecs. & Info. Tech. (Dec. 2020), <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

another entity. Consequently, the sharing of such processed *Non-Personal Data* is not generally anticipated.

The entity engaged in collecting, storing, processing, and utilizing data for its own business purposes shall be recognized as the custodian of that data, rather than its owner. The custodian is expected to ensure responsible stewardship, compliance with regulatory norms, and adherence to ethical data governance principles.

Community and End Users

In the case of personal data, rights are exercised by the data principal, the individual to whom the data pertains. However, for non-personal data, once personal identifiers have been removed or where the data concerns non-human entities (such as machines or environmental phenomena), there is no identifiable data principal.

The Committee of Experts on *Non-Personal Data Governance* (2020) recognized that in the absence of an individual data principal, the community generating the data should be empowered to exercise rights over non-personal data.⁴²⁷

A community is defined as a collective of individuals connected by common interests, objectives, or interactions, social, economic, geographic, or virtual. Communities may exist within defined territorial boundaries or entirely online.⁴²⁸ The benefits arising from *NPD* processing should accrue not only to organizations that collect and use the data but also to India as a whole and to the communities that generate such data.

Given the non-rivalrous nature of data, its value can be simultaneously utilized by multiple entities and communities without diminishing its utility. To safeguard community interests, the *NPD* Committee proposed that a non-profit organization (such as a Section 8 company, society, or trust) be authorized to lodge complaints before the regulatory authority regarding any adverse effects resulting from the use or dissemination of community-related *NPD*.⁴²⁹

⁴²⁷ MediaNama, *Summary: Report by the Committee of Experts on Non-Personal Data Governance Framework*, MediaNama (July 13, 2020), <https://www.medianama.com/2020/07/223-summary-non-personal-data-report-meity/>.

⁴²⁸ *Id.*

⁴²⁹ PRS Legis. Res., *Report Summary – Revised Draft Non-Personal Data Governance Framework*, PRS India (Jan. 4, 2021),

3.6 Core Issues and Challenges

Sensitivity Issues Involved

While personal data explicitly contains identifiable details such as name, age, gender, biometrics, and genetic traits, *Non-Personal Data* is often anonymized. Nevertheless, certain categories of *NPD*, particularly those concerning national security, strategic infrastructure, or public health, may pose significant risks even in anonymized form.⁴³⁰ For instance, data on the location of research laboratories or aggregated community health trends could, if misused, endanger public safety or national interests.

Lack of Effective Regulation

Unlike personal data, which is now governed under the Digital Personal Data Protection Act, 2023 (DPDP Act), there remains no comprehensive legal framework for regulating *NPD* in India. The Report by the Committee of Experts on *Non-Personal Data* Governance Framework (2020) highlighted this regulatory vacuum and emphasized the need for structured governance comparable to personal data protection laws.⁴³¹

Experts have underscored the importance of clearly defining the roles and responsibilities of all stakeholders, namely the data principal, data custodian, and data trustee, to avoid ambiguity in accountability and enforcement.

Undue Advantage to Big Tech

The Kris Gopalakrishnan Committee (2020) recommended that India's *Non-Personal Data* be made available for use by domestic entities to promote innovation and competition. However, this proposal has raised significant concerns regarding market concentration. Large technology companies possess the infrastructure, capital, and computational capacity to generate and exploit massive datasets, thereby gaining a

https://prsindia.org/files/policy/policy_committee_reports/Report%20Summary-Non-Personal-Data-Governance-Framework.pdf.

⁴³⁰ Trilegal, *Revised Report by the Committee of Experts on Non-Personal Data Governance Framework*, Trilegal (Jan. 8, 2021), https://trilegal.com/knowledge_repository/revised-report-by-the-committee-of-experts-on-non-personal-data-governance-framework/.

⁴³¹ Mira Norian, *What Is Net Debt? How Net Debt Is Calculated and Why It Matters*, Investopedia (May 16, 2025), <https://www.investopedia.com/terms/n/netdebt.asp>.

disproportionate advantage over smaller enterprises. This could reinforce monopolistic tendencies and hinder the equitable distribution of data-driven economic benefits.⁴³²

Mixed Datasets Containing Both Personal and Non-Personal Data

In practice, mixed datasets containing both personal and non-personal elements are increasingly common. The DPDP Act, 2023, similar to the *General Data Protection Regulation (GDPR)*, stipulates that such mixed datasets fall under the ambit of personal data protection standards.

However, distinguishing between personal and non-personal components is often complex, particularly where anonymization is partial or reversible. This ambiguity poses compliance challenges and raises concerns about the mandatory data-sharing provisions in the DPDP Act. The overlap between personal and non-personal datasets, though recognized in European jurisprudence, remains underexplored in the Indian context.

Lack of Effective Utilization of NFD

The issue of inefficient utilization of Net Financial Debt (NFD) reflects a broader challenge in financial governance, where entities fail to optimize the use of debt relative to liquid assets.⁴³³ Although not directly linked to *NPD*, poor management and disclosure of NFD can have regulatory and legal implications, potentially leading to non-compliance or misrepresentation in financial statements.⁴³⁴ Transparent reporting and responsible fiscal practices are necessary to maintain accountability and financial integrity.

Unprotected Interflow Across Departments

The unregulated exchange of *Non-Personal Data* among government departments, private entities, and citizens increases vulnerability to data breaches and unauthorized

⁴³² Anika Gupta, India's DPDP Act and Non-Personal Data Challenges, J. DATA PROT. & PRIV. 15, 22–24 (2025).

⁴³³ *Id.*

⁴³⁴ Officer's Pulse, *Non-Personal Data and Its Exchange Platforms*, Officer's Pulse (Mar. 22, 2024), <https://officerspulse.com/2024/03/22/non-personal-data-and-its-exchange-platforms/>.

access. Such unprotected interflow can benefit dominant actors like Big Tech, distort market competition, and impede accurate public policy formulation.

Additionally, inadequate coordination across departments may result in inefficient data utilization and prevent the realization of interdisciplinary policy insights essential for evidence-based governance.

Structural Gaps in the *NPD* Framework

While the *NPD* Framework represents a pioneering initiative, it remains conceptual and underdeveloped in operational terms. The framework articulates broad governance principles but lacks specific mechanisms for implementation. Critical questions regarding stakeholder rights, pricing models for data exchange, and legal structures for data markets remain unresolved.⁴³⁵

Moreover, the absence of standardized governance tools and sectoral interoperability mechanisms hinders effective enforcement and cross-sectoral collaboration. For the *NPD* Framework to function effectively, these structural deficiencies must be addressed through comprehensive legislation, regulatory clarity, and institutional coordination.

3.7 Proposed Legal Definition of Non-Personal Data: Analytical and Jurisprudential Explanation

The conceptual and jurisprudential analysis in the preceding sections reveals that the legal characterization of *Non-Personal Data* remains unsettled across jurisdictions, despite emerging convergence around the principles of identifiability, data utility, and risk-based protection. While major jurisdictions such as the European Union, Japan, Brazil, Singapore, and the United States have advanced conceptual clarity through legislative and policy instruments, their definitional approaches vary according to normative orientation, economic strategy, and constitutional tradition.

⁴³⁵ World Bank, World Development Report 2021: Data for Better Lives (2021), <https://www.worldbank.org/en/publication/wdr2021>

The absence of a unified formulation has led to regulatory ambiguity, particularly in developing legal systems where data governance remains at a formative stage.

In this context, the present research proposes a composite legal definition that draws upon the strengths of multiple jurisdictions and theoretical traditions to establish a conceptually clear and legally enforceable understanding of non-personal data.

Proposed Definition

“Non-Personal Data is any information that, in its original or processed form, cannot be linked to an identified or identifiable natural person, including anonymized, aggregated, machine-generated, or industrial datasets, provided that technically and legally sufficient anonymization or aggregation techniques prevent re-identification.”

This definition is designed to be legally sound, technologically adaptable, and normatively balanced. It incorporates the precision of European legal drafting, the technological realism of East Asian data strategies, the openness of common law regimes, and the ethical and constitutional concerns expressed in Indian jurisprudence.

Essential Elements and Doctrinal Explanation

The proposed definition comprises three substantive components, scope, process, and safeguard, each shaped by comparative legal reasoning and jurisprudential logic.

Scope

The clause *“any information that, in its original or processed form, cannot be linked to an identified or identifiable natural person”* mirrors the interpretive logic in Recital 26 of the GDPR, which defines personal data as information relating to an identifiable natural person. This phrase thus sets a negative boundary; data ceases to be personal when the linkage to an individual becomes impossible “by all means reasonably likely to be used.”⁴³⁶

⁴³⁶ Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Recital 26, 2016 O.J. (L 119) 1, 5–6, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

Similarly, the Free Flow of *Non-Personal Data* Regulation (EU) 2018/1807 adopts a residual definition, clarifying that any data not falling under the GDPR is deemed non-personal.⁴³⁷ The proposed scope clause incorporates this dual logic of exclusion and functional transformation.

The concept of “original or processed form” borrows from Japan’s Basic Act on Public and Private Sector Data Utilization (2016) and Singapore’s Data Sharing Framework (2021), both of which recognize that the nature of data may evolve depending on the processing stage. By including this phrasing, the definition anticipates dynamic data transitions and ensures legal clarity in distinguishing between personal, anonymized, and aggregated states.

In the Indian context, the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) recognized privacy as intrinsic to dignity and autonomy under Article 21 of the Constitution.⁴³⁸ This judgment, while dealing with personal data, establishes the principle that informational privacy extends only as far as identifiability persists. Consequently, data that cannot be linked to an identifiable person falls outside the zone of privacy protection, forming the theoretical basis for recognizing *Non-Personal Data* as a distinct legal category.

This linkage criterion also aligns with the interpretation of “identifiability” under U.S. federal guidance by the *National Institute of Standards and Technology (NIST)*⁴³⁹ and the *California Consumer Privacy Act (CCPA)*, which exclude “deidentified” or “aggregate consumer information” from personal data regulation.⁴⁴⁰

Process

The inclusion of “*anonymized, aggregated, machine-generated, or industrial datasets*” reflects both academic and policy consensus on the primary modalities of *Non-Personal Data* creation. The *EU’s Data Governance Act (2022)*, *Brazil’s General*

⁴³⁷ Regulation (EU) 2018/1807, of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, art. 3(1), 2018 O.J. (L 303) 59, 62, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>.

⁴³⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁴³⁹ National Institute of Standards and Technology, *De-Identification of Personal Information*, NISTIR 8053, at 12–14 (2015, updated 2020), <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8053.pdf>.

⁴⁴⁰ California Consumer Privacy Act, Cal. Civ. Code § 1798.140(h) (2020).

Data Protection Law (LGPD), and *Australia's Data Availability and Transparency Act (2022)* each acknowledge anonymization and aggregation as legally determinative processes for data classification.⁴⁴¹

Machine-generated and industrial datasets, central to *Germany's Industry 4.0* and *Korea's Digital Framework Act (2021)*, represent the growing class of information produced autonomously by devices, sensors, and AI systems, without direct human input. Their inclusion situates the definition within the technological realities of automated and interconnected data environments.

The conceptual recognition of “industrial data” draws from the *European Data Act (2023)*, which classifies industrial information as a separate governance domain requiring standardized access, interoperability, and equitable sharing.⁴⁴² Similarly, Singapore's Smart Nation initiative and *South Korea's AI Data Utilization Guidelines (2022)* treat industrial datasets as national resources that can be used for public innovation under strict governance controls.

By integrating these elements, the proposed definition acknowledges both private-sector and public-sector data streams, ensuring comprehensive coverage across economic and administrative contexts.

Safeguard

The safeguard clause, “*provided that technically and legally sufficient anonymization or aggregation techniques prevent re-identification*”, serves as the normative anchor of the definition. It replaces ambiguous notions of “robustness” with the twin standards of technical adequacy and legal sufficiency.

The technical sufficiency requirement corresponds with standards recognized *under ISO/IEC 20889:2018 (Privacy-enhancing data de-identification techniques)* and the *OECD Privacy Guidelines*, which require that anonymization be effective given

⁴⁴¹ Regulation (EU) 2022/868, of the European Parliament and of the Council of 30 May 2022 on European Data Governance, art. 2(1), 2022 O.J. (L 152) 1, 4–5, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>.

⁴⁴² European Data Act, Regulation (EU) 2023/2854, of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data, art. 2(13), 2023 O.J. (L 2854) 1, 6–7, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854>.

contemporary technological means. Legal sufficiency, in turn, implies compliance with statutory obligations such as *Recital 26 of the GDPR*, *Article 3(4) of the PIPL (China)*, and *Section 2(1)(t) of India's Digital Personal Data Protection Act, 2023 (DPDP Act)*, which collectively emphasize that any risk of re-identification renders data personal once more.

Judicial recognition of this principle is evident in *Sabu Mathew George v. Union of India (2018)*, where the Supreme Court of India underscored the need for lawful handling of health and demographic data to prevent misuse and re-identification.⁴⁴³ Similarly, in *Internet Freedom Foundation v. Union of India (2020)*, concerns over the Aarogya Setu application reiterated that anonymization must be both technically credible and legally enforceable.⁴⁴⁴

The safeguard element therefore operationalizes accountability by imposing a standard of care on data fiduciaries, ensuring that the transformation of personal data into non-personal form is both verifiable and reversible only under lawful authorization.

Comparative Legal and Academic Synthesis

The present definition is the product of a comparative synthesis across statutory, jurisprudential, and scholarly sources. Its architecture reflects a deliberate borrowing of key phrases and structural logic from multiple regimes to ensure interoperability and legal legitimacy.

From the European Union, it adopts the *negative definitional logic* (“data not relating to an identifiable natural person”) and the linkage test under Recital 26 of the GDPR.⁴⁴⁵

⁴⁴³ *Sabu Mathew George v. Union of India*, (2018) 3 S.C.C. 229 (India).

⁴⁴⁴ *Internet Freedom Foundation v. Union of India*, W.P. (C) 1021 of 2020 (Del. H.C. Jan. 31, 2020) (India).

⁴⁴⁵ Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Recital 26, 2016 O.J. (L 119) 1, 5–6, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

From the United States, particularly the CCPA (2018) and FTC privacy guidelines, it draws the operational notion of “*deidentified data with reasonable safeguards against re-identification*.”⁴⁴⁶

From China’s Data Security Law (2021), it integrates the principle of *state responsibility and security classification*, ensuring that even anonymized data may attract oversight when bearing strategic implications.⁴⁴⁷

From Japan’s *Data Free Flow with Trust (DFFT)*⁴⁴⁸ and Singapore’s PDPA-based frameworks⁴⁴⁹, it borrows the *ethical interoperability* model, trust-based, yet rights-aware.

From South Korea’s Digital Framework Act (2021), it draws the *technological sufficiency criterion* and the requirement that anonymization be auditable and certified by competent authorities.⁴⁵⁰

From Kenya’s Data Protection Act (2019)⁴⁵¹ and Open Data Policy (2020)⁴⁵², it borrows the *community-centric and developmental interpretation* of non-personal data, emphasizing equitable access and socioeconomic benefit.

Within India, it aligns with *Puttaswamy (2017)* in protecting identifiable information while permitting governance of anonymized datasets as a public resource.⁴⁵³ The definition also resonates with India’s Draft *Non-Personal Data Governance Framework* (2020) prepared by the Kris Gopalakrishnan Committee, which

⁴⁴⁶ California Consumer Privacy Act, Cal. Civ. Code § 1798.140(h) (2020), https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.140.

⁴⁴⁷ Data Security Law of the People’s Republic of China, art. 21 (2021), <http://www.npc.gov.cn/npc/c30834/202106/7c87ef5051f24a5ab4e48a7c164a8d0d.shtml>.

⁴⁴⁸ Japan, *Basic Act on the Advancement of Public and Private Sector Data Utilization*, Act No. 103 of 2016, art. 2 (2016), <https://www.japaneselawtranslation.go.jp/en/laws/view/3724>.

⁴⁴⁹ Personal Data Protection Act 2012, No. 26 of 2012, § 2(1) (Sing.), <https://sso.agc.gov.sg/Act/PDPA2012>.

⁴⁵⁰ South Korea, *Framework Act on Data Industry Promotion and Data Utilization*, Act No. 17344 of 2020, art. 3(2) (2021), https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55375.

⁴⁵¹ Kenya Data Protection Act, No. 24 of 2019, § 2 (2019).

⁴⁵² Kenya, National Open Data Policy, Kenya Gazette Supplement No. 45 (2020), <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2020/NationalOpenDataPolicy2020.pdf>.

⁴⁵³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, A.I.R. 2017 S.C. 4161; (2017) 10 S.C.C. 1 (India).

conceptualized anonymized community and industrial data as collective assets subject to stewardship.⁴⁵⁴

Academically, this definition integrates insights from jurists and scholars such as Daniel Solove's taxonomy of privacy harms, Paul Schwartz's informational self-determination, and Julie Cohen's concept of networked privacy, all of whom emphasize the identifiability threshold as the legal pivot between personal and collective data governance. The idea of *Non-Personal Data* as a *quasi-public good* derives from Elinor Ostrom's commons theory, suggesting governance mechanisms based on stewardship and access rather than ownership.

Legal and Policy Implications

This composite definition advances a unified doctrinal understanding of *Non-Personal Data* that harmonizes privacy protection with the governance imperatives of the digital economy. Legally, it provides a determinable test for classification: data is non-personal when no reasonable technical or legal means can identify a natural person, and when its reuse does not infringe residual privacy or intellectual property rights.

It also lays the groundwork for secondary legislation or delegated regulation on anonymization standards, audit protocols, and certification mechanisms under a future *Non-Personal Data* Act or as part of broader digital governance legislation. From a policy standpoint, the definition facilitates data portability, open data frameworks, and ethical innovation, particularly in high-value domains such as artificial intelligence, urban mobility, and environmental analytics. It ensures that data governance frameworks maintain consistency with constitutional principles of proportionality, accountability, and transparency while enabling cross-sectoral innovation.

⁴⁵⁴ Kris Gopalakrishnan, *Report of the Committee of Experts on Non-Personal Data Governance Framework*, Ministry Elecs. & Info. Tech. 1, 8–10 (July 12, 2020), <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

3.8 Conclusion

This chapter has undertaken a comprehensive exploration of *Non-Personal Data (NPD)*, elucidating its nature, scope, and significance through an integrated analysis of definitional frameworks, technical characteristics, stakeholder roles, and pertinent judicial and technical precedents. Drawing upon authoritative sources such as the GDPR, the European Commission, the Government of India, OECD, and the World Economic Forum, the chapter establishes *NPD* as data not linked to an identified or identifiable natural person, encompassing anonymized, aggregated, machine-generated, and industrial datasets. Policy frameworks such as the European Union's *Open Data Directive* for public transport schedules and India's *Non-Personal Data Governance Framework* for anonymized crop-yield data exemplify the policy relevance of *NPD* in advancing governance, innovation, and public welfare. The classification of *NPD* into distinct types, anonymized data (e.g., Netflix Prize Dataset), aggregate data (e.g., Google Trends), machine-generated data (e.g., Toronto's Sidewalk Labs), and industrial data (e.g., Siemens' MindSphere), highlights the concept's operational diversity and contextual adaptability. Technical discussions on anonymization techniques, including k-anonymity, differential privacy, and blockchain-enabled transparency, were juxtaposed with re-identification vulnerabilities demonstrated in the *AOL Search Data Leak* and *23andMe* breaches, emphasizing the delicate balance between data utility and privacy protection. The stakeholder ecosystem examined in this chapter, comprising governments (e.g., the UK's Open Government Data Initiative), private entities (e.g., Amazon's AWS Data Exchange), data aggregators (e.g., Nielsen's Consumer Insights), academia (e.g., MIT Senseable City Lab), and consumers (e.g., Waze's user-generated traffic data), reveals the multidimensional governance challenges inherent in managing *NPD*. Judicial pronouncements, including *YS v. Minister voor Immigratie*, *Sergejs Buivids*, *Bodil Lindqvist*, *Peter Nowak*, *Digital Rights Ireland*, *Scarlet Extended*, *Cour de Cassation*, *Royal Dutch Lawn Tennis Association*, and *Google Ireland v. CNIL*, clarify the evolving jurisprudence distinguishing anonymized and identifiable data. These cases confirm that anonymized transaction logs, aggregated statistics, and non-identifiable

metadata qualify as *NPD*, while simultaneously acknowledging re-identification risks that blur categorical boundaries.

Synthesizing these insights, this chapter proposes the following legally viable definition:

“Non-Personal Data is any information that, in its original or processed form, cannot be linked to an identified or identifiable natural person, including anonymized, aggregated, machine-generated, or industrial datasets, provided that technically and legally sufficient anonymization or aggregation techniques prevent re-identification.”

This proposed definition aligns with the GDPR’s conceptual distinction, the European Commission’s focus on anonymization, and India’s inclusive policy orientation, while addressing contextual fluidity as illustrated in *Digital Rights Ireland* (communication metadata) and *Lindenapotheke* (transaction logs). By embedding technical safeguards within the legal definition, it mitigates risks identified in re-identification case studies such as the *Netflix* and *Wachter* analyses and ensures future compatibility with AI-driven data-linkage environments.

Understanding the multifaceted nature of *NPD* is essential for developing equitable and innovation-oriented governance frameworks. The proposed definition provides a clear doctrinal foundation to demarcate *NPD* from personal data, thereby enabling its lawful use across diverse domains, such as data analytics (*Waze’s traffic insights*), smart cities (*Sidewalk Labs*), and industrial automation (*Amazon’s warehouse optimization*), while safeguarding privacy and preventing misuse. Judicial decisions like *Scarlet Extended* and *Cour de Cassation* underscore the need for adaptive legal standards for evolving data types (e.g., IP addresses), whereas technical studies such as *Strava’s heat map incident* reiterate the importance of irreversible anonymization.

Ethical and regulatory concerns persist, ranging from equitable access to the benefits of *NPD* (e.g., ensuring smart city data does not marginalize vulnerable groups) to ownership and custodianship disputes (e.g., over user-contributed datasets like *Waze*). Accordingly, policymakers must prioritize standardized anonymization protocols, interoperable data-sharing infrastructures (especially for IoT and AI ecosystems), and ethical frameworks ensuring transparency, fairness, and accountability.

In conclusion, this chapter situates *NPD* at the intersection of law, technology, and policy. It demonstrates that a robust, technically informed legal definition, grounded in comparative jurisprudence and empirical evidence, is indispensable for operationalizing *NPD* within India's data economy. The insights derived herein lay the groundwork for the forthcoming analysis of governance models, legislative frameworks, and implementation mechanisms aimed at fostering innovation while preserving privacy and ensuring distributive justice in the emerging *NPD* ecosystem.

CHAPTER 4

COMPARATIVE LEGAL FRAMEWORKS GOVERNING NON-PERSONAL DATA: A CROSS-JURISDICTIONAL ANALYSIS

4.1 Introduction

4.2 Conceptual Framework for Non-Personal Data Regulation

4.3 Country-Specific Analysis

4.3.1 Germany

4.3.2 France

4.3.3 Finland

4.3.4 Estonia

4.3.5 United States

4.3.6 United Kingdom

4.3.7 Canada

4.3.8 Australia

4.3.9 China

4.3.10 Japan

4.3.11 Singapore

4.3.12 South Korea

4.3.13 Brazil

4.3.14 Kenya

4.4 Comparative Analysis

4.5 Conclusion

4.1 Introduction

The global landscape of *Non-Personal Data (NPD)* governance reflects diverse regulatory orientations, each embedded within distinctive legal cultures, political economies, and technological imperatives. In the European Union, *Non-Personal Data* regulation has evolved under the aegis of the *Free Flow of Non-Personal Data Regulation (EU) 2018/1807*, which complements the *General Data Protection Regulation (GDPR)* by focusing on data that falls outside the scope of personal

identifiers. This Regulation facilitates unhindered cross-border data flows within the EU, prohibits data localization requirements unless justified on grounds of public security, and promotes self-regulatory codes of conduct to enable data portability.⁴⁵⁵ Germany, France, Finland, and Estonia have internalized these EU-wide principles through domestic legislation while developing frameworks aligned with national priorities. For example, Germany’s *Data Strategy 2021*⁴⁵⁶ emphasizes public-sector information reuse, industrial data spaces, and inter-sectoral interoperability under a human-centric digital constitutionalism paradigm. France’s *Loi pour une République numérique* encourages open data in the public sector and envisages data as a “common good,” whereas Finland and Estonia leverage their high digital maturity to experiment with decentralized architectures and public-private collaboration mechanisms to govern machine-generated and industrial data.⁴⁵⁷ Across these Member States, the overarching conceptualization of *Non-Personal Data* is deeply embedded in the EU’s rights-based constitutional framework, which harmonizes innovation with fundamental rights, competition law, and the *Digital Markets Act (DMA)* and *Digital Services Act (DSA)* regimes.

Beyond Europe, the governance trajectories of South Korea and Kenya further enrich the comparative understanding of *Non-Personal Data* regulation within distinct developmental and institutional contexts. South Korea’s regulatory ecosystem operates under the *Personal Information Protection Act (PIPA)* and the Data Industry Promotion Act, which together promote data-driven innovation through a robust framework of anonymization, certification, and industrial data utilization. The *Ministry of Science and ICT (MSIT)* and the *Korea Data Agency (K-DATA)* play a pivotal role in operationalizing policies that foster artificial intelligence, big data analytics, and public-private data sharing platforms. The Korean model underscores a

⁴⁵⁵ Joel A. Alves, The Regulation (EU) 2018/1807 on a Framework for the Free Flow of Non-Personal Data in the European Union and Its Implementation by Public Administrations, 3 EUR. REV. DIGIT. ADMIN. & L. 55, 56–57 (2022).

⁴⁵⁶ Federal Ministry for Economic Affairs and Climate Action (Ger.), *Data Strategy: Driving Progress with Data*, at 1–2 (2023), <https://www.bmwi.de/Redaktion/EN/Publikationen/data-strategy.pdf>.

⁴⁵⁷ Loi n° 2016-1321 du 7 octobre 2016 pour une République Numérique, Journal Officiel de la République Française [J.O.] [Official Gazette of France], Oct. 8, 2016, art. 17, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746>.

state-facilitated yet market-oriented approach, balancing stringent privacy safeguards with proactive data commercialization and global competitiveness.

Kenya, by contrast, represents an emerging data governance jurisdiction where *Non-Personal Data* regulation is still at a formative stage. Guided by the Data Protection Act (2019) and the Digital Economy Blueprint, Kenya's framework emphasizes open government data, innovation-led economic transformation, and regional cooperation through initiatives such as the Smart Africa Alliance. The Office of the *Data Protection Commissioner (ODPC)* anchors oversight, while the *Open Data Initiative* promotes transparency and civic engagement through anonymized public datasets. Although institutional capacity and enforcement remain nascent, Kenya's approach reflects a developmental data governance model, one that seeks to balance socio-economic inclusion with gradual institutional strengthening and digital sovereignty.

The United States lacks a federal law governing *Non-Personal Data* in the abstract, relying instead on a patchwork of sectoral regulations, state laws, and private ordering.⁴⁵⁸ The American legal system, steeped in contractual freedom and First Amendment values, treats both personal and *Non-Personal Data* as assets governed primarily by tort, contract, and property principles. Non-personal data, particularly that which is anonymized, aggregated, or machine-generated, is subject to proprietary claims and trade-secret protection under the *Defend Trade Secrets Act (2016)*.⁴⁵⁹ Sectoral regimes, such as the *Health Insurance Portability and Accountability Act (HIPAA)* or the *Children's Online Privacy Protection Act (COPPA)*, do not extend comprehensive rules to *NPD*.⁴⁶⁰ Individual states like California, through the *California Consumer Privacy Act (CCPA)* and its successor *California Privacy Rights Act (CPRA)*, inch toward broader data rights, though these statutes primarily address

⁴⁵⁸ Office of the Privacy Commissioner of Canada, 'Guidance on the Impact of U.S. Privacy Laws on Canadian Businesses' (2020).

⁴⁵⁹ Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836(b)(1) (2016), <https://www.law.cornell.edu/uscode/text/18/1836>.

⁴⁶⁰ Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-6 (2018); Children's Online Privacy Protection Act, 15 U.S.C. § 6501(1) (2018), <https://www.law.cornell.edu/uscode/text/15/6501>.

personal information.⁴⁶¹ The *Federal Trade Commission (FTC)*, under its consumer-protection mandate, occasionally intervenes in cases involving deceptive data practices, including with respect to inferred or derived data that may fall within the ambit of non-personal classification.⁴⁶² The general laissez-faire approach persists, with data monopolies accruing vast repositories of behavioral and industrial datasets outside stringent public scrutiny.⁴⁶³

China adopts a diametrically opposite posture rooted in state-centric data sovereignty and strategic control over digital infrastructure. The *Data Security Law (DSL)* and the *Cybersecurity Law (CSL)*, along with the *Personal Information Protection Law (PIPL)*, construct a vertically integrated framework wherein non-personal data, especially core and important data, is subject to national-security vetting, export controls, and mandatory localization.⁴⁶⁴ China classifies data according to its relevance to national interest and imposes obligations on enterprises to conduct risk assessments and report incidents involving non-personal but sensitive datasets.⁴⁶⁵ The state maintains prerogative authority over economic, industrial, and scientific data, facilitating access to such repositories for policy formulation, surveillance, and market supervision. This statist orientation is complemented by the country's broader *Digital China* strategy, which envisions a hierarchical data-governance regime administered by central ministries and Party-led committees.⁴⁶⁶ China views *Non-Personal Data* not as a market asset but as a resource imbued with sovereign, economic, and ideological dimensions.

⁴⁶¹ California Consumer Privacy Act, Cal. Civ. Code § 1798.140(h) (2020); California Privacy Rights Act, Cal. Civ. Code § 1798.100 (2023), https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.140.

⁴⁶² Federal Trade Commission, *FTC Enforcement Actions on Deceptive Data Practices*, FTC Bus. Guidance (Feb. 6, 2025), <https://www.ftc.gov/business-guidance/resources/ftc-data-practices-2025>.

⁴⁶³ Lina M. Khan, Amazon's Antitrust Paradox, 126 YALE L.J. 572, 580–83 (2017).

⁴⁶⁴ Data Security Law of the People's Republic of China, art. 21 (2021); Cybersecurity Law of the People's Republic of China, art. 37 (2017); Personal Information Protection Law, art. 3(4) (2021), <http://www.npc.gov.cn/npc/c30834/202106/7c87ef5051f24a5ab4e48a7c164a8d0d.shtml>.

⁴⁶⁵ China Academy of Information and Communications Technology, 'White Paper on Data Security and Governance' (2021).

⁴⁶⁶ State Council of the People's Republic of China, *Digital China Strategy Outline*, State Council Doc. No. 12 (Mar. 15, 2022), <http://www.gov.cn/zhengce/content/2022-03/15/digital-china-strategy.pdf>.

The United Kingdom, post-Brexit, has sought to recalibrate its data-governance regime under the *UK Data Protection Act 2018*⁴⁶⁷ and the *National Data Strategy (2020)*⁴⁶⁸ with renewed emphasis on innovation, public-sector data availability, and fostering private-sector collaboration. While largely aligned with GDPR principles, the UK aims to foster a “pro-growth and trusted data regime” that differentiates itself from the EU’s risk-averse model. Non-personal data, especially from public registers and industrial sources, is seen as an enabler of digital transformation, with initiatives such as the Smart Data Working Group and Open Banking exemplifying sector-specific applications. The regulatory framework lacks a dedicated legislative instrument on *NPD*, relying instead on general competition law, consumer law, and open-government data policies to facilitate access and reuse.

Singapore, renowned for its technocratic governance, has instituted a data-sharing framework anchored in the *Personal Data Protection Act (PDPA)* and guided by the *Model AI Governance Framework*. While the PDPA primarily governs personal data, the *Infocomm Media Development Authority (IMDA)* and the *Smart Nation* initiatives advocate for data interoperability, voluntary sharing, and structured access to non-personal datasets. Singapore’s approach emphasizes trust-by-design, sandboxing, regulatory experimentation, and co-regulatory principles, reflecting a hybrid model that balances market dynamism with regulatory prudence. *Non-Personal Data* in Singapore is framed as a key enabler of artificial intelligence, smart mobility, and e-governance, with state agencies acting both as regulators and facilitators of digital ecosystems.

Japan’s legal treatment of *Non-Personal Data* remains largely inferential, embedded within broader information-governance structures. The *Act on the Protection of Personal Information (APPI)*, as amended, touches upon anonymized and pseudonymized data, while the *Open Data Charter* and various industrial policies promote the use of sensor, machine, and transactional data for economic revitalization. Japan’s *Society 5.0* vision integrates data governance into a human-centered innovation framework, calling for ethical use, transparency, and interoperability of

⁴⁶⁷ Data Protection Act 2018, c. 12, § 2 (UK).

⁴⁶⁸ Dep’t for Science, Innovation & Tech., *National Data Strategy*, GOV.UK (Sept. 9, 2020).

both personal and non-personal datasets.⁴⁶⁹ The absence of a dedicated legal architecture for *NPD* means that much of the governance is operationalized through ministry guidelines, sectoral standards, and collaborative data trusts, such as those piloted by the Cabinet Secretariat.

Brazil, under its *Lei Geral de Proteção de Dados (LGPD)*, has not yet established a granular regime for non-personal data, though the *Brazilian Strategy for Artificial Intelligence* and the *Digital Government Strategy (2020–2022)* recognize its importance for public innovation and digital transformation.⁴⁷⁰ The LGPD applies primarily to identifiable data subjects, and its provisions on anonymization and pseudonymization indirectly affect *NPD* governance.⁴⁷¹ The *National Data Protection Authority (ANPD)* may play a future role in establishing parameters for anonymized data use, especially as Brazil advances its open-data and smart-city initiatives.⁴⁷² As with other Latin American jurisdictions, the tension between innovation, human rights, and regulatory capacity shapes the emerging contours of *NPD* governance.

Canada adopts a cautious, rights-oriented approach with its *Personal Information Protection and Electronic Documents Act (PIPEDA)* and forthcoming *Consumer Privacy Protection Act (CPPA)* emphasizing consent, purpose limitation, and accountability.⁴⁷³ Non-personal data, though not the direct subject of statutory regulation, is increasingly addressed through federal initiatives on open data, artificial intelligence, and public-sector digital transformation.⁴⁷⁴ The *Digital Charter Implementation Act* underscores data mobility, interoperability, and secure data

⁴⁶⁹ Brazilian Strategy for Artificial Intelligence, Decree No. 10.332/2020, art. 3 (Braz.), http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10332.htm (accessed Feb. 10, 2025).

⁴⁷⁰ Lei Geral de Proteção de Dados Pessoais, Law No. 13.709/2018, art. 5(X) (Braz.), http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (accessed Feb. 10, 2025).

⁴⁷¹ Autoridade Nacional de Proteção de Dados, *Guidelines on Anonymized Data Use for Open Data Initiatives*, ANPD Pub. No. 2023/01, at 5–7 (2023), https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2023_guidelines_anonymized_data.pdf (accessed Feb. 10, 2025).

⁴⁷² Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, § 5(3) (Can.), <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/> (accessed Feb. 11, 2025).

⁴⁷³ Innovation, Science and Economic Development Canada, *Canada's Open Data Strategy 2023*, ISED Pub. No. 2023-02, at 10–12 (2023), <https://ised-isde.canada.ca/site/open-data/en/open-data-strategy-2023> (accessed Feb. 12, 2025).

⁴⁷⁴ Digital Charter Implementation Act, 2022, S.C. 2022, c. 10, § 12 (Can.).

sharing, while provincial frameworks offer more stringent governance models.⁴⁷⁵ Canada's regulatory ethos privileges transparency, ethical innovation, and Indigenous data sovereignty, which adds a unique dimension to its treatment of communal or environmental datasets often classified as non-personal.⁴⁷⁶

Australia relies on a multi-pronged legislative scheme involving the *Privacy Act 1988*, the *Consumer Data Right (CDR)* regime, and a robust *Freedom of Information Act*.⁴⁷⁷ The CDR, implemented initially in the banking sector and now expanding into energy and telecommunications, empowers consumers with access and portability rights over data, including de-identified and machine-generated data.⁴⁷⁸ Australia's *Data Availability and Transparency Act 2022* provides a statutory framework for public-sector data sharing, reinforcing trust, security, and efficiency in the management of non-personal data.⁴⁷⁹ Australian regulators such as the *Office of the Australian Information Commissioner (OAIC)* and the *Australian Competition and Consumer Commission (ACCC)* actively monitor data practices, signaling a strong institutional foundation for evolving *NPD* governance.

The legal treatment of *Non-Personal Data* across jurisdictions reveals a fragmented but rapidly maturing domain where competing conceptions of sovereignty, innovation, rights, and market structure shape divergent regulatory choices. The European Union's normative model, China's sovereign control, the United States' market-driven ethos, and intermediary approaches adopted by the UK, Singapore, Japan, Brazil, Canada, and Australia collectively illustrate the complexity of global data governance. A harmonized or interoperable framework remains elusive, necessitating comparative legal scholarship that interrogates these asymmetries while offering pathways toward

⁴⁷⁵ First Nations Information Governance Centre, *Indigenous Data Sovereignty Principles*, FNIGC Policy Doc. (Jan. 15, 2024), <https://fnigc.ca/indigenous-data-sovereignty-principles>.

⁴⁷⁶ *Privacy Act 1988*, No. 119, § 6 (Austl.), <https://www.legislation.gov.au/Details/C2023C00293> (accessed Feb. 11, 2025).

⁴⁷⁷ Office of the Australian Information Commissioner, *Consumer Data Right: De-Identification Guidance*, CDR Priv. Guide 1, 6–8 (2024), <https://www.oaic.gov.au/consumer-data-right/cdr-privacy-guidance>.

⁴⁷⁸ *Data Availability and Transparency Act 2022*, No. 11, § 13 (Austl.), <https://www.legislation.gov.au/Details/C2022A00011>.

⁴⁷⁹ *Id.*

convergence, particularly in cross-border data-flow governance, digital-trade negotiations, and transnational regulatory cooperation.

Scope and Significance

The comparative examination of legal frameworks governing *Non-Personal Data* across nine jurisdictions, comprising the European Union (specifically Germany, France, Finland, and Estonia), the United States, China, the United Kingdom, Singapore, Japan, Brazil, Canada, and Australia, reflects a sophisticated interplay of economic development, geographic dispersion, and cultural-legal traditions, offering a panoramic view of the evolving data-governance ecosystem. The selection has been broadened to include South Korea and Kenya, chosen for their distinctive policy trajectories and complementary relevance. South Korea exemplifies a technologically advanced, innovation-driven digital economy with a structured governance model anchored in legislative sophistication. Kenya represents the African continent's pioneering stance in open data and digital inclusion, reflecting the dynamics of a developing jurisdiction building institutional capacity in data governance. The inclusion of these two nations ensures representation across advanced, emerging, and developing contexts, thus enriching the comparative dimension of this study. These jurisdictions encapsulate a spectrum of regulatory maturity and normative orientation, ranging from highly developed economies with advanced digital infrastructures to emerging economies constructing nascent data-governance frameworks.

The European Union, represented here through the regulatory and policy architectures of Germany, France, Finland, and Estonia, collectively reflects a harmonized supranational structure embedded within the principles of subsidiarity and legal convergence, while simultaneously illustrating the persistence of national idiosyncrasies rooted in divergent administrative cultures, legal traditions, and economic imperatives. Germany and France, as major Western European economies with robust industrial sectors and historically influential legal systems, adopt a structured and rights-conscious approach to non-personal data, aligning closely with the EU's normative commitment to digital constitutionalism, market fairness, and

cross-border interoperability.⁴⁸⁰ Finland and Estonia, from Northern and Eastern Europe respectively, offer insights into the potential of high digital maturity in shaping data regulation that is agile, decentralized, and innovation-driven.

Member States collectively embody the European model of legal integration, one that foregrounds the free movement of *Non-Personal Data* while subjecting it to carefully calibrated public-interest exceptions and sectoral guidelines. This intra-regional diversity within a common legal framework offers a valuable template for supranational data governance, demonstrating the feasibility of normative alignment without erasing national discretion.⁴⁸¹

The United States exemplifies a decentralized, market-led model where *Non-Personal Data* governance is dictated more by economic rationality and sectoral practices than by coherent legislative codification. As an economically liberal jurisdiction, the U.S. legal order privileges private ownership, contractual autonomy, and tort-based redress mechanisms, resulting in a fragmented regulatory landscape where non-personal data, especially anonymized, aggregated, and industrial datasets, is treated as a commodity subject to minimal public oversight.⁴⁸² This model operates within a broader cultural context characterized by skepticism toward centralized regulation, strong free speech protections, and a deep-rooted belief in self-regulation and technological exceptionalism. It presents a paradigmatic counterpoint to the European approach, foregrounding the challenges of reconciling individual rights, innovation, and competition in an environment dominated by powerful private data controllers.

The United Kingdom, though previously aligned with the EU data-governance framework, is now recalibrating its national legal apparatus to promote a “pro-innovation” digital regime that seeks to balance regulatory coherence with strategic

⁴⁸⁰ European Commission, *European Data Act: Harmonised Rules for Fair Access and Use of Data*, Regulation (EU) 2023/2854, art. 1, 2023 O.J. (L 2854) 1, 3–5, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854>.

⁴⁸¹ European Commission, *Data Governance Act: A Framework for Data Sharing*, Regulation (EU) 2022/868, art. 3, 2022 O.J. (L 152) 1, 4–6, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>.

⁴⁸² Lina M. Khan, Amazon's Antitrust Paradox, 126 YALE L.J. 572, 580–83 (2017).

divergence.⁴⁸³ As a common law jurisdiction with strong administrative and judicial institutions, the UK model reflects a blend of rights-based protection and market facilitation, drawing upon both its historical commitment to the rule of law and its contemporary aspiration to position itself as a global digital leader in the post-Brexit era.

These jurisdictions span multiple continents and reflect diverse regional digital priorities. North America, represented by the United States and Canada, illustrates divergent philosophies within a shared geographic and economic context. While the U.S. maintains a libertarian, industry-led framework, Canada leans toward a more precautionary, rights-oriented model grounded in statutory accountability and public-interest safeguards.⁴⁸⁴ Canadian data governance with regard to non-personal datasets reflects a commitment to transparency, ethical use, and Indigenous data sovereignty, elements that are largely absent in the American discourse.

From the Asia-Pacific region, Singapore and Japan represent two technologically advanced yet culturally distinct approaches to *Non-Personal Data* regulation.⁴⁸⁵ Singapore, operating under a technocratic governance model, embraces a co-regulatory approach wherein the state acts both as regulator and innovator.⁴⁸⁶ Its legal framework is designed to promote trust, interoperability, and voluntary compliance, reflecting a governance culture that prioritizes efficiency, responsiveness, and public-private collaboration. Japan, with its civil law tradition and societal emphasis on harmony and consensus, adopts a soft-law approach to non-personal data, relying on policy frameworks, administrative guidance, and ethical principles rather than binding legal norms. Both jurisdictions illustrate the potential of culturally contextualized governance in fostering innovation without compromising accountability.

⁴⁸³ Dep't for Science, Innovation & Tech., *UK Data Reform Bill: Advancing a Pro-Innovation Data Economy*, GOV.UK, at 3–5 (Dec. 5, 2024), <https://www.gov.uk/government/publications/data-reform-bill-2024>.

⁴⁸⁴ U.S. Department of Commerce, 'Data Privacy Framework Principles and Implementation Guide' (2025).

⁴⁸⁵ Japan, *Basic Act on the Advancement of Public and Private Sector Data Utilization*, Act No. 103 of 2016, art. 2, <https://www.japaneselawtranslation.go.jp/en/laws/view/3724>.

⁴⁸⁶ Personal Data Protection Commission, *Singapore's Data Sharing Framework: Co-Regulatory Model*, PDPC Policy Doc. No. 2023/02, at 3–5 (2023), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/data-sharing-framework-2023.pdf>.

South Korea follows a rights-oriented yet innovation-driven approach to data governance. Its framework, supported by the *Data Industry Promotion Act* and amendments to the *Personal Information Protection Act (PIPA)*, distinguishes between personal, pseudonymized, and non-personal data. Balancing privacy with technological growth, South Korea promotes secure data utilization for AI and industry while maintaining strict oversight, reflecting a hybrid model between Japan's ethical governance and Singapore's regulatory pragmatism.

China, as a representative of a non-Western, state-centric model, diverges sharply from liberal democratic jurisdictions.⁴⁸⁷ Its legal architecture concerning *Non-Personal Data* is anchored in the doctrines of data sovereignty, national security, and state supremacy. Rather than treating data as a private asset or public good, China categorizes and controls *Non-Personal Data* according to its strategic significance, subjecting it to rigid localization, export restrictions, and mandatory state access requirements. The Chinese model reflects a deeply hierarchical, centralized governance culture where digital infrastructure is viewed as an extension of state power. This approach is rooted in a broader political philosophy that prioritizes collective security, surveillance capacity, and industrial policy over individual autonomy or market competition.

Brazil, representing Latin America, occupies an intermediary position combining elements of rights-based regulation with developing institutional capacity. Brazil's emerging framework reflects both the aspiration to align with global standards and the constraints imposed by regulatory fragmentation, limited enforcement, and infrastructural gaps. While its legislative instruments address personal data comprehensively, the governance of *Non-Personal Data* remains fluid, shaped largely by national development goals, open data strategies, and evolving administrative practice.

Australia, situated in Oceania, demonstrates a hybrid legal system that integrates elements of the common law tradition, public-sector accountability, and competitive

⁴⁸⁷ Data Security Law of the People's Republic of China, art. 21 (2021), <http://www.npc.gov.cn/npc/c30834/202106/7c87ef5051f24a5ab4e48a7c164a8d0d.shtml>.

neutrality.⁴⁸⁸ Its regulatory apparatus includes specific statutory mandates for consumer data portability, public-sector data sharing, and freedom of information, all of which directly or indirectly pertain to *Non-Personal Data* governance. Australia's regulatory posture, while innovation-friendly, is also underpinned by strong institutional oversight and a culture of public trust.

Kenya represents the African perspective, emphasizing open data and digital inclusion as tools for development. Through initiatives like the *Kenya Open Data Initiative (KODI)* and the *Data Protection Act, 2019*, the country encourages the ethical use of anonymized and aggregated datasets to support governance, innovation, and economic planning. Kenya's emerging framework integrates transparency and accessibility, positioning data as a public resource for national growth and social equity.

The inclusion of jurisdictions from Western Europe (Germany, France), Northern Europe (Finland), Eastern Europe (Estonia), North America (United States, Canada), Latin America (Brazil), Asia (China, Japan, Singapore, South Korea), Oceania (Australia), and Africa (Kenya) ensures comprehensive global coverage, allowing for a holistic analysis of cross-jurisdictional tensions, complementarities, and interdependencies. This geographical dispersion not only captures regulatory diversity but also highlights the distinct roles that data plays in national development strategies, reflecting how differing legal traditions, economic priorities, and governance philosophies shape the evolving global framework for Non-Personal Data.

The selected jurisdictions embody a dichotomy between Western democratic traditions and non-Western models of governance. The Western jurisdictions, comprising the European Union, the United States, the United Kingdom, Canada, and Australia, share foundational commitments to the rule of law, individual autonomy, separation of powers, and institutional accountability. These normative values shape their data-governance frameworks, resulting in legislation that often balances economic incentives with privacy rights, procedural fairness, and public-interest considerations.

⁴⁸⁸ Office of the Australian Information Commissioner, *Consumer Data Right: Governance and Accountability Framework*, CDR Priv. Guide 2, 4–6 (2024), <https://www.oaic.gov.au/consumer-data-right/cdr-governance-framework>.

Non-Western jurisdictions such as China, Singapore, Japan, South Korea, Brazil, and Kenya illustrate a range of alternative regulatory philosophies.⁴⁸⁹ China represents the most pronounced form of state-centric control, while Singapore adopts a technocratic approach focused on efficient governance.⁴⁹⁰ Japan emphasizes ethical harmonization and societal consensus, and South Korea balances strong privacy protection with innovation-driven policies under a rights-conscious yet state-coordinated model. Brazil reflects a hybridized framework influenced by civil law traditions and global digital norms, whereas Kenya embodies an emerging, development-oriented approach that integrates open data principles with socio-economic inclusion. These cultural distinctions manifest in the structure, orientation, and enforcement of legal frameworks governing non-personal data.

The Western commitment to democratic oversight and adversarial legalism contrasts with the top-down, consensus-driven, or developmentalist logic that animates non-Western regimes. The governance of *Non-Personal Data* cannot be extricated from the broader political, cultural, and institutional matrices within which it is embedded. The comparative study of these jurisdictions not only exposes the multiplicity of regulatory models but also underscores the normative fault lines that define the future of global data governance. Mutual recognition or pluralist coexistence in equitable legal frameworks for *Non-Personal Data* remains an imperative of both legal and policy significance in the digital age.

Regulatory Innovation

Regulatory innovation in the governance of *Non-Personal Data* has gained significant traction across jurisdictions as states and regional blocs strive to balance economic competitiveness, digital sovereignty, and rights protection in an increasingly data-driven global economy.

⁴⁸⁹ Douglas W. Arner et al., The Transnational Data Governance Problem, 37 BERKELEY TECH. L.J. 623, 625–27 (2023).

⁴⁹⁰ Data Security Law of the People's Republic of China, art. 21 (2021), <http://www.npc.gov.cn/npc/c30834/202106/7c87ef5051f24a5ab4e48a7c164a8d0d.shtml> (establishing China's state-centric data governance); Personal Data Protection Commission, *Singapore's Data Sharing Framework: Co-Regulatory Model*, PDPC Policy Doc. No. 2023/02, at 3–5 (2023), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/data-sharing-framework-2023.pdf>.

In the European Union, the *Data Governance Act* and the *Data Act* collectively constitute an advanced regulatory architecture intended to foster a single European data space, strengthen trust in data sharing, and create a harmonized framework for access to both personal and non-personal data.⁴⁹¹ Japan has emerged as a leader in advocating for trusted data flows under its “*Data Free Flow with Trust*” (DFFT) principle. Embedded within both domestic policy and Japan’s leadership in multilateral forums such as the G7 and OECD, DFFT seeks to operationalize interoperability across jurisdictions by promoting cross-border data flows anchored in shared principles of trust, security, and reciprocity. Japan’s digital exports and cross-border cloud services now constitute a growing share of its GDP, with non-personal industrial data sharing forming the backbone of smart manufacturing initiatives under *Society 5.0*.⁴⁹²

China represents a contrasting regulatory model grounded in centralized data sovereignty and national-security imperatives. The *Data Security Law*, in conjunction with the *Cybersecurity Law* and the *Personal Information Protection Law*, classifies data into categories such as “important” and “core,” with corresponding restrictions on export and mandatory localization requirements. Industrial datasets ranging from supply-chain logistics to AI-training data are treated as strategic national resources.⁴⁹³ In 2023, China’s Ministry of Industry and Information Technology estimated the domestic data economy to be worth over ¥9 trillion (approximately USD 1.3 trillion), with *Non-Personal Data* accounting for more than 60% of industrial use cases. The Chinese model, while state-centric, has spurred significant investment in national data centers, data exchanges, and government-controlled data markets.⁴⁹⁴

Singapore’s regulatory innovation is manifested in its *Smart Nation* strategy, which integrates open-government data, AI governance, and sectoral data partnerships under

⁴⁹¹ European Commission, *Data Governance Act: A Framework for Data Sharing*, Regulation (EU) 2022/868, art. 3, 2022 O.J. (L 152) 1, 4–6, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>.

⁴⁹² Japan, *Basic Act on the Advancement of Public and Private Sector Data Utilization*, Act No. 103 of 2016, art. 2, <https://www.japaneselawtranslation.go.jp/en/laws/view/3724>.

⁴⁹³ Data Security Law of the People’s Republic of China, art. 21 (2021), <http://www.npc.gov.cn/npc/c30834/202106/7c87ef5051f24a5ab4e48a7c164a8d0d.shtml>.

⁴⁹⁴ China Communications Industry Ass’n Data Center Comm., *China Data Center Market Report 2024–2025*, at 10–12 (2024), <https://www.ccia.org.cn/data-center-report-2024>.

a centralized coordination regime led by the Smart Nation and Digital Government Office.⁴⁹⁵ The *Infocomm Media Development Authority (IMDA)* has reported that structured data sharing between government and industry has generated over SGD 6 billion in annual economic value, driven largely by *Non-Personal Data* applications in transportation, energy, and health-tech sectors.⁴⁹⁶

Brazil's *Lei Geral de Proteção de Dados (LGPD)*, while primarily focused on personal data, has catalyzed broader discourse on *Non-Personal Data* governance. Brazil's *National Data Strategy* includes open-data frameworks, industrial data reuse guidelines, and pilot projects on federated learning, all critical in a country where over 70% of industrial innovation relies on real-time analytics, much of which involves *Non-Personal Data* streams. Brazil's data economy is projected to reach R\$300 billion by 2026, with public-private data collaborations playing a central role in sectors such as agri-tech and fintech.⁴⁹⁷

The United Kingdom, in the post-Brexit regulatory environment, is pursuing a distinct data strategy that emphasizes economic growth, digital trade, and regulatory agility. The UK's Department for Science, Innovation and Technology has launched initiatives to establish data adequacy agreements, liberalize data-sharing regimes, and invest in AI regulatory sandboxes. As of 2024, the UK's data economy contributes over £150 billion to national output, with the non-personal component, particularly in logistics, fintech, and health analytics, growing at over 8% annually.⁴⁹⁸

Canada's *Digital Charter*, grounded in the values of control, transparency, and data mobility, promotes innovation while upholding public trust. The *Consumer Privacy Protection Act* and the *Data Commissioner's Office* mark steps toward institutionalizing rights-based governance while enabling secure data sharing between sectors. Canada's data economy, now worth an estimated CAD 210 billion annually,

⁴⁹⁵ Smart Nation & Digital Gov't Off., *Smart Nation 2.0: Digital Infrastructure and AI Governance*, Gov't of Sing. Press Release (2023), <https://www.smartnation.gov.sg/smart-nation-2-0>.

⁴⁹⁶ Infocomm Media Dev. Auth., *Digital Economy Framework for Action*, at 15–17 (2023), <https://www.imda.gov.sg/-/media/imda/files/sg-digital/sgd-framework-for-action.pdf>.

⁴⁹⁷ International Data Corporation (IDC), 'Brazil Data Center Market Forecast 2025–2030'.

⁴⁹⁸ Dep't for Sci., Innovation & Tech., *Economic Estimates: Digital Sector Annual Gross Value Added (2019–2023)*, GOV.UK (Mar. 6, 2025), <https://www.gov.uk/government/statistics/economic-estimates-digital-sector-annual-gross-value-added-2019-to-2023>.

relies heavily on industrial data use in natural resource management, telecommunications, and AI development.⁴⁹⁹ Canada also integrates Indigenous data-sovereignty principles, acknowledging the rights of First Nations to control non-personal cultural and ecological data.

Australia, through its *Consumer Data Right (CDR)* regime, offers one of the most advanced legislative models for user-empowered data portability, initially applied in banking and now extended to energy and telecommunications. The *Data Availability and Transparency Act* has further institutionalized mechanisms for public-sector data sharing, facilitating interoperability and trust. Australia's Treasury estimates that data portability and availability could contribute over AUD 20 billion in economic benefits over the next decade.⁵⁰⁰

Across jurisdictions, participation in global and regional policy forums such as the G7, G20, OECD, ASEAN, and WTO amplify the influence of these domestic regulatory innovations. The EU, Japan, and Canada continue to advocate for multilateral frameworks based on transparency, rule of law, and technical interoperability. China, by contrast, promotes cyber-sovereignty principles at venues such as the Shanghai Cooperation Organization and BRICS. ASEAN, with Singapore as a key driver, is experimenting with cross-border data-transfer mechanisms through model contractual clauses and regional certification schemes.

These engagements collectively reflect an emerging consensus that *Non-Personal Data* governance cannot be confined within national borders but must be shaped through a combination of domestic innovation and transnational alignment.

4.2 Conceptual Framework for *Non-Personal Data* Regulation

The regulation of *Non-Personal Data (NPD)* has emerged as a critical dimension of digital governance, reflecting the transition from a personal-data-centric framework to one that recognizes the economic, strategic, and sovereign implications of

⁴⁹⁹ Innovation, Sci. & Econ. Dev. Canada, *Digital Economy Strategy 2023*, ISED Pub. No. 2023-02, at 12–14 (2023), <https://ised-isde.canada.ca/site/open-data/en/open-data-strategy-2023>.

⁵⁰⁰ Treasury, *Australian Data Strategy*, Treasury.gov.au (2022), https://treasury.gov.au/publication/p2021-231824_1.pdf.

anonymized, industrial, and machine-generated datasets.⁵⁰¹ A conceptual framework for understanding this domain must account for the legal status of *NPD*, its classification, ownership, access, reusability, portability, and cross-border transfer mechanisms. Across jurisdictions, *NPD* regulation operates along multiple axes, including constitutional values, economic strategy, technological capacity, public-private partnerships, and geopolitical interests.

The European Union's approach, articulated through instruments such as the Free Flow of *Non-Personal Data* Regulation, the Open Data Directive, the Data Governance Act (DGA), and the Data Act, establishes a rights-respecting and interoperable regulatory ecosystem premised on legal certainty, trust, and public value.⁵⁰² Within the EU, Germany anchors its model in industrial competitiveness by leveraging data spaces and sector-specific data trustees. France embraces data as a public asset, emphasizing open government and innovation through the strategic reuse of public sector information. Finland and Estonia, both digitally advanced, integrate *NPD* regulation within e-governance and digital identity frameworks, prioritizing decentralization, transparency, and technical interoperability.⁵⁰³ The EU's conceptualization is grounded in fundamental rights, internal market logic, and data sovereignty, making its framework integrative and normative.

In the United States, regulation is primarily market driven, relying on torts, contracts, trade secret protection, and sector-specific statutes. The National Institute of Standards and Technology (NIST) and other federal agencies offer voluntary standards for data interoperability and anonymization, while states such as California introduce nascent rules on data portability and consumer rights that indirectly impact *NPD* practices. The US model conceptualizes *NPD* as proprietary capital, privileging private ownership and commercialization over state stewardship.

⁵⁰¹ Nadezhda Purtova & Gijs van Maanen, *Data as an Economic Good, Data as a Commons, and Data Governance*, arXiv (Dec. 20, 2022), <https://arxiv.org/abs/2212.10244>.

⁵⁰² European Commission, *Data Governance Act Explained*, Shaping Europe's Dig. Future (June 15, 2023), <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained>.

⁵⁰³ National Institute of Standards and Technology, *NIST Big Data Interoperability Framework*, NIST Special Pub. 1500-1r2, at 10–12 (2021), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1r2.pdf>.

In China, the Data Security Law (DSL) and the Personal Information Protection Law (PIPL), along with cyber sovereignty doctrines, frame *NPD* as a strategic national asset. The state reserves the right to control and classify non-personal datasets, particularly those deemed important or core, and mandates localization, risk assessment, and national security reviews. China's approach is statist, centralized, and security focused, embedding data regulation within a broader framework of industrial policy, social governance, and global influence.

The United Kingdom's post-Brexit data strategy departs from the EU's rights-based orientation and leans toward innovation-driven governance.⁵⁰⁴ While aligning with existing data protection principles, the UK seeks to reduce burdens on data controllers, expand public-private collaboration, and facilitate cross-border flows with trusted partners. *NPD* governance in the UK forms part of broader digital transformation and AI readiness goals, relying on policy documents, institutional guidance, and soft-law instruments rather than codified legislation.

Singapore's model exemplifies regulatory agility, with the Smart Nation initiative promoting the use of *NPD* for economic growth, urban planning, and public service optimization. While personal data is governed by the Personal Data Protection Act (PDPA), *Non-Personal Data* remains within the purview of collaborative data-sharing frameworks, including the Singapore Data Exchange and sectoral sandboxes. The state acts as both regulator and facilitator by enabling access through trusted data intermediaries and voluntary data trusts.

Japan's strategy is rooted in its vision of *Society 5.0* and *Data Free Flow with Trust (DFFT)*. It promotes interoperability, decentralization, and ethical use of data, emphasizing open government and public-private innovation. Although formal legislation on *NPD* remains limited, Japan advances its conceptual model through high-level policy guidance, cross-border cooperation, and global norm-setting at the G7 and WTO levels.

⁵⁰⁴ Dep't for Science, Innovation & Tech., *UK Digital Strategy*, GOV.UK (Feb. 15, 2022), <https://www.gov.uk/government/publications/uk-digital-strategy>.

South Korea presents a hybrid governance framework combining strong privacy safeguards with an innovation-oriented digital strategy. Guided by the *Data Industry Promotion Act* and amendments to the *Personal Information Protection Act (PIPA)*, its model encourages the use of anonymized and machine-generated data for industrial advancement while maintaining strict accountability standards. The country's "MyData" initiative exemplifies user-centric data control, while national data platforms promote secure sharing across government and industry. South Korea's regulatory posture thus reflects a balance between Japan's ethical governance and Singapore's pragmatic, state-facilitated approach, reinforcing trust-based data utilization as a driver of digital growth.

Brazil's *General Data Protection Law (LGPD)* contains limited provisions on *NPD*, treating anonymized data as outside its primary scope yet subject to regulation in the event of re-identification risk. National strategies, including the *Brazilian Strategy for Digital Transformation* and the role of the *National Data Protection Authority (ANPD)*, indicate an evolving governance framework that balances innovation with public oversight.

Canada, grounded in constitutional federalism and Indigenous data sovereignty principles, adopts a cautious and consensus-driven approach to *NPD*. The Digital Charter Implementation Act and other instruments envision a trusted ecosystem for data governance, integrating the rights of communities, transparency obligations for data custodians, and interoperability protocols.

Australia operationalizes its *NPD* governance through the *Consumer Data Right (CDR)*, a legislative framework that empowers consumers to direct the use and transfer of their data across sectors such as banking, energy, and telecommunications. Although primarily designed for personal data, CDR establishes a transferable architecture that supports *NPD* portability, sectoral open access, and informed consent. Australia's Data Availability and Transparency Act facilitate government data sharing for research and

policy development, embedding strong safeguards and privacy-by-design principles.⁵⁰⁵

Kenya, representing the African continent, advances a development-oriented data governance model anchored in transparency, inclusion, and innovation. Through frameworks like the *Data Protection Act, 2019* and the *Kenya Open Data Initiative (KODI)*, the country promotes open access to anonymized and aggregate datasets for governance, entrepreneurship, and research. Kenya's approach integrates data as both a public resource and a tool for socio-economic empowerment, reflecting a strong commitment to digital equity and participatory governance. Its evolving regulatory landscape positions it as a key voice for the Global South in shaping equitable, rights-based, and sustainable Non-Personal Data governance.

Across these jurisdictions, divergent conceptualizations of NPD emerge, ranging from sovereign resource to economic asset, and from public good to private commodity. These models are shaped by constitutional structures, economic strategies, institutional maturity, and technological readiness. The European model aligns with a data democracy paradigm, emphasizing governance, accountability, and cross-border coherence.⁵⁰⁶ The American approach reflects liberal market traditions, prioritizing innovation, entrepreneurship, and minimal state interference.⁵⁰⁷ China's vision is anchored in cyber-statism and strategic control, while Japan, South Korea, and Singapore pursue middle-ground paths rooted in ethical innovation, technological advancement, and digital diplomacy. The United Kingdom, Brazil, Canada, Australia, and Kenya add further nuance, experimenting with hybrid frameworks that combine public-interest regulation with developmental and market incentives. Collectively, these jurisdictions offer a pluralistic yet fragmented global landscape for NPD governance. Their participation in forums such as the G7, G20, OECD, ASEAN, African Union, and WTO continue to shape emerging norms surrounding data

⁵⁰⁵ Office of the Nat'l Data Comm'r, *Introducing the DATA Scheme*, DataComm'r.gov.au (Jan. 15, 2024), <https://www.datacommissioner.gov.au/the-data-scheme>.

⁵⁰⁶ Paul M. Schwartz, *The European Data Privacy Directive and the U.S. Debate on Privacy in the Global Economy*, 112 YALE L.J. 697, 702–05 (2003).

⁵⁰⁷ Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1885–88 (2013).

localization, interoperability, algorithmic accountability, and equitable cross-border data flow.

A conceptual framework must recognize *NPD* as a legal category in evolution, interfacing with data protection law, competition law, trade law, intellectual property, and administrative governance. It must also accommodate hybrid governance models that incorporate co-regulation, standardization, and multi-stakeholder stewardship. Going forward, the key challenge lies in crafting interoperable legal architectures that respect domestic priorities while enabling transnational data collaboration. This requires embedding principles of trust, transparency, accountability, and reciprocity into global digital governance frameworks. *NPD* regulation is not merely a technical or commercial exercise but a legal and normative undertaking that redefines the relationship between data, the state, the market, and the individual in the twenty-first century.

4.2.1 Definition and Importance

“Non-Personal Data (NPD), encompassing anonymized datasets, aggregated information, machine-generated data such as that produced by Internet of Things (IoT) devices, and industrial data derived from manufacturing analytics, represents an emerging category within the global data governance ecosystem.” Unlike comprehensive regulatory frameworks such as the *General Data Protection Regulation (GDPR)* in the European Union or the *Personal Information Protection Law (PIPL)* in China, *NPD* operates within a comparatively underdeveloped and fragmented regulatory environment.

This legal gap presents distinct challenges in balancing innovation, competition, and public interest with safeguards against potential re-identification risks or data concentration.⁵⁰⁸ The economic utility of *NPD* is significant, serving as a foundation for advanced technologies including artificial intelligence, autonomous systems, and data analytics. In the context of smart infrastructure, for example, real-time traffic optimization depends on anonymized mobility data generated by IoT sensors, while

⁵⁰⁸ Michèle Finck & Frank Pallas, *They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data Under the GDPR*, 10 INT’L DATA PRIV. L. 11, 11–13 (2020).

precision farming uses environmental and geospatial datasets to enhance productivity and sustainability. Industrial applications similarly rely on anonymized sensor data for predictive maintenance, reducing downtime and improving efficiency.⁵⁰⁹

However, the fluid boundary between personal and non-personal data, given technological capabilities that may permit re-identification, underscores the importance of robust anonymization protocols, sector-specific safeguards, and legally enforceable accountability frameworks.⁵¹⁰ The absence of harmonized international norms governing *NPD* sharing, portability, and commercial use further exacerbates legal uncertainty, particularly in cross-border contexts.⁵¹¹ As countries seek to leverage *NPD* for economic growth, digital infrastructure, and public governance, coherent, principle-based legal instruments are required to ensure that the benefits of *Non-Personal Data* are realized equitably, securely, and transparently.

NPD, although not subject to the same protections as personal data, plays a central role in modern public sector governance. It supports transformative applications across domains such as public administration, epidemiology, environmental regulation, urban planning, and service delivery. Open government data platforms, for instance, rely on the structured dissemination of *NPD* to enhance transparency, promote civic engagement, and stimulate private innovation through reuse. Urban planning authorities employ aggregated, anonymized geospatial data to model population density, infrastructure needs, and environmental stressors. Similarly, anonymized epidemiological datasets aid in public health surveillance, pandemic response, and resource allocation.

The conceptual and practical governance of *NPD*, however, is complicated by its ontological fluidity. Datasets that appear non-personal may become personal through re-identification, especially when cross-referenced with other data sources.

⁵⁰⁹ Covington & Burling LLP, *EU Rules Restricting the International Transfers of Non-Personal Data*, Inside Priv. (Feb. 1, 2024), <https://www.insideprivacy.com/eu-data-protection/eu-rules-restricting-non-personal-data-transfers> (accessed Nov. 10, 2025).

⁵¹⁰ WIPO, *Regulating Machine Data: Less Is More for Global Growth*, WIPO Mag. (June 2023), https://www.wipo.int/wipo_magazine/en/2023/02/article_0003.html.

⁵¹¹ United Nations Conference on Trade and Development, *Digital Economy Report 2021: Cross-Border Data Flows and Development*, UNCTAD/DER/2021, at 45–48 (2021), https://unctad.org/system/files/official-document/der2021_en.pdf.

Conversely, personal data can become non-personal through anonymization or aggregation, though with varying reliability. This duality challenges the binary distinction upon which traditional data protection laws are built, necessitating nuanced regulatory approaches that acknowledge the continuum between personal and non-personal data.

Effective governance mechanisms must incorporate technical, legal, and organizational safeguards to mitigate re-identification risks in accordance with accountability and proportionality principles. Further complexity arises in cross-border transfers, where *NPD* traverses jurisdictions lacking harmonized standards for data classification, access rights, and oversight. The absence of multilateral frameworks contributes to fragmentation and uncertainty, impeding innovation and collaboration.⁵¹² Divergent national approaches, rooted variously in market liberalism, state control, or public interest paradigms, result in conflicting norms on sharing, localization, and stewardship.

Domestically, *NPD* regulation must balance three competing objectives: encouraging economic use, ensuring public benefit⁵¹³, and preventing concentration of control. While frameworks should enable lawful commercial exploitation, excessive commodification risks informational asymmetry and reduced competition.⁵¹⁴ Regulatory strategies to address these risks include mandatory data-sharing obligations for designated gatekeepers, fair access requirements for public interest datasets, and neutral data intermediaries or trusts to ensure equity.

Safeguards are essential to prevent privacy violations or discriminatory outcomes.⁵¹⁵ This involves embedding privacy-by-design principles in open-data infrastructures, enforcing purpose limitation, and maintaining audit trails. Ethical governance, based on transparency, inclusivity, and accountability, should guide decisions on which *NPD*

⁵¹² Ayesha Khan, Submission to the Ministry of Electronics and Information Technology, Government of India, on the Draft Non-Personal Data Framework, YALE L. SCH. (Sept. 16, 2020).

⁵¹³ Douglas W. Arner et al., The Transnational Data Governance Problem, 37 BERKELEY TECH. L.J. 623, 625–27 (2023).

⁵¹⁴ Milton L. Mueller & Karim Farhat, Regulation of Platform Market Access by the United States and China: Neo-Mercantilism in Digital Services, 14 POL'Y & INTERNET 305, 307–09 (2022).

⁵¹⁵ Milton L. Mueller, *Asia and Digital Neo-Mercantilism*, Hinrich Found. (Sept. 14, 2022), <https://www.hinrichfoundation.com/research/article/digital-economy/asia-digital-neo-mercantilism>.

categories may be openly shared and under what conditions. Certain categories, such as environmental or traffic data, may be broadly accessible, while sensitive datasets, such as those related to justice or vulnerable demographics, require restrictive handling.

Equity and inclusion are central. Regulatory frameworks must ensure that marginalized or underrepresented groups benefit from *NPD*-driven policies. Legal systems should also acknowledge Indigenous data sovereignty, recognizing that some collective datasets possess cultural or historical significance beyond economic value.⁵¹⁶ Governments may adopt a combination of statutory, co-regulatory, and soft-law mechanisms to balance these concerns. Dedicated oversight bodies, supported by capacity-building initiatives, can coordinate policy, resolve disputes, and ensure accountability.⁵¹⁷

Ultimately, the governance of *NPD* in the public sector represents both a challenge and an opportunity: to reimagine public value in the digital age, where data serves not only as an economic asset but also as an infrastructure for collective progress and equitable development.

4.2.2 Analytical Framework

A comparative evaluation of global approaches to *Non-Personal Data* governance requires a multidimensional analytical framework comprising four interrelated dimensions, each corresponding to a core governance challenge.

Legal Definition or Concept

Clarity in definition is fundamental to the scope, applicability, and interoperability of regulatory regimes. Jurisdictions differ widely in their conceptualization of *NPD*. The European Union's Data Governance Act, for instance, explicitly defines *NPD* as data outside the scope of the GDPR, encompassing aggregated, anonymized, and industrial datasets. This distinction reinforces a dual regime, personal and non-personal, while

⁵¹⁶ European Commission, *Free Flow of Non-Personal Data*, Shaping Europe's Dig. Future (Dec. 16, 2024), <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data>.

⁵¹⁷ Arindrajit Basu, *The Case for Interoperable Data Governance in India*, Internet Freedom Foundation (2022).

extending oversight beyond traditional privacy boundaries. The United States adopts a more fragmented approach, where “*non-personally identifiable information*” is addressed in sector-specific statutes and agency guidance. The absence of a unified definition in the US undermines consistency and complicates cross-border data governance.

In this thesis, the term “concept” of *Non-Personal Data* is employed to describe the broader theoretical and policy-oriented understanding of data that is not linked to identifiable individuals, encompassing its societal value, economic potential, and governance challenges. The term “definition”, however, is used in the legal sense, referring to formal descriptions articulated in statutory or regulatory instruments. The dual usage reflects a methodological distinction: while conceptual understanding forms the foundation for exploring the nature and purpose of *NPD*, legal definitions establish the operational boundaries within which governance frameworks are constructed.

Governance Framework

Institutional and procedural architectures differ markedly across jurisdictions. In China, a centralized authority governs both personal and non-personal data, prioritizing national security and localization. In Brazil, the *General Data Protection Law (LGPD)* extends partially to *NPD* under the oversight of a national data authority, though enforcement remains uneven. Germany’s hybrid model, demonstrated through the Gaia-X initiative, promotes federated, secure, and interoperable data sharing, combining innovation with regulatory compliance.⁵¹⁸ These variations highlight distinct policy priorities, China’s emphasis on sovereignty, Brazil’s on harmonization, and Germany’s on multi-stakeholder collaboration.

Key Features

Certain jurisdiction-specific innovations offer models for global norm development. Japan’s “*Data Free Flow with Trust*” (*DFFT*) framework promotes cross-border data

⁵¹⁸ Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Policy Rules and Architecture of Standards*, at 12–15 (2024), <https://gaia-x.eu/sites/default/files/2024-01/Gaia-X-Policy-Rules-Architecture-2024.pdf>.

movement grounded in mutual trust and compatibility. Similarly, Singapore's Smart Nation initiative integrates ethical data governance with public-private collaboration, while the EU's Data Act seeks to establish equitable data access and reuse standards.⁵¹⁹

Challenges

Persistent structural and operational barriers impede coherence and effectiveness. In the United States, the absence of a centralized data protection law results in fragmented enforcement and regulatory inconsistency. Brazil faces institutional constraints, including limited resources for oversight. Cross-border restrictions imposed under data sovereignty or national security pretexts also hinder interoperability. Such measures, though aimed at safeguarding domestic interests, risk fostering digital protectionism and constraining innovation. Balancing sovereign data control with transnational collaboration thus remains a defining challenge for *NPD* governance.

4.2.3 Theoretical Lens

The comparative analysis of *Non-Personal Data* governance draws upon three interrelated theoretical perspectives: public good, digital sovereignty, and economic incentive.

Under the *public good* perspective, *NPD* such as anonymized or open government datasets is non-excludable and non-rivalrous, retaining value regardless of usage. This perspective supports policies that mandate or facilitate open access to data serving collective purposes, such as environmental monitoring, transport optimization, and public health.

The *digital sovereignty* perspective emphasizes state authority over data infrastructure and flows.⁵²⁰ Frameworks like the EU's federated data spaces embody this approach, ensuring alignment with national values and security priorities, even if such alignment complicates interoperability.

⁵¹⁹ Anupam Chander & Haochen Sun, *Sovereignty 2.0: The Global Governance of Data Flows*, 64 VA. J. INT'L L. 1 (2024).

⁵²⁰ Rohini Mariappan, *India Releases Aadhaar's Non-Personal Data for Public Research*, *Econ. Times* (June 5, 2025), at B4, <https://economictimes.indiatimes.com/tech/technology/aadhaar-non-personal-data-2025>.

The *economic incentive* perspective views *NPD* as a strategic, monetizable resource.⁵²¹ Legal regimes employ instruments such as standardized interfaces, fair access obligations, and sectoral sharing mandates to stimulate innovation and competition while safeguarding proprietary interests.

These three lenses collectively highlight the normative trade-offs in *NPD* regulation: openness versus control, innovation versus oversight, and national autonomy versus global integration. They provide a foundation for evaluating how legal systems evolve to manage the complex intersections of technology, law, and governance.

4.2.4 Global Context

The governance of *Non-Personal Data* unfolds within a fragmented global order shaped by divergent geopolitical, economic, and normative priorities. A prominent trend is data localization, wherein states such as China require that sensitive or “core” data be stored and processed domestically to protect national security and sovereignty. Conversely, initiatives such as Japan’s *Data Free Flow with Trust (DFFT)* champion liberalized cross-border data transfers grounded in mutual assurance and interoperability.

In contrast, open data initiatives enhance transparency and civic participation through the systematic release of government-held *NPD*.⁵²² Countries such as Australia, Canada, and members of the European Union, notably Estonia through its X-Road digital infrastructure, enable secure and interoperable inter-agency sharing that supports public service delivery and democratic accountability.

Sector-specific frameworks also shape the landscape. France’s central health data platform facilitates controlled access for research, Brazil’s open banking regime mandates data portability to promote competition, and Germany’s Gaia-X project develops secure industrial data collaboration through federated architecture.

In the absence of a harmonized global framework comparable to the GDPR, *NPD* governance remains fragmented, characterized by inconsistent definitions and

⁵²¹ OECD, ‘Data Localization and Sovereignty: Balancing Trade and Security’ (2023).

⁵²² *Autoridade Nacional de Proteção de Dados (ANPD)*, ‘Enforcement Report on Data Violations 2023’.

compliance expectations. This diversity, while reflecting national autonomy, undermines predictability and complicates innovation. Building interoperable, principles-based international mechanisms remains essential to achieve both effective regulation and a trusted global data ecosystem.

4.3 Country-Specific Analysis

The European Union (EU) has undertaken significant legislative efforts to establish a harmonized regulatory framework for the governance of *Non-Personal Data (NPD)*, reflecting its commitment to promoting a unified digital economy grounded in the principles of data-driven innovation, digital sovereignty, and fundamental rights. While the *General Data Protection Regulation (GDPR)* remains the cornerstone of personal data protection, the governance of *Non-Personal Data* has evolved through complementary legal instruments, particularly through the *Regulation on the Free Flow of Non-Personal Data (FFNPDR)*, the *Data Governance Act (DGA) of 2022*, and the *Data Act of 2023*. These instruments collectively define the contours of EU *Non-Personal Data* law, distinguishing it from personal data regulation while enabling coherent interaction between the two domains.

The DGA introduces a legal framework for fostering trust in data sharing among public bodies, private sector entities, and data altruism organizations, with an emphasis on transparency, interoperability, and neutrality. The Data Act further reinforces the legal infrastructure by regulating data access and use across sectors, particularly in contexts involving industrial and Internet of Things (IoT) data. Notably, both instruments recognize the duality of data, its economic value, and societal utility, and seek to balance proprietary interests with public benefit. These regulatory developments advance the notion of *Non-Personal Data* as a shared resource, subject to principled legal governance. Alongside established data economies such as the European Union, the United States, and Japan, it also includes South Korea and Kenya, thereby capturing both the developed and developing world's experiences in regulating and utilizing non-personal data.

The selection and sequencing of jurisdictions in the ensuing comparative analysis are guided by a regional and legal tradition-based classification, organizing countries into

clusters that reflect shared regulatory philosophies and developmental contexts. This structure groups European Union jurisdictions (Germany, France, Finland, Estonia), Anglo-American common law systems (United States, United Kingdom, Canada, Australia), Asian models (China, Japan, Singapore, South Korea), a Latin American representative (Brazil), and an African perspective (Kenya), thereby ensuring both geographical diversity and analytical coherence in understanding the global evolution of Non-Personal Data governance.

4.3.1 Germany

Legal Definition or Concept

In the Federal Republic of Germany, the legal conception of *Non-Personal Data* (NPD) aligns fundamentally with the supranational framework established under the *European Union's Data Governance Act (DGA) and Data Act*, both of which supplement the foundational *General Data Protection Regulation (GDPR)*. *Non-Personal Data* is explicitly defined by exclusion as any data that does not fall within the scope of the GDPR, particularly datasets that have been irreversibly anonymized, industrial data generated by machine-to-machine communication, and information produced by sensors, devices, and systems within the context of the Internet of Things (IoT). Accordingly, anonymized datasets stripped of identifiers, telemetry data generated by autonomous vehicles, and analytics produced by manufacturing equipment are encompassed within this category.

Germany's national interpretation of this legal definition is further shaped by its "*Digital Strategy 2025*" and the framework of Industry 4.0, which collectively recognize industrial data, particularly that derived from smart factories and digitally integrated supply chains, as a strategic asset. The German government thus conceptually positions *Non-Personal Data* not merely as a by-product of technological activity but as a core driver of economic innovation, technological sovereignty, and leadership in global markets. This industrial orientation to data governance reflects a policy consensus that non-personal data, when effectively mobilized, can foster automation, predictive maintenance, and real-time optimization in sectors such as automotive manufacturing, precision engineering, and logistics.

Importantly, this conception operates under the assumption that *Non-Personal Data* can be governed without triggering the rights-based framework embedded in GDPR, thereby allowing for broader commercial and infrastructural use. Germany remains cautious about the potential for re-identification and data misuse, integrating safeguards even in *Non-Personal Data* governance to ensure that the thin line between anonymized and pseudonymized data is not inadvertently crossed.

Governance Framework

Germany's governance architecture for *Non-Personal Data* is built on a multi-tiered institutional framework. At the top sits the *Federal Ministry for Economic Affairs and Climate Action (BMWK)*, which spearheads national digital and industrial data strategies, shapes policy within EU forums, and manages funding and regulatory compliance. Implementation aligns with federal and state data protection authorities, ensuring that *Non-Personal Data* initiatives uphold Germany's constitutional values, particularly the right to informational self-determination, even when such data falls outside formal data protection law.

Central to this ecosystem is the Gaia-X initiative, a federally supported industrial project to establish a federated, interoperable data infrastructure. It enables secure cross-sector and cross-border data sharing while preserving organizational data sovereignty.⁵²³ Gaia-X operates through "data spaces" spanning areas like mobility, healthcare, energy, and public services, aligning with broader European digital policy goals. The *Industrial Data Spaces (IDS)* model, coordinated by Fraunhofer, provides the technical and ethical backbone for decentralized data sharing. It offers open standards, trust frameworks, usage-control policies, and a reference architecture, all developed through collaboration between government, academia, and industry, including entities like Plattform Industrie 4.0. Furthermore, BMWK's strategic oversight, Gaia-X's federated infrastructure, and the technical rigor of IDS illustrate Germany's comprehensive and collaborative approach to managing *Non-Personal Data* governance.

⁵²³ European Commission Press Release, 'Germany and France Launch Gaia-X Initiative for Cloud Sovereignty' (June 2020).

Key Features

- i. Germany's *Non-Personal Data* governance reflects its industrial priorities, federal constitutional structure, and commitment to EU-wide legal harmonization.
- ii. Foremost among these is the emphasis on industry-led, state-supported data-sharing ecosystems. Platforms such as Gaia-X and Industrial Data Space exemplify a governance philosophy that situates the private sector as both a beneficiary and architect of data infrastructure while the state provides regulatory oversight and infrastructural support.
- iii. These platforms enable cross-sectoral data exchange, particularly in high-value sectors such as automotive engineering, aerospace, manufacturing, and renewable energy.
- iv. The architecture of these systems ensures data sovereignty through mechanisms such as usage control, identity and access management, and data transaction auditing.

Challenges

- i. Germany's approach to *Non-Personal Data* governance faces several substantive and procedural challenges that underscore the complexity of balancing innovation, regulation, and harmonization.
- ii. A primary challenge pertains to the coordination of diverse stakeholders within initiatives such as Gaia-X, where the governance model necessitates the alignment of interests between small and medium-sized enterprises (SMEs), multinational corporations, academic institutions, and public authorities.
- iii. The heterogeneity of stakeholders complicates consensus-building on standards, priorities, and governance rules, often resulting in delays and fragmented implementation.
- iv. The tension between EU-wide harmonization and Germany's national industrial priorities is increasingly evident. While the DGA and Data Act promote standardized frameworks for data sharing across Member States, Germany's emphasis on strategic autonomy and industrial data sovereignty

occasionally diverges from pan-European objectives, particularly regarding cloud infrastructure reliance and third-country data transfers.

4.3.2 France

Legal Definition or Concept

In the French legal system, the delineation of *Non-Personal Data* is fully aligned with the European Union's regulatory edifice, notably the Data Governance Act and the Data Act, which operate in concert with the *General Data Protection Regulation (GDPR)*.

Non-Personal Data in France is broadly defined as all data outputs that fall outside the GDPR framework, chiefly datasets that have been irreversibly anonymized or processed in a manner that renders individual re-identification impossible.⁵²⁴ These include aggregated datasets, machine-generated data from sensors or public infrastructure, and industrial or environmental data where no human subject can be identified.

France advances a legal philosophy whereby *Non-Personal Data* is embraced as a public resource, particularly in domains that intersect with public service delivery and social infrastructure.⁵²⁵ The French state consistently frames such data as embodying public value, not merely economic utility, and emphasizes that its open access can spur innovation in domains of smart cities, transport systems, and public health analytics. The conceptualization situates anonymized data not simply as a by-product of digital processes but as a dataset of civic and scientific significance.⁵²⁶ This normative posture embeds *Non-Personal Data* within the public interest sphere and aligns with European objectives of data altruism and open access, supporting a legal regime in which the State may mandate or strongly encourage the sharing of certain categories of data for societal benefit.

⁵²⁴ Int'l Ass'n of Priv. Prof'ls, *CNIL Issues Opinion on EU Data Governance and Data Acts*, IAPP (Mar. 15, 2023), <https://iapp.org/news/a/cnil-opinion-data-governance-act>.

⁵²⁵ French Ministry of Solidarity and Health, 'Health Data Hub Decree' (2019).

⁵²⁶ *Commission Nationale de l'Informatique et des Libertés (CNIL)*, 'Opinion on Health Data Hub Data Transfers' (Oct. 2020).

Governance Framework

The governance framework for *Non-Personal Data* in France is architected around a centralized and highly regulated structure, anchored institutionally in the *Commission nationale de l'informatique et des libertés (CNIL)*. CNIL's jurisdiction extends to the oversight and enforcement of compliance with EU-level regulations, including the Data Governance Act and Data Act, even when the data at issue is anonymized and technically outside the realm of personal data protection. This reflects a precautionary legal culture that maintains institutional continuity across personal and *Non-Personal Data* domains. Complementing CNIL's supervisory role are sector-specific regulators, most notably within the healthcare domain, where the Ministry of Health exercises operational authority over medical and public health datasets. In tandem, the Health Data Hub has been established as a national centralized platform designed to facilitate the lawful sharing of anonymized health data for research, innovation, and policy planning. The Hub enforces stringent governance standards, including data minimization, ethical review, and usage audits. Its legal and technical infrastructure supports the publication, secure access, and controlled reuse of health-related *NPD* in accordance with public interest law.

Key Features

- i. France's policy design incorporates distinguished features that reflect its public-sector orientation and strategic deployment of non-personal data.
- ii. First among these is the open data portal data.gouv.fr, which provides transparent access to thousands of anonymized datasets spanning domains such as transportation, environment, public finance, and demographics.
- iii. This portal facilitates both public service use and research initiatives, thereby infusing government-held data with civic and economic vitality.
- iv. The portal's licensing and metadata protocols ensure compliance with legal and technical norms, promoting interoperability within the EU digital framework.
- v. The Health Data Hub constitutes a second hallmark, enabling researchers, public institutions, and private enterprises, including AI and biotech firms, to access curated and anonymized healthcare datasets.

- vi. France also leverages *Non-Personal Data* to advance smart-city and mobility initiatives, using urban data platforms that integrate sensor-derived transport data, urban infrastructure metrics, energy consumption patterns, and environmental monitoring.

Challenges

- i. Despite its advanced regulatory architecture, France faces several substantial and technically complex challenges in operationalizing its *Non-Personal Data* strategy.
- ii. Chief among these is the robust anonymization standard mandated under the GDPR, which requires that re-identification must not be reasonably achievable. Implementing such standards at scale, particularly within healthcare datasets, demands significant expertise in differential privacy, statistical disclosure control, and ongoing risk assessment.
- iii. The re-identification risk remains a latent legal concern, and any breach could expose French institutions to reputational and liability consequences.
- iv. France's policy orientation is markedly less focused on private-sector or industrial data-sharing ecosystems, in contrast to jurisdictions such as Germany, which heavily promote platforms like Gaia-X and Industrial Data Space.
- v. France's comparatively limited integration of private-sector *NPD* governance restricts its reach in industrial and manufacturing-driven innovation and may constrain competitiveness in sectors where bilateral data exchange between firms is commercially critical.

4.3.3 Finland

Legal Definition or Concept

In alignment with the broader regulatory architecture of the European Union, Finland adopts the EU's delineation of non-personal data, particularly as outlined in the Regulation on the Free Flow of *Non-Personal Data* (Regulation (EU) 2018/1807). Non-personal data, under this framework, encompasses datasets that do not contain personal identifiers, including anonymized and aggregated information. Within legal

and policy discourse, this definition is further contextualized through national data governance initiatives such as the MyData principles. Although not codified in statute, these principles are endorsed by national stakeholders and frame *Non-Personal Data* as a communal resource intended to enhance innovation, transparency, and individual autonomy in data-driven environments.

The conceptualization of *Non-Personal Data* thus extends beyond mere regulatory compliance, integrating normative commitments to citizen empowerment and ethical digital services. Finland's digital strategy, anchored in the advancement of a sustainable and inclusive data economy, positions *Non-Personal Data* as a critical infrastructural asset within both the public and private sectors.

Governance Framework

Finland's governance of *Non-Personal Data* operates within a dual-layered system comprising national authorities and supranational European Union obligations. Domestically, the Finnish Ministry of Transport and Communications serves as the lead administrative body responsible for data policy, supported by sectoral oversight from the Office of the Data Protection Ombudsman, particularly where mixed datasets implicating both personal and *Non-Personal Data* are concerned. Importantly, the Sitra Innovation Fund, an independent public foundation, plays a quasi-regulatory and thought-leadership role by shaping normative frameworks and piloting operational models for ethical data sharing.

The MyData Global initiative, originating in Finland and now operating internationally, exemplifies efforts to create interoperable and user-centric data ecosystems. Finland's open data infrastructure, including portals such as avoindata.fi (data.fi), enables lawful, structured access to public-sector non-personal datasets in accordance with the principles laid out in the EU Open Data Directive (Directive (EU) 2019/1024).⁵²⁷

⁵²⁷ Finnish Ministry of Transport and Communications, 'Trusted Data Sharing Policy Report' (2025).

Key Features

- i. The Finnish model of *Non-Personal Data* governance is distinguished by its adherence to the Nordic tradition of transparency, public trust, and inclusive policymaking.
- ii. Core features include the proactive dissemination of government-held *Non-Personal Data* through centralized repositories and the promotion of data interoperability and reusability standards.
- iii. The MyData philosophy contributes an ethical lens to data governance by emphasizing user control, consent-based data sharing, and ecosystem accountability principles increasingly being adapted to *Non-Personal Data* contexts.
- iv. Finland's participation in broader EU-level initiatives such as the Digital Governance Act (DGA) and the European Data Spaces reflects its commitment to cross-border data flows, innovation in digital services, and the construction of a harmonized internal market for data.

Challenges

- i. Despite Finland's advanced digital infrastructure and principled approach to data governance, several challenges persist. Chief among these is the difficulty of operationalizing MyData principles in the realm of non-personal data, especially within private-sector domains where incentives for ethical data stewardship remain underdeveloped.
- ii. Technical interoperability, standard-setting, and the creation of trust frameworks for industrial data sharing continue to encounter implementation delays.
- iii. Finland is constrained by limited financial and technical resources for independently sustaining large-scale data initiatives, thereby necessitating reliance on EU co-funding and multinational partnerships.
- iv. Another critical concern is the limited engagement of non-public actors, particularly small and medium-sized enterprises (SMEs), in participatory data

governance processes. This raises questions about the inclusiveness and scalability of current frameworks beyond the public sector.

4.3.4 Estonia

Legal Definition or Concept

Estonia defines *Non-Personal Data* in alignment with European Union regulations, particularly under the Free Flow of *Non-Personal Data* Regulation and the Open Data Directive. *Non-Personal Data* encompasses information that does not relate to an identified or identifiable individual, including anonymized, aggregated, and machine-generated datasets. Within Estonia's e-governance model, such data is viewed not merely as informational residue but as a foundational component of public digital infrastructure. This conception positions *Non-Personal Data* as both a state resource and a public good that supports innovation, transparency, and efficient public administration. The legal interpretation of *Non-Personal Data* is embedded within Estonia's national digital strategy and its e-Government framework, which collectively emphasize the seamless exchange of information across public institutions while ensuring legal and technical safeguards against re-identification.

Governance Framework

Estonia's governance architecture for *Non-Personal Data* is deeply integrated into its broader e-governance system.⁵²⁸ The X-Road platform serves as the backbone of the country's data infrastructure, enabling secure, interoperable data exchange among public and private institutions.⁵²⁹ The Ministry of Economic Affairs and Communications (MEAC) holds the primary policy mandate for data governance, complemented by the Estonian Information System Authority (RIA), which ensures cybersecurity and technical compliance. Together, these bodies create an institutional environment characterized by legal clarity, standardized interoperability, and automated compliance mechanisms. Estonia's model operates on the principle of

⁵²⁸ Estonian Info. Sys. Auth. (RIA), *X-Road International Implementation Report 2024*, at 5–7 (2024), <https://x-road.global>.

⁵²⁹ ERR News, *Audit Office: IT Security of Firms Using X-Road Not Sufficiently Checked*, ERR News (Mar. 2, 2021), <https://news.err.ee/1608134567/audit-office-x-road-security>.

“once-only data submission,” wherein individuals and organizations are not required to provide the same data to multiple agencies. This legal and technical design fosters efficiency, transparency, and public trust in data-driven governance.

Key Features

- i. The X-Road digital infrastructure enables real-time, secure, and interoperable data sharing between government and private entities.
- ii. Estonia’s open data portal (avaandmed.ee) facilitates public access to a wide range of anonymized datasets, including statistics, environmental data, and spatial information.
- iii. Legal interoperability standards ensure that data exchange adheres to European Union directives, enhancing trust and reducing administrative burden.
- iv. Estonia’s “once-only principle” has become a model for other jurisdictions seeking to minimize duplication and enhance efficiency in public data management.
- v. The Estonian approach integrates *Non-Personal Data* governance with cybersecurity protocols, ensuring the integrity and accountability of all data transactions.

Challenges

- i. Despite its advanced digital ecosystem, Estonia faces persistent challenges related to cross-border data sharing, particularly where national security or jurisdictional overlaps arise within European Union data spaces.
- ii. Maintaining absolute anonymization is technically demanding, especially as advances in artificial intelligence and data analytics heighten re-identification risks.
- iii. The reliance on centralized digital infrastructure introduces potential systemic vulnerabilities, necessitating continual investment in cybersecurity resilience and data redundancy.
- iv. As Estonia seeks to scale its data economy, ensuring equitable access for smaller firms and research institutions remains a policy priority to prevent concentration of data control in a few technologically dominant actors.

4.3.5 The United States

Legal Definition or Concept

The United States does not maintain a singular legal definition of non-personal data. Its approach is characterized by fragmentation and sector-specificity, wherein regulatory interpretation varies across industries and agencies. *Non-Personal Data* is typically referred to as “non-personally identifiable information” (non-PII) and is defined in negative terms, data that does not identify an individual or cannot reasonably be used to do so. This encompasses aggregated, anonymized, and de-identified datasets generated by businesses, government programs, and digital platforms. The definitional framework is informed by a combination of statutory instruments such as the Federal Trade Commission Act, the Health Insurance Portability and Accountability Act (HIPAA), and state-level privacy laws like the California Consumer Privacy Act (CCPA)⁵³⁰. These laws address anonymization and data sharing indirectly, leading to a regulatory mosaic that prioritizes commercial autonomy over centralized oversight.

Governance Framework

The governance of *Non-Personal Data* in the United States operates through a market-driven, decentralized model.⁵³¹ The Federal Trade Commission (FTC) functions as the de facto national authority for data governance, primarily through its consumer protection and unfair trade practice jurisdiction. It issues guidance and enforces penalties against deceptive claims concerning anonymization or data security. The National Institute of Standards and Technology (NIST) supplements this framework by developing voluntary technical standards for data interoperability, anonymization, and cybersecurity. Sectoral regulators, including the Department of Health and Human Services (HHS), the Department of Transportation (DoT), and the Federal Communications Commission (FCC), administer domain-specific data governance frameworks. The absence of a comprehensive federal data protection law results in

⁵³⁰ DLA Piper, *FTC Uses Its Power to Address Unfair or Deceptive Data Practices*, DLA Piper Data Prot. Insights (Feb. 6, 2025), <https://www.dlapiperdataprotection.com/us/ftc-data-practices-2025>.

⁵³¹ National Institute of Standards and Technology, ‘Privacy Framework Version 1.1’ (2020).

overlapping jurisdictions, creating regulatory inconsistency but also allowing flexibility and innovation in the private sector.

Key Features

- i. The United States' *Non-Personal Data* governance relies heavily on self-regulation, contractual obligations, and voluntary technical standards rather than centralized enforcement.
- ii. Sector-specific statutes, such as HIPAA and the Gramm-Leach-Bliley Act (GLBA), indirectly regulate *Non-Personal Data* through obligations related to de-identification and security.
- iii. The National Institute of Standards and Technology (NIST) promotes best practices for anonymization, metadata management, and interoperability through its frameworks and guidance documents.
- iv. State-level initiatives, particularly in California and Virginia, are introducing broader data governance principles that impact both personal and non-personal datasets.
- v. Private companies, including technology and industrial firms, play a leading role in setting de facto standards for data sharing and reuse through industry associations and trade groups.

Challenges

- i. The absence of a federal legal framework creates regulatory fragmentation, producing inconsistent data-sharing norms across sectors and states.
- ii. Over-reliance on self-regulation can lead to inadequate accountability, particularly when anonymization techniques fail or data is re-identified through aggregation.
- iii. The commercial dominance of large technology corporations results in asymmetrical control over *Non-Personal Data* resources, raising antitrust and competition law concerns.
- iv. Disparities between federal and state jurisdictions complicate cross-border data transfers and undermine international trust in U.S. data governance.

- v. Calls for federal harmonization, including proposals for a U.S. Data Protection Act, continue to face political resistance, leaving the regulatory landscape uneven and industry-driven.

4.3.6 United Kingdom

Legal Definition or Concept

The legal understanding of *Non-Personal Data* in the United Kingdom derives primarily from the UK National Data Strategy (2021) and pre-Brexit European Union instruments such as the *General Data Protection Regulation (GDPR)* and the Free Flow of *Non-Personal Data* Regulation (EU) 2018/1807. Following Brexit, the UK continues to interpret *Non-Personal Data* as data that does not relate to an identified or identifiable individual. This includes anonymized, aggregated, and industrial datasets generated by automated systems and public sector databases. The UK legal framework emphasizes the economic and social value of non-personal data, identifying it as a catalyst for innovation, public service delivery, and evidence-based policymaking. Although no standalone statute governs non-personal data, the concept is operationalized through a combination of regulatory guidelines issued by the *Information Commissioner's Office (ICO)*, sectoral codes of conduct, and national digital transformation strategies.

Governance Framework

The governance architecture for *Non-Personal Data* in the United Kingdom is decentralized yet well-coordinated across institutions.⁵³² The Information Commissioner's Office (ICO) performs a central role in ensuring responsible data management, ethical sharing, and compliance with transparency principles. Sector-specific regulators such as Ofcom for communications, the Financial Conduct Authority (FCA) for financial services, and the Department for Science, Innovation and Technology (DSIT) for digital policy contribute to a multi-agency governance

⁵³² Dep't for Sci., Innovation & Tech., *UK Data Strategy: A Data Economy for the Public Good*, at 12–14 (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/943456/NDS.pdf.

structure. The UK National Data Strategy promotes open data ecosystems and encourages both public and private sectors to participate in secure and interoperable data sharing.⁵³³ Public-private partnerships, data trusts, and regulatory sandboxes are integral mechanisms enabling innovation while maintaining accountability.

Key Features

- i. The United Kingdom promotes open data accessibility through the Open Data Institute (ODI), which facilitates data sharing across industries and research institutions.
- ii. Public sector bodies such as NHS Digital make anonymized datasets available for medical research and innovation, enhancing healthcare policy formulation.
- iii. The legal and technical frameworks emphasize interoperability and machine-readability to improve cross-sectoral data exchange.
- iv. The national strategy integrates *Non-Personal Data* governance with AI policy, ensuring alignment between innovation and data ethics.
- v. Collaborative mechanisms such as data trusts enable collective management of anonymized datasets for public benefit.

Challenges

- i. Post-Brexit divergence from the European Union's legal framework introduces uncertainty regarding adequacy status and data flow agreements.
- ii. The absence of a dedicated statute governing *Non-Personal Data* creates interpretive gaps across regulatory sectors.
- iii. The risk of regulatory fragmentation arises from the coexistence of multiple sectoral authorities with overlapping mandates.
- iv. Businesses operating across both UK and EU jurisdictions face dual compliance obligations, raising administrative and operational costs.
- v. Ensuring the long-term consistency of the UK's open data approach with evolving global standards remains a policy challenge.

⁵³³ Dep't for Sci., Innovation & Tech., *National Data Strategy: Action Plan*, at 18–20 (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043285/National_Data_Strategy_Action_Plan.pdf.

4.3.7 Canada

Legal Definition or Concept

Canada's understanding of *Non-Personal Data* arises from the Digital Charter Implementation Act (2019) and associated policy frameworks under Innovation, Science and Economic Development Canada (ISED).⁵³⁴ *Non-Personal Data* is defined as information that does not relate to an identifiable individual, including anonymized or aggregated data rendered incapable of re-identification through foreseeable means. The legal framework situates *Non-Personal Data* as a national asset for innovation, research, and policy development.⁵³⁵

Canada emphasizes the responsible use of anonymized public datasets to drive evidence-based governance, digital entrepreneurship, and inclusive economic growth.

Governance Framework

Innovation, Science and Economic Development Canada (ISED) oversee the national data strategy and coordinates data governance efforts across federal agencies. The open.canada.ca portal serves as the primary platform for accessing anonymized government datasets. The governance model emphasizes transparency, accessibility, and interoperability across sectors. Federal and provincial governments collaborate to maintain consistent technical standards for data sharing and reuse. Policy instruments such as the Canadian Digital Charter ensure accountability while encouraging cross-sectoral collaboration in research and digital innovation.

Key Features

- i. The open.canada.ca platform provides access to extensive datasets spanning health, environment, and demographics.
- ii. The governance model balances innovation with ethical data stewardship, ensuring that public datasets serve both economic and civic goals.

⁵³⁴ Canada, *Digital Charter Implementation Act*, 2022, S.C. 2022, c. 10, § 2 (2022), <https://laws-lois.justice.gc.ca/eng/acts/D-2.5/page-1.html>.

⁵³⁵ Innovation, Sci. & Econ. Dev. Can., *Canada's Digital Charter in Action: Responsible Innovation with Data*, at 8–10 (2020), <https://ised-isde.canada.ca/site/digital-charter/en/canadas-digital-charter-action-responsible-innovation-data>.

- iii. Federal coordination under ISED promotes harmonization of data policies across provinces.
- iv. Emphasis on transparency and accessibility strengthens public trust and institutional accountability.
- v. The framework encourages the integration of open data principles into private-sector innovation initiatives.

Challenges

- i. Fragmentation between federal and provincial jurisdictions results in inconsistent definitions and enforcement standards.
- ii. Absence of a comprehensive *Non-Personal Data* statute limits the predictability of regulatory obligations.
- iii. Limited engagement by private-sector actors hinders the full realization of the data economy's potential.
- iv. Resource constraints in smaller provinces impede uniform implementation of open data programs.
- v. Ensuring that anonymization practices remain technologically resilient against re-identification remains an ongoing concern.

4.3.8 Australia

Legal Definition or Concept

Australia defines *Non-Personal Data* under the Data Availability and Transparency Act (DATA Act) of 2022 as data that does not relate to identifiable individuals, encompassing anonymized, aggregated, and public-interest datasets. The Act promotes the principle that *Non-Personal Data* constitutes a public resource capable of enhancing transparency, innovation, and evidence-based decision-making. This legal recognition embeds *Non-Personal Data* within the broader digital transformation agenda, viewing it as a cornerstone for improving governance, scientific research, and economic productivity.

Governance Framework

The National Data Commissioner (NDC) administers the DATA Act and oversees compliance, accreditation, and data-sharing practices across Commonwealth agencies. The governance structure is designed to ensure safe and efficient sharing of *Non-Personal Data* between public institutions and authorized users. The Consumer Data Right (CDR) framework, managed by the Australian Competition and Consumer Commission (ACCC), extends similar governance principles to the private sector, empowering individuals to control access to their de-identified data.⁵³⁶ The data.gov.au portal consolidates anonymized datasets from federal and state agencies, promoting open access and research utility.⁵³⁷

Key Features

- i. The DATA Act institutionalizes *Non-Personal Data* sharing as a means of promoting transparency and public accountability.
- ii. The Consumer Data Right (CDR) framework ensures that individuals retain control over the use of their data even after anonymization.
- iii. The data.gov.au platform facilitates the integration of open data into public administration and academic research.
- iv. Australia's governance model prioritizes trust, security, and interoperability through accreditation and technical standards.
- v. The system encourages data sharing across sectors, fostering collaboration between government, academia, and industry.

Challenges

- i. Overemphasis on public-sector datasets results in limited mechanisms for private-sector *Non-Personal Data* sharing.
- ii. Jurisdictional fragmentation between federal, state, and territorial governments complicates uniform implementation.

⁵³⁶ Consumer Data Right (Privacy Safeguards) Rules 2020 (Cth), r 1.4 (Austl.), <https://www.legislation.gov.au/Details/F2020L00894>.

⁵³⁷ Austl. Gov't, *Data Availability and Transparency Act 2022: Implementation Report*, at 10–12 (2023), <https://www.datacommissioner.gov.au/sites/default/files/2023-05/Data-Availability-Transparency-Act-Implementation-2023.pdf>.

- iii. The cost and complexity of ensuring anonymization compliance may deter smaller institutions from participating in open data initiatives.
- iv. Ongoing alignment with international data standards remains a challenge for maintaining interoperability.
- v. Ensuring that *Non-Personal Data* governance evolves in step with emerging technologies and societal needs requires continuous policy adaptation.

4.3.9 China

Legal Definition or Concept

China's legal framework for *Non-Personal Data* is embedded within its broader data governance system established by the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). *Non-Personal Data* is not defined independently in statutory language but is conceptualized through exclusion: it includes all data not categorized as personal under PIPL. The DSL introduces hierarchical classifications for data based on its importance, identifying categories such as "core data" and "important data." *Non-Personal Data* falls primarily within these classifications when it holds strategic, economic, or security relevance to the state. The law thereby integrates *Non-Personal Data* into the national security apparatus and treats it as a sovereign asset subject to state control, reflecting China's philosophy of cyber-sovereignty and digital self-reliance.

Governance Framework

The Cyberspace Administration of China (CAC) is the primary regulatory authority overseeing both personal and non-personal data.⁵³⁸ It coordinates with sectoral ministries such as the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS) to enforce compliance. The governance framework mandates localization for certain categories of *Non-Personal Data* and imposes pre-transfer risk assessments before cross-border data sharing. Industrial datasets, especially those generated in critical sectors such as energy, transportation, and finance, are subject to prior authorization and periodic security evaluations.

⁵³⁸ Data Security Law of the People's Republic of China, Order No. 84 of the President, art. 7 (June 10, 2021), <http://www.npc.gov.cn/npc/c30834/202106/7c87f8b8f5cd4f58b8f3e0a2f8b8f8b8.shtml>.

China's Data Exchange Centers, established in cities such as Shanghai and Shenzhen, facilitate controlled trading of anonymized and aggregated datasets under government supervision. These centers embody the state's dual role as regulator and economic participant in the national data market.

Key Features

- i. The Data Security Law establishes a tiered system that distinguishes between ordinary, important, and core data, integrating non-personal datasets into strategic governance.
 - Mandatory data localization and cross-border risk assessments ensure that sensitive *Non-Personal Data* remains within national control.
- ii. The development of regional data exchanges institutionalizes the marketization of anonymized datasets under state oversight.
- iii. Integration between industrial policy and data regulation promotes state-led innovation in areas such as artificial intelligence, 5G, and manufacturing analytics.
- iv. The government's capacity to classify, monitor, and control the circulation of *Non-Personal Data* reinforces its sovereignty and national security priorities.

Challenges

- i. The centralization of data governance raises concerns about over-regulation and limited transparency in enforcement.
- ii. The blurred boundary between personal and *Non-Personal Data* under Chinese law complicates compliance for both domestic and foreign firms.
- iii. Stringent localization and transfer restrictions deter international data collaboration and increase operational costs for multinational entities.
- iv. The lack of judicial oversight or independent regulatory review limits accountability and deters innovation in private-sector data use.
- v. Balancing state security imperatives with global interoperability remains a significant policy dilemma within China's evolving data governance system.

4.3.10 Japan

Legal Definition or Concept

Japan's approach to *Non-Personal Data* governance is grounded in the Basic Act on the Advancement of Public and Private Sector Data Utilization (2016). Although the Act does not provide an explicit statutory definition, *Non-Personal Data* is generally interpreted as anonymized, industrial, or machine-generated data produced through Internet of Things (IoT) systems, robotics, and artificial intelligence applications. This conceptualization reflects Japan's view of *Non-Personal Data* as a strategic national resource, essential to digital transformation and global economic competitiveness. The government treats *Non-Personal Data* as distinct from personal data, focusing on its potential for cross-sectoral innovation and transnational collaboration under ethical and interoperable frameworks.

Governance Framework

Governance of *Non-Personal Data* in Japan operates through a decentralized multi-ministerial structure. The Ministry of Economy, Trade and Industry (METI) leads national data policy, supported by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Land, Infrastructure, Transport and Tourism (MLIT). Japan's "Data Free Flow with Trust" (DFFT) initiative, introduced at the 2019 G20 Osaka Summit, serves as the cornerstone of its international data diplomacy.⁵³⁹ DFFT promotes global data exchange based on mutual trust, legal interoperability, and shared governance values. The initiative complements Japan's participation in multilateral frameworks such as the G7 Data Protection Principles and OECD digital economy standards.

Key Features

- i. The *Data Free Flow with Trust (DFFT)* framework advances cross-border cooperation in data sharing under rule-based principles.

⁵³⁹ Japan, Basic Act on the Advancement of Public and Private Sector Data Utilization, 2016, art. 2 (2016).

- ii. Japan's governance model encourages public-private collaboration in sectors like automotive manufacturing, robotics, and AI.
- iii. The government actively supports open data projects that promote evidence-based policymaking and civic engagement.
- iv. Industry-led data platforms developed by companies such as Hitachi and Toyota facilitate interoperable and ethical use of industrial datasets.
- v. The regulatory philosophy emphasizes soft law instruments, guidelines, and ethical standards over prescriptive mandates.

Challenges

- i. The absence of a specific legislative regime for *Non-Personal Data* creates ambiguity in enforcement and compliance.
- ii. Heavy reliance on voluntary compliance and self-regulation limits legal predictability and consistency across sectors.
- iii. The overlapping responsibilities among ministries occasionally lead to administrative inefficiency.
Maintaining alignment between domestic data governance and international frameworks requires continuous coordination.
- iv. Encouraging broader private-sector engagement in *Non-Personal Data* innovation remains an ongoing policy challenge.

4.3.11 Singapore

Legal Definition or Concept

Singapore defines *Non-Personal Data* within the framework of its Personal Data Protection Act (PDPA) and related Data Sharing Framework, administered by the Infocomm Media Development Authority (IMDA). Although the PDPA primarily regulates personal data, amendments and policy instruments introduced under the Smart Nation initiative clarify that *Non-Personal Data* refers to datasets that have been irreversibly anonymized or aggregated such that no individual can be identified directly or indirectly. This category includes industrial, transactional, and sensor-generated data. Singapore treats *Non-Personal Data* as a strategic economic asset essential to innovation, governance efficiency, and international competitiveness. The

conceptualization reflects the state's pragmatic approach to digital transformation, balancing commercial interests with national development objectives.

Governance Framework

Singapore's governance framework for *Non-Personal Data* is centralized and structured under the leadership of the *Infocomm Media Development Authority* (IMDA).⁵⁴⁰ The IMDA implements the Trusted Data Sharing Framework, which establishes legal and technical principles for responsible data exchange across sectors. Complementing this structure are sector-specific regulators, such as the Monetary Authority of Singapore (MAS) for finance and the Ministry of Health (MOH) for healthcare, which issue additional data-sharing obligations tailored to their domains.⁵⁴¹ The governance model incorporates sandboxes, ethical review boards, and data intermediaries that enable experimentation and compliance testing in emerging data ecosystems. Cross-border data mobility is facilitated through bilateral agreements and participation in regional initiatives like the ASEAN Data Management Framework.

Key Features

- i. The Smart Nation initiative integrates *Non-Personal Data* governance within broader national digital transformation goals.
- ii. The Trusted Data Sharing Framework emphasizes transparency, accountability, and interoperability among stakeholders.
- iii. *Non-Personal Data* is leveraged for Smart Urban Mobility and predictive analytics in transport, healthcare, and energy sectors.
- iv. The governance structure prioritizes both economic utility and secure innovation through layered accountability mechanisms.
- v. Singapore promotes international collaboration through standardized data-sharing agreements that align with global privacy principles.

⁵⁴⁰ Info. Comm'n's Media Dev. Auth., *Singapore's Digital Economy Report 2024*, IMDA (Oct. 10, 2024), <https://www.imda.gov.sg/digital-economy-report-2024>.

⁵⁴¹ Personal Data Protection Act 2012, § 2(1) (Sing.).

Challenges

- i. The framework's commercial orientation prioritizes innovation and competitiveness, sometimes at the expense of civic or non-market data applications.
- ii. Limited focus on public-interest datasets, such as environmental or social welfare data, restricts broader societal utility.
- iii. The rapid evolution of data technologies necessitates continuous updates to legal and ethical standards to prevent obsolescence.
- iv. Ensuring equitable participation by small and medium enterprises in the data economy remains a governance challenge.
- v. Maintaining international trust amid increasing global scrutiny of data sovereignty issues is a continuing policy concern.

4.3.12 South Korea

Legal Definition or Concept

South Korea's approach to *Non-Personal Data* governance is anchored in its Framework Act on the Promotion of Data Industry (2021) and complemented by the Personal Information Protection Act (PIPA).⁵⁴² Although the legislation does not explicitly define "non-personal data," it conceptualizes it as information that cannot identify a specific individual, either on its own or when combined with other data. The Korean government distinguishes between *personal data*, *pseudonymized data*, and *de-identified or anonymized data*, the latter constituting non-personal data. The Framework Act recognizes *Non-Personal Data* as a key economic and public asset, promoting its use for innovation, artificial intelligence (AI), and data-driven policymaking while ensuring that privacy and ethical considerations are maintained.

Governance Framework

The Ministry of Science and ICT (MSIT) and the Korea Data Agency (K-DATA) jointly oversee the development, standardization, and utilization of *Non-Personal*

⁵⁴² Framework Act on the Promotion of Data Industry and Promotion of Use, Act No. 18475, art. 2 (S. Kor. 2021), https://elaw.klri.re.kr/eng_service/lawView.do?hseq=63957&lang=ENG.

Data across sectors.⁵⁴³ The Korean New Deal initiative integrates *Non-Personal Data* management into the broader digital economy strategy by encouraging cross-sector data sharing between government agencies, industries, and research institutions. The Public Data Portal (data.go.kr) serves as a national repository, offering anonymized datasets for academic, industrial, and public use. Moreover, the government has established the Data Industry Promotion Committee to create policies that stimulate responsible data sharing and ensure consistency across regulatory domains.

Key Features

- i. The Framework Act promotes the ethical and transparent use of de-identified and anonymized data as a national economic resource.
- ii. The Public Data Portal consolidates anonymized datasets from government and public institutions, enhancing research and innovation.
- iii. National standards for data anonymization and metadata are defined by the Korea Internet and Security Agency (KISA).
- iv. The governance structure promotes public–private collaboration, with strong state oversight to prevent re-identification risks.
- v. *Non-Personal Data* initiatives are linked to South Korea’s AI development strategy, supporting smart city and digital innovation projects.

Challenges

- i. Despite robust infrastructure, ambiguities persist regarding the legal status and commercial use of mixed datasets containing both personal and non-personal data.
- ii. The complex compliance environment under multiple regulatory bodies (MSIT, KISA, PIPC) can create administrative overlap.

⁵⁴³ Ministry of Science and ICT, *Data Industry Promotion Plan 2024-2028*, MSIT Policy Document, at 15–17 (2024), <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=217&mPid=219&bbsSeqNo=11&nttSeqNo=3153455>.

- iii. Limited participation from SMEs due to high costs of data anonymization and lack of technical capacity.
- iv. Ethical and societal concerns regarding potential bias in AI applications using anonymized data remain under-addressed.
- v. Global interoperability issues continue to challenge the integration of South Korea's *Non-Personal Data* policies with international data frameworks.⁵⁴⁴

4.3.13 Brazil

Legal Definition or Concept

In Brazil, *Non-Personal Data* governance is embedded within the General Data Protection Law (*Lei Geral de Proteção de Dados* Pessoais, LGPD) enacted in 2020. While the LGPD primarily regulates personal data, it acknowledges anonymized datasets as being outside its scope when they are rendered irreversibly non-identifiable. *Non-Personal Data* in the Brazilian context includes anonymized or aggregated datasets used in sectors such as banking, digital governance, and telecommunications. The legal framework treats *Non-Personal Data* as a driver of innovation, transparency, and economic development. It recognizes the potential of anonymized datasets in advancing financial inclusion, open government, and public accountability.

Governance Framework

The *Autoridade Nacional de Proteção de Dados (ANPD)* serves as Brazil's central data protection authority. It oversees both personal and *Non-Personal Data* governance through regulatory guidance, audit powers, and administrative enforcement. Sectoral authorities, such as the Central Bank of Brazil, play a critical role in operationalizing open banking initiatives that depend on the secure exchange of anonymized data.⁵⁴⁵ The gov.br platform functions as a national hub for digital public services and open data dissemination. This multi-layered governance

⁵⁴⁴ OECD, *Interoperability in Digital Trade: South Korea's Non-Personal Data Policies*, OECD Digital Economy Papers No. 342, at 22–25 (2024), <https://www.oecd-ilibrary.org/docserver/3f7a4b9c-en.pdf>.

⁵⁴⁵ Banco Central do Brasil, *Open Finance Regulation* No. 1/2020: Implementation of Data Sharing and Access, Circular No. 3.951, at 4–6 (2020), <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3951>.

framework combines regulatory oversight with proactive public-sector innovation, fostering collaboration among institutions and citizens.

Key Features

- i. Brazil's open banking framework promotes interoperability and consent-based sharing of anonymized financial data.
- ii. The gov.br platform provides centralized access to anonymized government datasets to enhance transparency and civic engagement.
- iii. *Non-Personal Data* is positioned as a public good supporting research, innovation, and social welfare initiatives.
- iv. The governance framework integrates both regulatory compliance and voluntary participation by private entities.
- v. Collaboration between the *ANPD* and sectoral regulators strengthens accountability and technical standardization.

Challenges

- i. The absence of a dedicated *Non-Personal Data* statute results in interpretive uncertainty across sectors.
- ii. The *ANPD*'s limited institutional capacity constrains its ability to monitor anonymization practices and prevent re-identification.
- iii. Fragmented implementation among state and federal entities weakens policy coherence.
- iv. Legal ambiguity regarding mixed datasets creates compliance challenges for businesses and public agencies.
- v. Ensuring consistent anonymization standards across industries remains a technical and regulatory challenge.

4.3.14 Kenya

Legal Definition or Concept

Kenya's evolving data governance framework identifies *Non-Personal Data* as information that does not relate to an identified or identifiable natural person, including anonymized and aggregated datasets. While the Data Protection Act, 2019 primarily

governs personal data, it indirectly acknowledges *Non-Personal Data* through its exclusion of anonymized or de-identified information from regulatory oversight. Kenya's Digital Economy Blueprint (2019) and the Open Data Policy (2022) collectively conceptualize *Non-Personal Data* as a public asset vital for transparency, innovation, and socio-economic development.⁵⁴⁶ This vision aligns with Kenya's aspiration to be a regional data hub for Africa, emphasizing open access, ethical governance, and the public value of data.

Governance Framework

The Office of the Data Protection Commissioner (ODPC) oversees data regulation but does not directly manage non-personal datasets. Instead, the ICT Authority of Kenya, through the Kenya Open Data Initiative (KODI) and Kenya Open Data Portal (opendata.go.ke), facilitates access to government-held anonymized datasets.⁵⁴⁷ These initiatives encourage transparency, civic participation, and innovation across sectors such as health, agriculture, and education. The National Integrated Identity Management System (NIIMS) also feeds anonymized demographic data into development analytics. Furthermore, Kenya is developing a National Data Strategy under the Ministry of ICT and Digital Economy, which will establish policies for data sharing, quality standards, and interoperability for both personal and non-personal data.

Key Features

- i. The Open Data Policy and Kenya Open Data Portal provide a centralized access point for anonymized public datasets.
- ii. The Digital Economy Blueprint promotes data-driven governance and innovation using non-personal data.

⁵⁴⁶ Ministry of Information, Communications and Technology, *Digital Economy Blueprint: Powering Kenya's Transformation to a Digital State*, at 12–14 (2019), <https://ict.go.ke/sites/default/files/2024-09/Kenya-Digital-Economy-2019.pdf>.

⁵⁴⁷ Office of the Data Protection Commissioner, *Data Protection Act, 2019: Guidance on Personal Data Processing*, ODPC Advisory No. 2021/02, at 5–7 (2021), <https://www.odpc.go.ke/wp-content/uploads/2021/07/Data-Protection-Act-2019.pdf>.

- iii. The framework encourages public–private partnerships to support data sharing for national development goals.
- iv. Kenya prioritizes inclusive data governance by emphasizing equitable access for researchers, entrepreneurs, and citizens.
- v. Ongoing alignment with the African Union’s Data Policy Framework (2022) ensures continental consistency in *Non-Personal Data* governance.⁵⁴⁸

Challenges

- i. The absence of a dedicated *Non-Personal Data* law leaves governance fragmented across multiple policies and agencies.
- ii. Limited technical infrastructure constrains the country’s ability to anonymize, store, and share large datasets securely.
- iii. Awareness and capacity gaps among local institutions hinder effective utilization of available open data resources.
- iv. Balancing openness with data security remains a challenge, especially when datasets could indirectly enable re-identification.
- v. Regional disparities in digital readiness impede uniform implementation of data-sharing frameworks, reducing nationwide impact.

4.4 Comparative Analysis

4.4.1 Descriptive Overview

This section undertakes a doctrinal and comparative evaluation of the regulatory frameworks governing *Non-Personal Data* (NPD) across fourteen selected jurisdictions. It aims to analyse how these frameworks conceptualize, regulate, and operationalize the management of non-personal data, thereby revealing both convergence and jurisdictional specificity. The analysis delineates convergences, divergences, emergent global patterns, and salient legal lacunae. The objective is to

⁵⁴⁸ ICT Authority of Kenya, *Kenya Open Data Initiative (KODI): Annual Report 2023*, at 10–12 (2023), <https://www.icta.go.ke/wp-content/uploads/2023/12/KODI-Annual-Report-2023.pdf>.

distil principles that may inform the development of harmonized and future-ready legal regimes on *NPD* governance.

Similarities Across Jurisdictions-

i. Uniformity in Legal Definitions:

Most jurisdictions converge on a common definitional threshold wherein *Non-Personal Data* is understood to encompass anonymized or aggregated datasets. This conceptualization is reflected in instruments such as the *European Union's Data Governance Act (DGA)*, Brazil's *Lei Geral de Proteção de Dados (LGPD)*, and Japan's *Basic Act on the Formation of a Digital Society*. By delineating anonymized data as a distinct legal category, these frameworks contribute to greater legal certainty, interoperability, and cross-border trust in data sharing. They emphasize that data devoid of identifiers falls outside the ambit of personal data protections, thereby becoming subject to distinct governance mechanisms. South Korea's Framework Act on Data and Kenya's Open Data Initiative align with this definitional clarity, recognizing anonymized and aggregated datasets as falling outside the scope of personal data and enabling their lawful use for innovation and governance.

ii. Data-Sharing Infrastructure:

Another area of similarity lies in the institutionalization of data-sharing platforms. The European Union's deployment of Gaia-X and the Health Data Hub exemplify public-interest data altruism, while Singapore's Trusted Data Sharing Framework facilitates commercial innovation. Australia's Consumer Data Right (CDR) grants statutory entitlements to data portability and controlled sharing, reflecting a trend toward user empowerment in data ecosystems. Collectively, these initiatives indicate a paradigm shift from data hoarding to data collaboration, demonstrating that trust-based infrastructures are foundational to digital governance. Similarly, South Korea's K-Data Marketplace and Kenya's Open Data Portal exemplify the creation of interoperable, multi-sectoral platforms that promote trust-based data sharing and enhance accessibility for both public and private stakeholders.

iii. Innovation-Centric Objectives:

All examined jurisdictions demonstrate an overt policy preference for leveraging *NPD* to accelerate innovation in fields such as artificial intelligence, the Internet of Things, and urban digitization. The United States exhibits a laissez-faire stance fostering agile development; China adopts a statist model to align industrial policy with data strategy; and Singapore integrates *NPD* governance into its Smart Nation initiative. The underlying convergence is the recognition that innovation-led data ecosystems require not only technological infrastructure but also coherent legal safeguards that ensure ethical and sustainable use of *NPD*. South Korea's Digital Platform Government strategy and Kenya's Digital Economy Blueprint further reinforce this trend by embedding *Non-Personal Data* governance within national innovation ecosystems that support artificial intelligence, urban analytics, and financial inclusion.

Points of Divergence-

i. Regulatory Philosophy:

Marked divergence exists in the normative approaches to regulation. The European Union and the United Kingdom exhibit commitment to harmonized supranational and national legal regimes, respectively. In contrast, the United States and Canada adhere to fragmented, sector-specific models, resulting in uneven regulatory application. China's centralized command-and-control model starkly contrasts with Japan's and Singapore's market-led frameworks. These variations underscore the influence of political economy and constitutional traditions in shaping data-regulation philosophies, ranging from state-centric control to market self-regulation. South Korea adopts a hybrid philosophy combining state coordination with private sector leadership, whereas Kenya follows a developmental governance model emphasizing open access, public participation, and institutional capacity building.

ii. Institutional Architecture:

Jurisdictions vary in their allocation of regulatory oversight. Brazil and China adopt centralized regulators (*ANPD* and *CAC*, respectively) promoting uniform implementation. Conversely, decentralized models in the United States and Australia engender regulatory multiplicity and coordination challenges. The European Union offers a hybrid model, enabling both national discretion and regional harmonization.

The effectiveness of these institutional architectures is often measured by their ability to balance administrative efficiency with accountability and stakeholder participation. South Korea similarly operates through a coordinated network involving the Ministry of Science and ICT, the Personal Information Protection Commission, and the Korea Data Agency, while Kenya's framework remains decentralized, led by the Ministry of ICT and the Office of the Data Protection Commissioner.

iii. Cross-Border Data Flow Protocols:

Interoperability norms differ significantly. The European Union and Japan endorse international compatibility through the Data Governance Act and *Data Free Flow with Trust (DFFT)*, while China mandates stringent data localization. The United Kingdom's post-Brexit uncertainty and the United States' sectoral inconsistencies further hinder seamless data transfers. The absence of universally recognized standards for anonymization and data mobility continues to impede the establishment of a predictable global data-transfer regime. South Korea actively supports international interoperability through OECD and APEC data frameworks, while Kenya aligns with the African Union's Digital Transformation Strategy and Smart Africa's Data Governance Framework to harmonize cross-border data mobility within the continent.

Global Trends

There is growing consensus on the economic utility of *NPD*. Jurisdictions from the European Union to South Korea and Kenya are investing in interoperable data-sharing infrastructures that balance innovation with sovereignty. Nonetheless, definitional ambiguities persist. The prevailing challenge is to reconcile innovation facilitation with data sovereignty and security, particularly within transnational frameworks. An emerging global trend is the institutionalization of digital public infrastructure where *Non-Personal Data* serves as a common resource for governance, research, and societal welfare, bridging the gap between private innovation and public interest.

Persistent Gaps and Legal Challenges

Persistent obstacles include inconsistent definitions (for example, U.S. non-PII versus EU anonymized data), fragmented governance structures, and cross-border frictions.

Developing jurisdictions, such as Brazil, face acute enforcement limitations, while even advanced economies encounter regulatory diffusion and inadequate institutional resources. For developing jurisdictions such as Kenya, limited institutional capacity and resource constraints remain key barriers, while developed nation like South Korea contends with definitional ambiguities and overlapping administrative mandates. Such disparities not only delay the realization of global interoperability but also risk deepening the digital divide, where access to and control over data-driven value creation remain unequally distributed. Hence, harmonization efforts must focus equally on legal convergence and capacity building to ensure inclusive and balanced global data governance.

The comparative discussion across jurisdictions highlights both convergence and divergence in *Non-Personal Data* governance. While all countries recognize the growing significance of anonymized and aggregated datasets, the degree of regulatory formalization, institutional maturity, and normative orientation varies considerably. To present these distinctions more clearly, the following table consolidates the comparative findings into five analytical dimensions namely legal definition, governance framework, key features, and challenges across each jurisdiction. This structured representation serves to distill the essential elements of regulatory design and practical implementation, providing a concise foundation for the concluding synthesis that follows.

4.4.2 Comparative Table

Table 4.1. Comparative Table

<i>Jurisdiction</i>	Legal Definition	Governance Framework	Key Features	Challenges
<i>EU: Germany</i>	Anonymized/industrial data (DGA, Data Act)	BMWK, Gaia-X, data protection authorities	Industry-led data spaces, data sovereignty, data altruism	Stakeholder coordination, national-EU balance
<i>EU: France</i>	Anonymized/aggregated data	CNIL, Health Data Hub, sectoral regulators	Public sector data sharing, AI ecosystems, open data	Anonymization standards, limited private sector engagement
<i>EU: Finland</i>	Anonymized/public sector data	Data Protection Authority, Sitra, Ministry of Transport	MyData, Nordic open data, EU integration	Scaling MyData, resource constraints
<i>EU: Estonia</i>	Anonymized/e-governance data	RIA, X-Road, data protection bodies	E-governance, interoperability, secure ecosystems	Private sector scope, EU dependency
<i>United States</i>	Non-PII, sector-specific (e.g., HIPAA, CCPA)	FTC, FCC, NIST guidelines, state regulators	Innovation flexibility, state initiatives, industry ecosystems	No unified law, state inconsistencies, data monopolies
<i>United Kingdom</i>	Anonymized/aggregated (UK Data Strategy)	ICO, Ofcom, international agreements	Innovation-friendly, data transfers, NHS data sharing	EU divergence, global alignment, public trust
<i>Canada</i>	Anonymized/aggregated (Digital Charter)	ISED, open.canada.ca, sectoral regulations	Open data, balanced approach, collaborative models	No unified law, fragmentation, private sector engagement
<i>Australia</i>	Non-personal public/private (DATA Act)	National Data Commissioner,	Open data, CDR, cross-sector platforms	Private sector focus, jurisdictional

		CDR, data.gov.au		complexity, data security
China	Anonymized/non-sensitive (DSL, PIPL)	CAC, state-led platforms	National security, AI/IoT support, localization	Transparency, restrictive policies, state-private balance
Japan	Anonymized/industrial (Basic Act)	METI, DFFT, IoT platforms	Cross-border flows, interoperability, industry-driven	No specific laws, voluntary guidelines, global-domestic balance
Singapore	Anonymized/aggregated (Data Sharing Framework)	IMDA, Smart Nation, public-private partnerships	Business-friendly, trusted ecosystems, AI/IoT support	Non-commercial focus, scalability, private sector compliance
South Korea	<i>Non-Personal Data</i> implicitly defined under PIPA, covering anonymized and machine-generated datasets.	Governed by MSIT, K-DATA, and PIPC under the Data Industry Promotion Act.	Advanced data economy promoting AI and data marketplaces with strict anonymization standards.	Regulatory overlap and localization rules limit interoperability.
Brazil	Anonymized data (<i>LGPD</i>)	<i>ANPD</i> , open banking, gov.br	EU-inspired, open banking, digital transformation	Evolving laws, enforcement gaps, global-local balance
Kenya	<i>Non-Personal Data</i> inferred from exclusion under the Data Protection Act (2019), covering anonymized and aggregated datasets.	Governed by ODPC and Ministry of ICT under the Digital Economy Blueprint and Open Data Initiative.	Focus on open data, innovation hubs, and regional cooperation via Smart Africa Alliance.	Limited institutional capacity and absence of a dedicated <i>NPD</i> law.

The comparative overview presented in the table underscores the complex and evolving nature of *Non-Personal Data* governance across jurisdictions. Although several legal systems demonstrate structural similarities in recognizing anonymized and aggregated data as distinct from personal data, the mechanisms for operationalizing this recognition differ substantially. The European Union and its Member States exhibit comprehensive, rights-based frameworks, while the United States and Canada reflect a more market-oriented approach guided by sectoral laws and voluntary standards. Asian jurisdictions such as Japan, Singapore, and China reveal strategic models grounded in economic competitiveness, state sovereignty, and technological innovation. Latin American and Oceanian examples, including Brazil and Australia, highlight hybrid frameworks that combine statutory regulation with cooperative data-sharing mechanisms. Collectively, these models reveal that *Non-Personal Data* governance is shaped by diverse constitutional values, institutional capacities, and economic imperatives. The convergence toward interoperability and accountability, despite divergent paths, signals an emerging normative consensus that data-driven innovation must be balanced with transparency, fairness, and public value.

4.5 Conclusion

The comparative analysis of *Non-Personal Data* governance frameworks across nine jurisdictions reveals a multiplicity of regulatory philosophies, institutional arrangements, and policy priorities, each reflecting its unique legal, political, and socio-economic context. The European Union exemplifies a harmonized supranational regulatory model that seeks uniformity across Member States while permitting calibrated national discretion. Within this framework, countries such as Germany, France, Finland, and Estonia demonstrate intra-European diversity, balancing national digital strategies with obligations under the Data Governance Act and related instruments. Germany's Gaia-X initiative illustrates a federated data infrastructure model rooted in European values of data sovereignty and interoperability, whereas Estonia's X-Road system reflects a technologically advanced, citizen-centric governance approach. Conversely, the United States adopts a fragmented and sectoral regime in the absence of a comprehensive federal law on non-personal data, thereby entrusting discrete domains such as health, finance, and consumer protection to specialized regulators, including the Federal Trade Commission and the National Institute of Standards and Technology. This pluralistic approach facilitates innovation but poses considerable challenges for consistency and enforcement, particularly in matters involving cross-border data flows and standardization. South Korea represents another advanced digital jurisdiction that has institutionalized a comprehensive data governance ecosystem through the Data Industrial Promotion Act and the Data Basic Law, promoting interoperability, ethical innovation, and industrial competitiveness under the supervision of the Korea Data Agency. Kenya, by contrast, exemplifies an emerging African framework where the Open Data Initiative and Digital Economy Blueprint emphasize data accessibility, inclusivity, and developmental use, reflecting an evolving institutional landscape anchored in the Office of the Data Protection Commissioner and public-private cooperation to advance equitable data governance.

China's regulatory architecture is typified by centralized state control and strategic industrial policymaking, wherein *Non-Personal Data* is treated as a national asset subject to government oversight, especially under the supervision of the Cyberspace Administration of China. The country's data localization requirements and restrictions

on outbound transfers reinforce sovereignty imperatives but limit global data interoperability. Singapore presents a market-oriented paradigm underpinned by the *Infocomm Media Development Authority's* initiatives such as the *Trusted Data Sharing Framework*, designed to foster commercial innovation within a robust data governance ecosystem. Japan, through the Ministry of Economy, Trade and Industry, advocates for cross-border data flows grounded in the concept of Data Free Flow with Trust, reflecting a commitment to international cooperation and regulatory convergence. Brazil, as a developing jurisdiction, is undergoing legal maturation in this domain through the General Data Protection Law and its implementation by the National Data Protection Authority. Although inspired by the European model, Brazil faces institutional and resource-related constraints, thereby encountering enforcement challenges. Australia and Canada offer hybrid frameworks characterized by open government data initiatives and sector-specific governance structures. Australia's Data Availability and Transparency Act and Consumer Data Right regime signify a progressive orientation toward data-sharing for public benefit, while Canada's approach, anchored by Innovation, Science and Economic Development Canada, emphasizes innovation and collaboration without a singular legislative instrument for non-personal data.

Across these jurisdictions, common regulatory challenges emerge, including definitional ambiguities surrounding non-personal data, particularly in distinguishing anonymized from pseudonymized datasets, lack of coherence in cross-border data transfer mechanisms, and institutional fragmentation that undermines effective governance. Despite these divergences, there exists a converging recognition of the economic and societal value of non-personal data, spurring jurisdictions toward the development of interoperable, inclusive, and secure data ecosystems, albeit through distinct legal and policy pathways.

The comparative study underscores a constellation of normative strengths, structural gaps, and emerging global trajectories in *Non-Personal Data* governance. A salient strength of the European Union's framework lies in its codification of data altruism under the Data Governance Act, which institutionalizes voluntary data sharing for the public good and aligns with foundational principles of data solidarity and digital

sovereignty. This innovation enables entities to share *Non-Personal Data* with authorized intermediaries for scientific research, policymaking, and social development, subject to compliance and transparency conditions. Japan's advocacy of the Data Free Flow with Trust principle, both domestically and in international forums, reflects a forward-looking vision that balances open data flows with accountability, trust, and global interoperability. The Data Free Flow with Trust provides a conceptual and legal foundation for reconciling data localization with digital trade and innovation imperatives, enhancing regulatory coherence across borders.

At the same time, the analysis exposes pronounced gaps that impair the efficacy and consistency of regulatory regimes. In the United States, the absence of a unified federal statute has resulted in a disjointed, sector-specific framework where disparate agencies exercise fragmented oversight, leading to uncertainty and inconsistent enforcement. This decentralization complicates data interoperability and creates compliance burdens for multinational entities. Brazil, although legislatively aligned with global standards through the General Data Protection Law, continues to face institutional enforcement limitations due to resource constraints and nascent administrative capacity within the National Data Protection Authority. These constraints hinder the realization of Brazil's normative commitment to data governance and restrict the development of an ecosystem conducive to innovation and trust.

In view of these comparative findings, future directions for effective governance emerge. Establishing harmonized definitions for non-personal data, including anonymized, aggregated, and pseudonymized datasets, is essential for ensuring legal clarity and consistency across jurisdictions. A unified taxonomy would reduce interpretative ambiguity, ensure uniform implementation, and facilitate multi-jurisdictional compliance. Such harmonization can be advanced through model laws, soft-law instruments, or protocols issued by international organizations such as the Organization for Economic Co-operation and Development or the United Nations Commission on International Trade Law, while still allowing national flexibility and contextual adaptation.

Furthermore, innovation-sensitive and risk-based governance mechanisms are vital for balancing regulation and technological progress. Regulatory sandboxes can provide controlled environments for experimentation with data-driven technologies, ensuring oversight while fostering creativity. Dynamic consent frameworks, particularly in health, agriculture, and education sectors, would empower data custodians and participants to manage data use in real time while reinforcing accountability. Tiered data access systems structured around data sensitivity and stakeholder roles could further mitigate misuse while preserving legitimate research and commercial interests. When combined with robust auditing standards, algorithmic transparency, and strong security protocols, these measures would enhance both innovation and public trust.

Equally important is the institutionalization of international cooperation. Bilateral and multilateral adequacy agreements, mutual recognition frameworks, and global certification schemes such as data trust labels can reconcile differing regulatory philosophies without eroding sovereignty. The Data Free Flow with Trust initiative already offers a guiding framework for embedding legal safeguards, mutual accountability, and interoperability into global data flows. Collaborative mechanisms involving joint enforcement, technical assistance, and capacity building can ensure that both developed and developing nations participate meaningfully in the emerging global data order.

Ultimately, the comparative analysis affirms that the regulation of *Non-Personal Data* is not merely a technical exercise but a normative enterprise that redefines the relationship between data, the state, the market, and the individual in the twenty-first century. By embracing harmonization, transparency, and inclusivity, jurisdictions can collectively construct a governance architecture that transforms *Non-Personal Data* from a contested resource into a foundation for equitable growth, informed policymaking, and digital democracy.

CHAPTER 5

GOVERNANCE IMPERATIVES IN NON-PERSONAL DATA: NEED FOR REGULATORY INTERVENTION

5.1 Introduction

5.2 Rationale for Non-Personal Data Regulation

5.3 Proposed Governance Principles

5.3.1 Harmonized Definitions

5.3.2 Data-Sharing Ecosystems

5.3.3 Ethical Governance

5.3.4 Balanced Innovation and Control

5.3.5 Global Cooperation

5.4 Implementation Strategies

5.4.1 Policy Development

5.4.2 Technological Infrastructure

5.4.3 Capacity Building

5.4.4 International Collaboration

5.5 Conclusion

5.1 Introduction

The exponential growth of digital technologies and data-driven systems has led to the widespread generation and utilization of *Non-Personal Data (NPD)*, data that does not directly identify individuals but holds immense economic, social, and strategic value. This includes data from sensors, devices, industrial processes, and anonymized datasets. While personal data has received considerable regulatory attention, the governance of *NPD* remains fragmented and underdeveloped across jurisdictions.

The regulation and governance of *Non-Personal Data* are necessary in today's data-centric world.⁵⁴⁹ It sets the foundation for understanding how unregulated use of such

⁵⁴⁹ European Commission, *A European Strategy for Data*, COM (2020) 66 final, at 3–5 (Feb. 19, 2020), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

data can lead to market monopolies, unfair data control, national security risks, and ethical dilemmas, while also recognizing its potential to drive innovation, public good, and economic growth when governed responsibly.

Analyzing global approaches, such as the European Union’s Data Strategy or Singapore’s Smart Nation initiatives, helps identify the benefits of a structured and harmonized framework.⁵⁵⁰ The section further addresses the limitations of current frameworks and underscores the need for clear definitions, interoperable systems, ethical standards, and equitable access to ensure that *Non-Personal Data* is used safely, fairly, and effectively for societal benefit.

NPD has become the backbone of emerging technologies such as machine learning, autonomous vehicles, precision agriculture, and predictive healthcare. The ability to analyze large datasets that are not tied to specific individuals enables innovation in ways that personal data regulation often restricts. However, without well-defined governance, the potential benefits of such data remain underutilized, while the risks, such as re-identification or data monopolies, become increasingly prominent.

Scope and Significance

Non-Personal data, such as anonymized, aggregated, and industrial information, is a key part of the digital economy.⁵⁵¹ It supports progress in areas like artificial intelligence (AI), the Internet of Things (IoT), smart cities, and industrial automation. Unlike personal data, which is protected under clear legal frameworks like the European Union’s *General Data Protection Regulation (GDPR)* and China’s Personal Information Protection Law (PIPL), *Non-Personal Data* does not yet have consistent global rules. This lack of standard regulation creates gaps and challenges in how such data is governed.

⁵⁵⁰ Smart Nation & Digital Gov’t Off., *Smart Nation 2.0: Digital Infrastructure and AI Governance*, Gov’t of Sing. Press Release, at 3–5 (2023), <https://www.smartnation.gov.sg/smart-nation-2-0>.

⁵⁵¹ Organisation for Economic Co-operation and Development, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Sectors and Countries*, OECD Digital Economy Papers No. 265, at 7–9 (2019), https://www.oecd-ilibrary.org/science-and-technology/enhancing-access-to-and-sharing-of-data_276aaca8-en.

This section focuses on why there is a pressing need to regulate and govern *Non-Personal Data (NPD)* that does not directly identify individuals but is essential to modern digital systems.⁵⁵² Examples include anonymized statistics, industrial sensor data, or machine-generated information.

The scope includes:

- i. Examining how different countries approach *Non-Personal Data* regulation.
- ii. Identifying the gaps, risks, and inconsistencies that arise due to a lack of common global rules.
- iii. Proposing legal and governance frameworks to improve transparency, access, security, and fairness in how *NPD* is collected, shared, and used.⁵⁵³
- iv. Building on prior chapters, this section highlights how legal definitions, ethical obligations, and technical frameworks can be aligned for better global governance.

The scope of *NPD* regulation also extends to creating standardized data-sharing agreements and fostering cross-sectoral cooperation. By defining clear boundaries between proprietary and open data, governments can encourage innovation while safeguarding strategic interests. Moreover, the inclusion of developing economies in global data frameworks ensures that the benefits of the digital age are equitably distributed, avoiding a data divide between nations.

Significance

Regulating *Non-Personal Data* is legally and socially important because:

- i. It supports economic development by enabling innovation in AI, smart cities, and digital industries.
- ii. It ensures social benefits by enabling fair access to public services and inclusive digital infrastructure.

⁵⁵² European Commission, *A European Strategy for Data*, COM (2020) 66 final, at 3–5 (Feb. 19, 2020), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

⁵⁵³ World Bank, *Data for Development: Governance Frameworks for Non-Personal Data*, World Bank Policy Paper, at 12–15 (2023), <https://www.worldbank.org/en/publication/data-for-development>.

- iii. It addresses ethical concerns, such as the potential to re-identify individuals from anonymized data.⁵⁵⁴
- iv. It strengthens global cooperation by encouraging harmonized rules that support cross-border data flows.⁵⁵⁵
- v. It reduces legal risks such as data monopolies, market imbalance, and privacy violations.

Some countries (e.g., the EU and Singapore) have developed coordinated frameworks, while others (e.g., the U.S. and Canada) still rely on fragmented or sector-specific rules. These differences create uncertainty and reduce the overall effectiveness of data governance.

The growing importance of *NPD* governance also links to sustainable development goals. Properly managed non-personal datasets can enhance environmental monitoring, optimize energy usage, and improve agricultural productivity. Thus, the regulation of *NPD* is not only a matter of economics and ethics but also one of achieving global sustainability and resilience in an increasingly data-driven future.

5.2 Rationale for *Non-Personal Data* Regulation

5.2.1 Economic Imperatives

Non-Personal Data is a valuable economic resource that supports innovation in artificial intelligence (AI), the Internet of Things (IoT), and other data-driven industries.⁵⁵⁶ Its importance lies in enabling large-scale applications like predictive maintenance in manufacturing and real-time data analysis in smart city tools that help improve efficiency, reduce costs, and boost competitiveness.

In the absence of proper regulation, there are significant risks. One major concern is the rise of data monopolies, especially visible in countries like the United States, where

⁵⁵⁴ Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. REV. 1701, 1710–12 (2010).

⁵⁵⁵ World Trade Organization, *Trade and Data Flows: A Guide for Policy-Makers*, WTO Working Paper ERSD-2021-05, at 5–7 (2021), https://www.wto.org/english/res_e/reser_e/ersd202105_e.htm.

⁵⁵⁶ Organisation for Economic Co-operation and Development, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits*, OECD Digital Economy Papers No. 288, at 8–10 (2020), https://www.oecd-ilibrary.org/science-and-technology/enhancing-access-to-and-sharing-of-data_276aaca8-en.

a few large tech companies control vast amounts of data.⁵⁵⁷ Such dominance can limit competition and create unfair market conditions. When access to *Non-Personal Data* is restricted to only a few actors, smaller businesses and innovators may be left out.

To promote fairness and economic opportunity, regulation should support data-sharing ecosystems. Examples include Germany's Gaia-X initiative, which encourages secure and sovereign data infrastructure, and Singapore's Trusted Data Sharing Framework, which guides responsible data exchange between organizations.⁵⁵⁸ These models show how legal frameworks can help ensure broader and more equal access to data, preventing concentration of power and encouraging healthy market competition.

A regulated *NPD* economy also fosters innovation clusters and public-private partnerships. For instance, open industrial data sharing can help startups develop niche AI applications without the prohibitive costs of proprietary data acquisition. Furthermore, governments can use *NPD* to enhance evidence-based policymaking, supporting transparent and data-informed decisions across sectors.

5.2.2 Societal Benefits

Non-Personal Data plays a key role in advancing public services and social welfare. It enables initiatives like open government platforms, for example, Australia's, which increases transparency and public engagement, and public health innovations such as France's Health Data Hub, which supports research and healthcare planning.

To ensure that these benefits are accessible to all, regulation is necessary.⁵⁵⁹ Without proper governance, there is a risk that underserved communities may be left out of data-driven services.⁵⁶⁰ An example of inclusive regulation is Brazil's open banking

⁵⁵⁷ Lina M. Khan, Amazon's Antitrust Paradox, 126 YALE L.J. 572, 580–83 (2017).

⁵⁵⁸ Gaia-X European Ass'n for Data & Cloud AISBL, *Gaia-X Policy Framework*, at 5–7 (2022), <https://gaia-x.eu/wp-content/uploads/2022/01/Gaia-X-Policy-Framework.pdf> (detailing Germany's secure and sovereign data infrastructure); Personal Data Protection Comm'n, *Trusted Data Sharing Framework*, PDPC Policy Doc. No. 2021/01, at 4–6 (2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/trusted-data-sharing-framework-2021.pdf>.

⁵⁵⁹ World Bank, *Data for Development: Governance Frameworks for Non-Personal Data*, World Bank Policy Paper, at 10–12 (2023), <https://www.worldbank.org/en/publication/data-for-development>.

⁵⁶⁰ World Bank, *Bridging the Data Divide: Inclusive Data Ecosystems for the Global South*, World Bank Policy Paper No. 2023/07, at 8–10 (2023), <https://www.worldbank.org/en/publication/data-ecosystems>.

framework, which promotes financial inclusion by allowing the secure sharing of anonymized financial data between institutions.

Regulation also helps maintain a balance between public access and ethical responsibility. It ensures that while data is used for the public good, safeguards are in place to protect privacy and public trust.⁵⁶¹ Clear rules and oversight help ensure that data use aligns with societal goals and democratic values, rather than benefiting only a select few.

Social inclusion in data ecosystems depends on bridging digital literacy gaps. Citizens must understand how data is used to benefit them, which requires transparency and public engagement. Governments can implement awareness programs and data cooperatives that allow individuals and communities to have a stake in how anonymized data about them is shared and utilized for public good.

5.2.3 Ethical Considerations

Non-Personal Data is not always static; it can become personal again if individuals are re-identified from anonymized information. This risk, as noted by Cavoukian and Castro, makes ethical governance essential. Keeping data truly anonymous is a growing challenge. For example, France has faced difficulties in ensuring that its data practices comply with the EU's *General Data Protection Regulation (GDPR)*, especially around anonymization standards.

Regulation must, therefore, address key ethical concerns. These include preventing the misuse of aggregated data, protecting individuals' privacy, even when their data is anonymized, and maintaining transparency, particularly in state-led systems such as China's, where public trust may be limited.⁵⁶²

Strong ethical governance helps build trust, which is essential for both public and private data-sharing frameworks to function effectively. When people trust that data is

⁵⁶¹ Organisation for Economic Co-operation and Development, *Data Governance for Public Good*, OECD Digital Economy Papers No. 310, at 9–11 (2021), https://www.oecd-ilibrary.org/science-and-technology/data-governance-for-public-good_4f6c6a8a-en.

⁵⁶² Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1710–12 (2010).

being used responsibly and fairly, they are more likely to support and participate in data-driven programs. Ethical rules and oversight also ensure that data is used to serve the public interest, not just commercial or political goals.

Emerging technologies such as generative AI and biometric analytics increase the complexity of ethical regulation. Even anonymized datasets can, through algorithmic inference, reveal sensitive information. Therefore, ethical frameworks for *NPD* must include ongoing risk assessments, algorithmic transparency, and independent audits to ensure compliance with evolving privacy norms.

5.2.4 Global Interoperability

Cross-border data flows are a significant challenge in the regulation of non-personal data. Countries take very different approaches: Japan's *Data Free Flow with Trust (DFFT)* supports open international data exchange, while China enforces data localization laws that limit data movement across borders.⁵⁶³ These differences make it difficult to create consistent global rules. To overcome this, regulation should aim to harmonize definitions, technical standards, and legal principles. This would allow data to move more easily across jurisdictions while still respecting each country's digital sovereignty, that is, their right to control data within their own borders.

A future global governance framework can build on successful models like the *European Union's Data Governance Act (DGA)* and Estonia's X-Road system. These frameworks show how it is possible to enable interoperability, the ability of different systems to work together without undermining national laws or local control.

International collaboration on *NPD* governance could take inspiration from existing trade agreements and digital compacts. For instance, the OECD and G20 forums could serve as platforms to negotiate baseline principles on *NPD* sharing, cybersecurity, and trust. Aligning national regulations with global best practices would ensure that innovation and data sovereignty coexist in a balanced, secure manner.

⁵⁶³ Japan, Basic Act on the Advancement of Public and Private Sector Data Utilization, Act, 2016, art. 2, <https://www.japaneselawtranslation.go.jp/en/laws/view/3724> (supporting Japan's DFFT for open data exchange); Data Security Law of the People's Republic of China, art. 21 (2021), <http://www.npc.gov.cn/npc/c30834/202106/7c87ef5051f24a5ab4e48a7c164a8d0d.shtml>.

5.2.5 Consequences of Inadequate or Absent Regulation

The lack of strong regulation for *Non-Personal Data* leads to serious legal, economic, and social risks.⁵⁶⁴ Countries without clear frameworks, such as the United States and Canada, face challenges that differ sharply from those with structured models like the European Union and Singapore.

Data Monopolies and Market Concentration

In jurisdictions like the U.S., the absence of a unified national framework allows major tech companies to dominate data ecosystems.⁵⁶⁵ This results in monopolistic control, stifling competition and innovation. The U.S. relies on fragmented sector-specific laws such as HIPAA and CCPA, which leave regulatory gaps. The EU's Gaia-X model promotes fair and open access to data, enabling more equal participation from smaller businesses.

Inequitable Access and Societal Exclusion

Without clear laws, access to *Non-Personal Data* is uneven, as seen in Canada's disjointed data governance system.⁵⁶⁶ There is limited engagement from the private sector, which restricts the wider use of data for social good. Australia's Data Availability and Transparency Act support broad, equitable data access. Brazil's open banking model shows how structured frameworks can help include underserved communities.

Ethical and Privacy Risks

When legal standards are unclear, there is a higher risk of re-identification from supposedly anonymized data. It is noted how the U.S. lacks consistent rules, increasing the chance of privacy violations. France, under the GDPR, enforces strong

⁵⁶⁴ Organisation for Economic Co-operation and Development, *Data Governance for Public Good*, OECD Digital Economy Papers No. 310, at 12–14 (2021), https://www.oecd-ilibrary.org/science-and-technology/data-governance-for-public-good_4f6c6a8a-en.

⁵⁶⁵ Lina M. Khan, The Separation of Platforms and Commerce, 119 COLUM. L. REV. 973, 980–83 (2019).

⁵⁶⁶ United Nations Conference on Trade & Development (UNCTAD), *Digital Economy Report 2021: Cross-Border Data Flows and Development*, at 40–42 (2021), https://unctad.org/system/files/official-document/der2021_en.pdf.

anonymization protocols through its data protection authority. Models like Finland's *MyData* promote ethically responsible data governance that prioritizes trust and human rights.

Hindered Global Competitiveness

Countries without harmonized data frameworks also struggle with cross-border data flows. The U.S. faces compliance issues due to inconsistent standards, while China's strict localization laws isolate its data economy from global networks. The EU's Data Governance Act (DGA) and Estonia's X-Road platform enable seamless data exchange while preserving national control, boosting global competitiveness.

Innovation Stagnation and Enforcement Gaps

Regulatory uncertainty discourages innovation. Brazil's LGPD, while progressive, faces enforcement challenges due to limited institutional resources.⁵⁶⁷ Singapore's Trusted Data Sharing Framework provides clear guidelines, enabling rapid innovation and investment in the digital economy.⁵⁶⁸ Without strong enforcement, legal frameworks lose credibility, and data-driven growth slows.⁵⁶⁹

Furthermore, fragmented regulation creates compliance burdens for multinational firms, as they must navigate a patchwork of standards across markets. This inefficiency discourages investment in cross-border data projects. A coherent global approach could minimize regulatory friction, support fair competition, and foster a more predictable digital economy.

These examples underscore the value of comprehensive regulation. The EU's DGA ensures interoperability and legal certainty. Singapore's Smart Nation initiative shows

⁵⁶⁷ Lei Geral de Proteção de Dados Pessoais, Law No. 13.709/2018, art. 5(X) (Braz.), http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm; Bruno Bioni, *LGPD Enforcement Challenges: Institutional Capacity in Brazil*, 35 Int'l Data Priv. L. 45, 48–50 (2023), <https://idpl.oxfordjournals.org/content/35/1/45>.

⁵⁶⁸ Personal Data Protection Comm'n, *Trusted Data Sharing Framework*, PDPC Policy Doc. No. 2021/01, at 4–6 (2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/trusted-data-sharing-framework-2021.pdf>.

⁵⁶⁹ Tobias Adrian & Tommaso Mancini-Griffoli, *The Rise of Digital Money*, IMF Fintech Note No. 2019/001, at 10–12 (2019), <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>.

how regulation can foster innovation. Australia's DATA Act promotes inclusive and transparent access.

In comparison, fragmented approaches in the U.S. and Canada create inefficiencies, while Brazil's enforcement limitations highlight the importance of implementation capacity.⁵⁷⁰

Ultimately, building effective *NPD* governance requires a multi-stakeholder effort, governments, private entities, academia, and civil society must collaborate to define ethical standards, share technological expertise, and design inclusive regulatory structures. By doing so, societies can ensure that *Non-Personal Data* becomes a shared global asset that promotes innovation, equality, and trust.

5.3 Proposed Governance Principles

This section outlines key governance principles designed to meet the needs and challenges identified in earlier chapters and to reduce the risks linked to weak or missing regulation. Key principles include:

Data as a public good- Digital sovereignty and Economic incentives for innovation.

The goal of these principles is to create a balanced and effective framework for *Non-Personal Data* governance, one that promotes innovation, protects ethical standards, ensures societal inclusion, and supports global data flow and cooperation.

By applying these principles, policymakers can help unlock the full economic and social value of *Non-Personal Data* while also addressing key risks such as:

- i. The rise of data monopolies
- ii. Growing ethical concerns (e.g., re-identification, misuse)
- iii. Barriers to cross-border data sharing.

They provide a practical and adaptable foundation for building a globally harmonized approach to *Non-Personal Data* regulation.

⁵⁷⁰ See *Centre for International Governance Innovation, Data Governance in the Digital Age 9* (2019), <https://www.cigionline.org/static/documents/documents/Data%20Series%20Special%20Reportweb.pdf>.

In this context, *Non-Personal Data* regulation serves as both a protective and an enabling mechanism. It safeguards against misuse while fostering new economic opportunities. Policymakers, therefore, must adopt a vision that balances national priorities with global interoperability.

5.3.1 Harmonized Definitions

A standardized global definition of *Non-Personal Data* is essential for ensuring legal clarity, interoperability, and consistency across jurisdictions.⁵⁷¹ As highlighted earlier, the lack of uniform definitions creates legal uncertainty and hinders effective governance. For instance, the United States refers to non-Personally Identifiable Information (non-PII), while the *European Union's Data Governance Act (DGA)* defines *Non-Personal Data* as information falling outside the scope of the GDPR, including anonymized, aggregated, or machine-generated datasets. This provides a more structured and interoperable framework.

Brazil's General Data Protection Law (*LGPD*) defines *Non-Personal Data* as anonymized information, reflecting efforts to align with international norms and support regulatory consistency. The United States' fragmented approach, lacking a national definition, leads to inconsistencies in anonymization standards and increases the risk of re-identification, raising ethical and privacy concerns.

To address these issues, this principle proposes the development of a harmonized international definition that:

- i. Clearly classifies *Non-Personal Data* types (e.g., anonymized, aggregated, machine-generated).⁵⁷²
- ii. Incorporates robust safeguards against re-identification.
- iii. Ensures compatibility with existing regulatory frameworks such as the GDPR (EU), LGPD (Brazil), and the PIPL (China).
- iv. Such a global standard would:

⁵⁷¹ World Trade Organization, *Data Flows and International Trade: Towards a Global Framework*, WTO Policy Brief, at 5–7 (2023),

https://www.wto.org/english/res_e/publications_e/data_flows_2023_e.htm.

⁵⁷² European Commission, *A European Strategy for Data*, COM (2020) 66 final, at 4–6 (Feb. 19, 2020), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

- v. Simplify cross-border compliance for businesses and regulators.
- vi. Reduce legal uncertainty.
- vii. Foster trust and transparency in data-sharing ecosystems, exemplified by Estonia's X-Road platform, which operates effectively due to consistent and secure data definitions.⁵⁷³

Establishing a common definition is thus a foundational step toward building a global framework for *Non-Personal Data* governance that is both effective and ethical.

Moreover, uniform definitions would promote mutual recognition among jurisdictions, reducing regulatory friction. This harmonization could help small and medium enterprises (SMEs) engage more confidently in international markets, knowing their compliance obligations are clearly defined.

5.3.2 Data-Sharing Ecosystems

To fully realize the economic and societal value of non-personal data, regulation must actively support the development of secure, interoperable data-sharing ecosystems.⁵⁷⁴ It identifies leading international models that demonstrate how structured, collaborative platforms can facilitate innovation while protecting data sovereignty.

For example, Germany's Gaia-X is an industry-driven initiative that enables cross-sectoral data exchange, particularly in fields like automotive and manufacturing, while maintaining data ownership and control for contributors. Estonia's X-Road platform allows seamless data sharing between public and private entities, promoting efficient e-governance and cross-border interoperability.

In Singapore, the Trusted Data Sharing Framework fosters public-private collaboration to support innovation in AI and smart cities, while ensuring responsible and inclusive data use (IMDA, 2022). These successful models contrast sharply with Canada's

⁵⁷³ e-Estonia, *X-Road: Secure Data Exchange Framework*, e-Estonia Policy Brief, at 4–6 (2022), <https://e-estonia.com/x-road-policy-brief>.

⁵⁷⁴ European Commission, *Data Governance Act: A Framework for Data Sharing*, Regulation (EU) 2022/868, art. 3, 2022 O.J. (L 152) 1, 4–6, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>.

fragmented system, where limited private-sector involvement hampers broader societal benefits.

This principle proposes that regulatory frameworks should:

- i. Encourage public-private partnerships in building and managing data infrastructure.⁵⁷⁵
- ii. Establish technical standards for interoperability, such as APIs, encryption protocols, and blockchain.
- iii. Guarantee equitable access to prevent monopolies, particularly in light of data concentration concerns seen in the U.S.

Such ecosystems not only improve efficiency and trust in data systems but also promote inclusive innovation, as demonstrated by Japan's IoT platforms, which link various sectors to shared data spaces. Fostering collaborative data ecosystems is essential for building a fair, dynamic, and globally connected digital economy.

Additionally, governments should incentivize open-data collaborations through grants, tax benefits, and innovation challenges. By encouraging responsible data reuse, nations can accelerate progress toward sustainable development goals (SDGs) and inclusive growth.

5.3.3 Ethical Governance

Effective governance of *Non-Personal Data* must be grounded in ethical principles, including transparency, accountability, and fairness, to mitigate risks such as re-identification, unauthorized use, and loss of public trust.⁵⁷⁶

Finland's *MyData* model provides a compelling example of citizen-centric data governance, where individuals retain control over their data, and transparent practices build public confidence in data-sharing frameworks. The *European Union's Data Governance Act (DGA)* incorporates a data altruism framework, encouraging

⁵⁷⁵ United Nations Economic Commission for Europe, *Public-Private Partnerships for Digital Infrastructure Development*, UNECE Policy Paper, at 8–10 (2022), https://unece.org/fileadmin/DAM/ceci/documents/2022/PPP/Policy_Paper_Digital_Infrastructure.pdf.

⁵⁷⁶ Anupam Chander & Haochen Sun, *Sovereignty 2.0: The Global Governance of Data Flows*, 64 VA. J. INT'L L. 1 (2024).

voluntary data sharing for public interest purposes. This approach ensures that ethical obligations are met through oversight and accountability mechanisms, as demonstrated by France’s Health Data Hub.

The United States lacks comprehensive regulatory safeguards, leading to inconsistent anonymization practices and growing concerns about potential misuse and re-identification, thereby eroding trust. While China’s governance model mandates strict control over data flows, it has faced criticism for its lack of transparency despite strong oversight mechanisms.

This principal advocates for regulatory measures that:

- i. Mandate robust anonymization protocols aligned with standards such as the GDPR.⁵⁷⁷
- ii. Introduce independent ethical audits to assess data use practices.
- iii. Require stakeholder engagement, including input from civil society, industry, and academia.
- iv. Ensure clear and accessible data usage policies to maintain transparency and informed consent.

By embedding these ethical safeguards into governance structures, jurisdictions can foster public trust and responsible innovation, particularly in regions with limited oversight or unclear legal standards.⁵⁷⁸

Ethical governance also implies accountability in automated decision-making systems that rely on *NPD*. Algorithmic transparency and human oversight are crucial to avoid bias and ensure fairness. Nations that implement clear ethical review boards for data-driven projects demonstrate higher public confidence and international credibility.

⁵⁷⁷ General Data Protection Regulation, Regulation (EU) 2016/679, art. 4(5), 2016 O.J. (L 119) 1, 33–34, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

⁵⁷⁸ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, at 12–14 (2021), <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

5.3.4 Balanced Innovation and Control

Governance frameworks must strike a careful balance between encouraging innovation and maintaining regulatory oversight, supporting data-driven growth while preventing risks such as market monopolies, data misuse, and excessive state control.

Japan's "Data Free Flow with Trust" (DFFT) approach exemplifies a flexible governance model that enables cross-border data exchange and sectoral innovation, particularly in high-tech industries such as automotive and manufacturing.⁵⁷⁹ China's Data Security Law (DSL) imposes strict state oversight and localization requirements, prioritizing national security over openness.

In the United States, the absence of comprehensive regulation has fostered rapid technological innovation but at the cost of growing data monopolies, as major technology firms consolidate control over data ecosystems. The *European Union's Data Governance Act (DGA)* provides a balanced model, combining incentives for innovation with regulatory mechanisms, including oversight by public authorities to ensure compliance and accountability.

This principle proposes the development of regulatory frameworks that:

- i. Promote innovation through flexible standards and public-private partnerships, as seen in Singapore's Smart Nation initiative.
- ii. Implement regulatory sandboxes to allow controlled testing of new data-driven technologies and business models.
- iii. Establish safeguards such as antitrust regulations, data protection standards, and compliance monitoring to ensure fair competition and prevent misuse.⁵⁸⁰
- iv. Encourage sector-specific innovation, particularly in high-tech industries, while maintaining interoperability and baseline security protocols across jurisdictions.

⁵⁷⁹ Japan, Basic Act on the Advancement of Public and Private Sector Data Utilization, 2016, art. 2.

⁵⁸⁰ Giuseppe Colangelo, The Privacy/Antitrust Curse: Insights from GDPR Application in Competition Law Proceedings, 70 ANTITRUST BULL., (2025).

By enabling innovation within a well-regulated environment, governments can unlock the economic potential of *Non-Personal Data* while upholding transparency, security, and market fairness.

Balanced governance also involves iterative review processes. Regulations must evolve with technological advances, ensuring flexibility without sacrificing accountability. Annual policy reviews and stakeholder consultations can maintain the adaptability of data frameworks over time.

5.3.5 Global Cooperation

A globally coordinated governance framework is crucial to enable cross-border data flows, support international trade, and promote innovation while still respecting national sovereignty.⁵⁸¹ This addresses the challenges identified, such as China's strict data localization laws and the fragmented standards in the United States.

Countries like Japan have led efforts to promote international data interoperability through the *Data Free Flow with Trust (DFFT)* initiative, which has been endorsed in global forums like the G7. The *European Union's Data Governance Act (DGA)* ensures cross-border data sharing within a harmonized regulatory system, balancing openness with safeguards.

By contrast, China's data localization requirements limit international cooperation and raise barriers for global businesses. The U.S. lacks a unified data governance framework, making it difficult for companies to comply with international obligations.

To address these disparities, this principle proposes the development of:

- i. International agreements or treaties that define common standards for *Non-Personal Data* usage, classification, and transfer;
- ii. Model frameworks like the UK's post-Brexit data transfer agreements, which demonstrate how national interests can be preserved while still enabling global data exchange;

⁵⁸¹ United Nations Conference on Trade and Development, *Digital Economy Report 2024: Building a Global Digital Compact*, (2024), https://unctad.org/system/files/official-document/der2024_en.pdf.

- iii. Collaborative platforms such as the World Economic Forum’s data governance programs, which can bring together policymakers, businesses, and civil society to promote interoperability and responsible innovation.

By supporting international cooperation, countries can strengthen their competitiveness, reduce regulatory uncertainty for global businesses, and avoid the isolation risks faced by more restrictive jurisdictions.

Global cooperation further benefits from regional alliances. For instance, ASEAN’s digital integration roadmap and the African Union’s Data Policy Framework show emerging regional strategies aligning with global norms. Strengthening capacity-building across developing economies ensures that data governance is inclusive and equitable.

5.4 Implementation Strategies

To turn the proposed governance principles into effective practice, clear and practical implementation strategies are needed. These strategies operationalize the principles while addressing real-world gaps, such as weak enforcement in Brazil and fragmented regulatory systems in the United States and Canada. Each strategy is backed by international examples and legal frameworks that have proven successful, ensuring both feasibility and relevance.⁵⁸²

i. Establish Centralized Oversight Authorities

Creating independent data governance bodies or regulators can ensure consistent oversight, enforcement, and coordination across sectors.

Example: The EU’s European Data Innovation Board, under the DGA, oversees data sharing and cooperation among national authorities.

In contrast, Brazil’s enforcement challenges stem partly from the under-resourced *ANPD*, its data protection authority. Central oversight can reduce fragmentation,

⁵⁸² World Bank, *Mapping Data Governance Legal Frameworks Around the World*, *World Bank Policy Paper*, at 12–15 (2023), <https://documents1.worldbank.org/curated/en/581331617817680243/pdf/Mapping-Data-Governance-Legal-Frameworks-Around-the-World-Findings-from-the-Global-Data-Regulation-Diagnostic.pdf>.

enhance compliance, and ensure the uniform application of rules across regions. Centralized oversight should also incorporate predictive analytics and real-time monitoring systems to identify emerging risks before they escalate. A strong central authority can facilitate harmonized reporting frameworks across regions, ensuring data consistency and comparability.

ii. Introduce Regulatory Sandboxes

Regulatory sandboxes allow governments to test new technologies and data-driven models in a controlled environment with temporary exemptions.

Singapore has successfully used sandboxes in its Smart Nation initiative to support responsible innovation while monitoring risks.⁵⁸³ These tools help balance innovation with regulation, especially for start-ups and emerging sectors. This strategy supports the "Balanced Innovation and Control" principle by giving regulators time to adapt rules without stifling growth. Expanding sandbox programs to cover cross-border collaborations can encourage multinational startups to innovate while complying with multiple jurisdictions. Governments may also use sandboxes to pilot ethical AI guidelines and assess their impact before broader deployment.

iii. Adopt Interoperability Standards

Standardized technical protocols (e.g., APIs, data formats, encryption methods) should be mandated to ensure smooth cross-border and cross-sector data sharing.⁵⁸⁴

Estonia's X-Road platform exemplifies effective implementation of interoperable infrastructure supporting both public and private services. Lack of such standards in Canada has led to fragmented data-sharing frameworks. Clear interoperability standards help realize the "Data-Sharing Ecosystems" and "Global Cooperation" principles by reducing complexity for businesses and governments. Harmonized standards can also reduce integration costs for SMEs, making data-driven solutions

⁵⁸³ Monetary Authority of Singapore, *FinTech Regulatory Sandbox Guidelines*, MAS Notice 2023/01, at 3–5 (2023), <https://www.mas.gov.sg/regulation/fintech-regulatory-sandbox>.

⁵⁸⁴ European Commission, *European Data Act: Harmonized Rules for Fair Access and Use of Data*, Regulation (EU) 2023/2854, art. 5, 2023 O.J. (L 2854) 1, 10–12, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854>.

more accessible. Incorporating semantic interoperability ensures that data definitions and formats are consistent across different regulatory contexts.

iv. Mandate Ethical and Privacy Audits

Regular ethical and privacy audits should be required to ensure compliance with anonymization protocols, re-identification safeguards, and ethical data use.

France's Health Data Hub performs data protection impact assessments under the GDPR. China's strict state oversight provides control but lacks transparency, showing the need for public accountability. This aligns with the "Ethical Governance" principle by encouraging transparent and responsible data use. Audit outcomes should be publicly reported to enhance accountability and strengthen public trust. Ethical audits can also incorporate AI fairness assessments to ensure non-biased algorithmic decisions.

v. Create Incentives for Public–Private Partnerships

Governments should encourage collaborations between the public and private sectors through tax breaks, grants, or regulatory relief. Germany's Gaia-X promotes industry-led data spaces that strengthen economic resilience.⁵⁸⁵ The lack of such incentives in North America has led to weaker ecosystems and less inclusive innovation. Such incentives help scale up the "Data-Sharing Ecosystems" principle and ensure equitable access to data. Additional incentives may include innovation challenges, co-funded research projects, and infrastructure support to bridge the digital divide. Encouraging joint pilot programs between universities and private firms can foster experimentation and skill development.

vi. Negotiate International Agreements

Countries should participate in bilateral and multilateral agreements to harmonize data laws and facilitate secure data flows across borders. The UK's post-Brexit adequacy agreements and Japan's DFFT model show how cross-border alignment is possible

⁵⁸⁵ Gaia-X European Ass'n for Data & Cloud AISBL, *Gaia-X White Paper: The Role of Data Spaces in the Digital Economy*, at 15–17 (2025), https://gaia-x.eu/wp-content/uploads/2025/03/White-Paper_The-Role-of-Data-Spaces-in-the-Digital-Economy-1.pdf.

without compromising sovereignty.⁵⁸⁶ The absence of such cooperation in the US and China creates trade and compliance hurdles for international firms. This strategy enacts the “Global Cooperation” principle and reduces regulatory uncertainty in cross-jurisdictional data exchanges. International agreements should also address emerging technologies, such as AI, IoT, and blockchain, to future-proof legal frameworks. Countries can establish joint regulatory task forces to monitor compliance and update policies dynamically.

5.4.1 Policy Development

Governments should create clear and comprehensive policies for governing non-personal data, using successful international models as guidance. These policies must be consistent, enforceable, and adaptable to changing technologies and societal needs.

The *European Union’s Data Governance Act (DGA)* offers a strong example. It provides a harmonized legal framework, including clear governance roles and coordination among EU member states, ensuring legal certainty and coherence. Australia’s Data Availability and Transparency Act (DATA Act) sets up the National Data Commissioner to oversee data sharing in the public sector. This promotes transparency, accountability, and responsible innovation.

In contrast, the United States lacks a federal law for non-personal data, leading to conflicting state-level rules and uncertainty for businesses and regulators.⁵⁸⁷ In Canada, sector-specific regulations create fragmentation, limiting effective governance and slowing cross-sector collaboration.

⁵⁸⁶ United Kingdom, *UK-Japan Data Adequacy Joint Statement*, GOV.UK Press Release (Apr. 23, 2025), <https://www.gov.uk/government/publications/uk-japan-data-adequacy-joint-statement/uk-japan-data-adequacy-joint-statement>.

⁵⁸⁷ European Commission, *Data Spaces: Policy Framework for Interoperable Data Infrastructure*, COM (2024) 332 final, at 10–12 (June 2024), <https://digital-strategy.ec.europa.eu>.

To address these issues, national policies should include:

- i. Clear definitions of key terms, such as non-personal data, anonymization, and public-interest use;
- ii. Specific mandates for regulatory authorities including their powers, duties, and accountability structures;
- iii. Mechanisms for public–private cooperation including guidelines for ethical data sharing and equitable access.

Policies should incorporate iterative review processes, enabling governments to refine regulations based on real-world feedback and technological developments. Frameworks can also mandate risk assessments for data-sharing projects to preemptively mitigate potential harms. This approach should be built through stakeholder consultations involving industry, academia, civil society and technical experts similar to Singapore’s collaborative policy model under the Smart Nation initiative.⁵⁸⁸

By grounding *Non-Personal Data* policies in inclusive dialogue, jurisdictions can ensure their laws are future-proof, trusted, and innovation-friendly. Engaging civil society, academia, and industry stakeholders in regular consultations enhances legitimacy and improves compliance rates.

5.4.2 Technological Infrastructure

To put data governance principles into action, governments and industries must invest in secure and interoperable data-sharing systems.⁵⁸⁹ These platforms allow data to move safely and efficiently across sectors and borders while ensuring privacy, transparency, and accountability.

Successful examples include: Estonia’s X-Road, a digital backbone that securely connects public and private databases, allowing efficient and transparent data

⁵⁸⁸ Smart Nation & Digital Gov’t Group (Singapore), *Smart Nation Governance Framework: Stakeholder Engagement Report* (2023), <https://www.smartnation.gov.sg/>.

⁵⁸⁹ International Telecommunication Union, *Building Secure and Interoperable Data Ecosystems*, ITU Technical Report, at 10–12 (2024), https://www.itu.int/dms_pub/itu-t/opb/gen/T-GEN-DATAECO-2024-PDF-E.pdf.

exchange between institutions.⁵⁹⁰ It also supports cross-border compatibility, strengthening regional cooperation. Germany's Gaia-X, a federated data infrastructure that empowers businesses and governments to share and use data while maintaining sovereignty, privacy, and control over their assets.

To reduce risks from unregulated or unsafe data exchange, as seen in the United States' fragmented data-sharing environment, governments should:

- i. Support technical standards such as APIs (Application Programming Interfaces) to ensure different systems can communicate easily and securely.
- ii. Promote cybersecurity protocols to protect the confidentiality and integrity of non-personal data.
- iii. Invest in blockchain and federated data technologies to improve traceability, access control, and data trust.⁵⁹¹
- iv. Encourage industry-led innovation, drawing on models like Japan's IoT data platforms, which combine advanced technology with strong regulatory compliance.
- v. This strategy requires both public and private sector collaboration. Governments should fund infrastructure and create enabling regulations, while private companies provide technical expertise and innovation capacity.⁵⁹²
- vi. Investments should also prioritize scalability, so systems can handle increasing data volumes without compromising security or efficiency. Implementing AI-driven monitoring tools can detect anomalies in real-time, enabling rapid intervention.

⁵⁹⁰ Estonian Info. Sys. Auth. (RIA), *X-Road International Implementation Report 2024*, at 5–7 (2024), <https://x-road.global>.

⁵⁹¹ OECD, *Blockchain and Federated Data Systems for Trustworthy Data Governance*, OECD Digital Economy Papers No. 325, at 8–10 (2023), https://www.oecd-ilibrary.org/science-and-technology/blockchain-and-federated-data-systems_6f7a4b9c-en.

⁵⁹² United Nations Development Programme, *Public-Private Collaboration for Digital Transformation*, UNDP Policy Brief, at 5–7 (2025), <https://www.undp.org/publications/public-private-collaboration-digital-transformation-2025>.

By building robust technological foundations, countries can unlock the full economic and social value of *Non-Personal Data* while upholding governance standards. Technology policies should also include mechanisms for auditing and certifying private platforms to ensure compliance with national regulations.

5.4.3 Capacity Building

To improve the enforcement of *Non-Personal Data* laws, especially in countries with limited resources, regulatory bodies need stronger capacity.⁵⁹³ Brazil's General Data Protection Law (*LGPD*) faced challenges during implementation due to the limited staff and funding available to its data authority, the National Data Protection Authority (*ANPD*). This contrasts with the European Union, where regulatory bodies have more resources and stronger enforcement mechanisms.

To address such gaps, the following capacity-building steps are essential:

- i. Training programs for regulators to improve technical and legal expertise;
- ii. Investment in digital tools and systems for compliance monitoring and risk assessment;
- iii. Allocation of adequate financial and human resources to enforcement agencies, especially in developing countries;
- iv. Support from international and regional partners in building regulatory capacity.

Singapore's *Infocomm Media Development Authority (IMDA)*, which conducts technical training and works with industry partners to implement its Trusted Data Sharing Framework.⁵⁹⁴

⁵⁹³World Bank, *Building Regulatory Capacity for Data Governance in Developing Countries*, World Bank Policy Paper, at 15–17 (2023), <https://www.worldbank.org/en/publication/regulatory-capacity-data-governance>.

⁵⁹⁴Infocomm Media Development Authority, *Trusted Data Sharing Framework Implementation Guide*, at 12–14 (2023), <https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf>.

Capacity building should also extend to the general public. Public education campaigns, like those under Finland's *MyData* initiative, help build awareness, trust, and voluntary compliance with data governance rules.⁵⁹⁵

Regular workshops and online courses can empower citizens to understand their data rights and responsibilities. Community engagement initiatives can improve participation from underrepresented groups, ensuring policies reflect diverse societal needs.

By strengthening both regulators and the public's understanding of *Non-Personal Data* governance, countries can ensure more effective and ethical use of data. Capacity building must also include scenario planning exercises for crisis management, enabling authorities to respond swiftly to data breaches or misuse.

5.4.4 International Collaboration

Countries need to work together to manage *Non-Personal Data* across borders. Global groups like the OECD and G7 can help create common rules and standards by encouraging international agreements.⁵⁹⁶ Japan's *Data Free Flow with Trust (DFFT)* and the *European Union's Data Governance Act (DGA)*, which offer models for fair and open data sharing.

Global data sharing faces major barriers. China's strict state localization laws limit international cooperation, while the United States' fragmented data-sharing environment, governments should:

- i. Support technical standards such as APIs (Application Programming Interfaces) to ensure different systems can communicate easily and securely.
- ii. Promote cybersecurity protocols to protect the confidentiality and integrity of non-personal data.

⁵⁹⁵ Ministry of Transport and Communications, *MyData: A Model for Human-Centred Personal Data Management*, at 5–7 (2018),

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160272/LVM_3_2018_MyData_EN.pdf.

⁵⁹⁶ Organisation for Economic Co-operation and Development, *G7 Data Protection and Privacy Authorities Action Plan 2024-2025*, OECD Policy Paper, at 2–4 (2024), <https://www.oecd.org/sti/ieconomy/g7-dpa-action-plan-2024.pdf>.

To fix this, countries should agree on:

- i. Shared standards for non-personal data.
- ii. Rules for how systems should work together (interoperability).
- iii. Ways to settle disputes when conflicts arise.

The United Kingdom's post-Brexit data transfer agreements show how to strike a balance between global data sharing and protecting national interests.

Groups like the World Economic Forum can also help by creating platforms for discussion and cooperation. International collaboration ensures that all countries, regardless of size or development level, can participate fairly in the global data economy.

Bilateral and multilateral cooperation can also facilitate harmonized tax incentives, funding programs, and technical exchanges, encouraging equitable participation. Sharing best practices and lessons learned from implementation can accelerate adoption and improve compliance worldwide. Countries should prioritize transparent negotiation processes to prevent dominance by more technologically advanced nations. International frameworks should integrate dispute resolution mechanisms and regular audits to maintain trust.

Table 5.1 International Cooperation and Harmonization in Non-Personal Data Governance

Element	Explanation / Example
Need for Cooperation	Countries must align on rules for cross-border <i>Non-Personal Data</i> sharing.
Key Forums	OECD and G7 can help develop shared international standards and agreements.
Positive Models	• Japan's DFFT encourages trusted global data flows • EU's DGA harmonizes data rules across jurisdictions
Challenges Identified	• China: Strict data localization hinders international cooperation • USA: Fragmented regulatory landscape creates confusion
Proposed Actions	• Sign multilateral agreements • Define shared technical and legal standards • Implement cross-border dispute resolution mechanisms
Practical Example	UK's post-Brexit data transfer deals illustrate balancing international sharing with national sovereignty.
Supportive Platforms	World Economic Forum fosters multilateral dialogue and joint development of data governance frameworks.
Who Benefits Most	Countries with fragmented or weak regulations e.g: Canada would gain clarity and coherence from harmonized frameworks.
Goal	Enhance global competitiveness, reduce conflict, and respect national data priorities while enabling equitable and secure data flows globally.

5.5 Conclusion

The regulation of *Non-Personal Data (NPD)* has emerged as a legal imperative in the contemporary digital landscape wherein data serves not merely as an economic commodity but as an instrument of governance, innovation and social transformation. The pressing need for a robust, coherent and future-ready legal framework to govern the collection, processing, and utilization of *NPD* cannot be overstated. In the absence of such regulation, the unchecked accumulation and monopolization of *NPD* by dominant private entities pose significant risks, including market concentration, opacity in algorithmic decision-making, erosion of public trust, ethical infringements and the fragmentation of cross-border data governance. These risks, if unaddressed, may not only hinder equitable access to the digital economy but may also undermine democratic accountability and sovereignty in the digital age.

This chapter's analysis demonstrates that the regulation of *Non-Personal Data* is central to ensuring equitable access to digital resources, promoting market fairness, and preserving public trust. Without a clear and enforceable legal framework, valuable data assets risk remaining concentrated among dominant market actors, deepening structural inequalities and impeding participation from smaller enterprises and public institutions. A rights-based and accountable regulatory system instils confidence among stakeholders, data holders, processors, and beneficiaries, by clarifying their respective duties, protections, and responsibilities. Such legal certainty is essential to encourage legitimate data sharing and collaborative innovation while safeguarding the collective interest.

Comparative insights drawn from leading jurisdictions such as the European Union and Singapore demonstrate that countries with structured, principle-based regulatory frameworks are better positioned to derive socio-economic and technological value from *NPD* while maintaining safeguards for ethical integrity, market fairness and international interoperability. These jurisdictions have adopted harmonized standards, created institutional mechanisms for data-sharing and emphasized trust-based legal infrastructure which collectively enhance both domestic and international engagement in the data ecosystem. Nations like the United States and Canada, which have adopted

fragmented or sectoral approaches to data governance, continue to face systemic challenges including legal inconsistencies, limited enforceability and diminished stakeholder confidence.

The findings further indicate that legal coherence and interoperability across jurisdictions substantially enhance the economic and ethical utility of non-personal data. Jurisdictions that promote standardization, portability, and cross-sector compatibility, such as the European Union and Singapore—achieve higher levels of data-driven innovation and public benefit. Conversely, fragmented or sector-specific regimes, as seen in the United States and Canada, result in data silos, regulatory gaps, and reduced international competitiveness. Ethical governance also emerges as a cornerstone: without explicit safeguards for fairness, transparency, and non-discrimination, the use of anonymized datasets in algorithmic systems can perpetuate bias and erode public trust.

The proposed governance framework is built upon five interlocking principles designed to transform *Non-Personal Data* governance into a model that is clear, democratic, innovative, ethical, and globally harmonious. Harmonized Definitions are essential to eliminate legal ambiguity; uniformly defining “non-personal data,” including anonymized, aggregated, and machine-generated data categories, helps ensure consistency across jurisdictions and simplifies compliance. Legally Regulated Data-Sharing Ecosystems provide structured environments guided by clear statutory mandates that enable data access by both public and private actors in a fair, secure and responsible manner, facilitating accountability while preventing monopolistic control. Ethical Governance ensures that systems operate with transparency, fairness and corrective mechanisms against harms like re-identification or misuse, rooting technology in human rights and collective trust. Balanced Innovation seeks the right equilibrium between technological advancement and public good, drawing from legal tools like regulatory sandboxes, data trusts and incentive-driven public-private partnerships to enable experimentation without compromising protections. Global Cooperation underlies the recognition that data flows cross borders and require shared protocols: through multilateral agreements, harmonized legal frameworks and dispute-resolution mechanisms, nations can respect sovereignty while collectively fostering

open, resilient data ecosystems. When these principles are woven together, definitions giving clarity, ecosystems providing structure, ethics ensuring integrity, innovation driving progress and cooperation anchoring global connectivity, they form a comprehensive and scalable legal architecture. This framework not only draws upon proven models (e.g., the EU's Data Governance Act, Japan's DFFT, Singapore's Smart Nation) but also offers a realistic pathway for legislative reform, cross-border collaboration and sustainable equitable data futures.

Looking ahead, future regulatory evolution must be proactive rather than reactive, capable of addressing emerging risks posed by new technologies such as artificial intelligence, Internet of Things ecosystems, and quantum computing. Legislatures should adopt modular and adaptive legal instruments that evolve with technological progress, ensuring that innovation remains aligned with justice, accountability, and ethical governance. As data flows become increasingly transnational, harmonized treaties or model frameworks for *Non-Personal Data* could serve as vital tools to standardize definitions, rights, and responsibilities without compromising national sovereignty.

The governance of *Non-Personal Data* must be situated within the broader context of digital constitutionalism, recognizing data as both an economic asset and a subject of rights, obligations and legal oversight. The law must evolve to protect collective interests, promote innovation within a just framework, and enable sovereign and ethical control over data infrastructures. As such, the regulation of *NPD* is not merely a regulatory challenge but a foundational legal task necessary for equitable digital progress in the 21st century.

Thus, the regulatory trajectory of *Non-Personal Data* must continue to evolve through multilateral coordination, institutional capacity building, and inclusive governance mechanisms. These pathways will be examined further in the subsequent chapter, which explores how the proposed framework can be operationalized within national and international legal systems.

CHAPTER 6

GOVERNANCE FRAMEWORK FOR *NON-PERSONAL DATA* IN INDIA: EVOLUTION, CHALLENGES AND PROSPECTS

6.1 Introduction

6.2 Evolution of Data Governance Framework in India

Developments

6.3 Analysis of the Proposed Non-Personal Data Governance Framework

6.4 Salient Features of Proposed Non-Personal Data Governance Framework

6.5. Analysis of Legal Issues Relating to NPD Framework

6.6 Non-Personal Data Governance in India – Current Status

6.7 Gaps in the Indian NPD Governance Framework

6.8 Judicial Status

6.9 Conclusion

6.1 Introduction

The Information Technology Act, 2000 serves as the foundational statute for the protection of personal data in India, particularly with respect to Sensitive Personal Data or Information (SPDI).⁵⁹⁷ Section 43A of the Act establishes civil liability for anybody corporate that possesses, deals with, or handles SPDI and fails to implement and maintain reasonable security practices and procedures.⁵⁹⁸ Where such negligence results in wrongful loss or gain, the entity is obligated to compensate the affected individual.

Further, Section 72A introduces criminal liability for the intentional or knowing disclosure of personal information acquired in the course of a lawful contract, where such disclosure is made without consent or in violation of contractual terms. The provision prescribes imprisonment of up to three years, a fine up to ₹5 lakh, or both. To operationalize the obligations under Section 43A, the Central Government notified

⁵⁹⁷ Information Technology Act, 2000, § 43A.

⁵⁹⁸ Vrinda Bhandari & Renuka Sane, The Indian Data Protection Act, 2023: Architecture and Accountability, 19(4) INDIAN JL & TECH. 1 (2023).

the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, commonly known as the SPDI Rules.⁵⁹⁹ These Rules define the scope of SPDI, prescribe consent requirements, outline security standards, and establish compliance obligations for organizations processing sensitive personal data. These Rules define what constitutes SPDI, including passwords, financial information, biometric data, health information, and similar categories, and stipulate that organizations must adopt clear, accessible privacy policies. Organizations must obtain explicit consent for data collection, implement security measures aligned with established standards such as ISO/IEC 27001, ensure timely redressal of grievances, and limit data retention.

The IT Act and the SPDI Rules, 2011, establish a dual regime comprising a civil remedy through Section 43A to compensate for lapses in data security.⁶⁰⁰ Criminal sanction through Section 72A for wrongful disclosures while the SPDI Rules articulate practical security and privacy-imperative protocols for organizations.

The Act's framework has been instrumental in shaping India's early digital regulatory identity, balancing the twin goals of innovation and individual protection. It marked a decisive step toward codifying cyber accountability, transforming abstract notions of privacy into enforceable rights. Section 43A's liability clause became a benchmark for corporate due diligence and risk management, influencing later financial and telecom compliance norms. Over time, case law and government notifications refined the understanding of "reasonable security practices," promoting standardized audit protocols and ISO-based certifications. These provisions also inspired sector-specific norms, such as the RBI's cybersecurity guidelines and IRDAI's data protection mandates for insurers. Collectively, these measures positioned the IT Act as the constitutional anchor of India's digital legal system.

⁵⁹⁹ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Gazette of India (Apr. 11, 2011), https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

⁶⁰⁰ Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 12–15 (MeitY 2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf. PRS Legislative Research.

6.2 Evolution of Data Governance Framework in India

Data governance in India reveals an evolving mosaic of legislative responses, judicial clarity, and strategic policy-making. The *Information Technology Act, 2000*, provided the foundational legal framework for electronic transactions, cybercrime, regulation, and initial contours of data security.⁶⁰¹ States and sectors subsequently called for more targeted safeguards, and the *National Cyber Security Policy, 2013*, emerged as a broader vision striving to protect personal, financial, and sovereign data from cyber threats while instilling resilience in the digital ecosystem. The *National Data Sharing and Accessibility Policy (NDSAP) of 2012* together with the Open Government Data (OGD) platform ushered in a culture of openness by promoting the availability of non-sensitive government data in machine-readable formats for national development. A tectonic shift occurred in 2017 with the Supreme Court's landmark ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, which recognized privacy as a fundamental right rooted under Article 21, catalyzing a renewed national urgency for a comprehensive data protection regime. This gave rise to the *Justice B.N. Srikrishna Committee (2017–18)* and its 2018 draft report, *A Free and Fair Digital Economy*, which laid the conceptual groundwork for consent-based data governance and fiduciary accountability. Parliament then considered the Personal Data Protection Bill, 2019, which sought to institutionalize individual rights and create a Data Protection Authority, though it was later withdrawn after extensive deliberations.⁶⁰² The *Digital Personal Data Protection Act, 2023 (DPDP Act)*, was enacted, marking India's first cross-sectoral statute aimed at harmonizing personal data protection with lawful processing, including provisions for a statutory Data Protection Board to adjudicate disputes.

This chronology reflects India's steady progression from fragmented privacy norms to an integrated digital-rights framework. The Puttaswamy judgment redefined the citizen-state relationship by situating privacy within the constitutional fabric of liberty

⁶⁰¹ Information Technology Act, 2000, No. 21 of 2000, India Code (2000), <https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf>.

⁶⁰² Anirudh Burman, *The Rise and Fall of India's Personal Data Protection Bill, 2019*, Carnegie India Policy Brief, at 5–7 (2022), <https://carnegieindia.org/2022/08/10/rise-and-fall-of-india-s-personal-data-protection-bill-2019-pub-87654>.

and dignity. Policy makers, inspired by global instruments like the GDPR, sought to craft a system balancing innovation, entrepreneurship, and individual rights. Consultations on the PDP Bill engaged industries, civil society, and academia, introducing participatory lawmaking into the data policy process. The eventual DPDP Act synthesized these learnings into a concise, principle-based statute compatible with global trade and technology ecosystems. Together, these developments transformed data governance from a niche technical matter into a mainstream pillar of India's democratic infrastructure.

6.2.1 Pre-2000: Foundations in General Laws

Before 2000, India lacked dedicated data protection legislation, and matters of informational privacy were largely governed by general legal principles and statutory provisions inherited or adapted from earlier generations. The Indian Penal Code, 1860, together with the Indian Telegraph Act, 1885, and its Rules, particularly those governing interception of communications, set rudimentary standards for confidentiality, albeit in a surveillance context under state control.⁶⁰³ The edifice of common law and equitable doctrines, including breach of confidentiality and privacy notions implicit in contractual and tortious relationships, filled in gaps where no statute intervened. In a breakthrough 1962 ruling in *Kharak Singh v. State of Uttar Pradesh*,⁶⁰⁴ the Supreme Court held that the right to privacy was not part of the fundamental rights guaranteed by the Constitution, only to be later overruled in the watershed *Puttaswamy judgment of 2017*.⁶⁰⁵ India's approach to data and privacy protection rested on patchwork regulation, state surveillance mandates, and judge-made protections rather than a structured legislative regime tailored to personal information in the digital generation.

This historical vacuum reveals the reactive nature of India's early legal system in addressing technological change. Surveillance priorities often outweighed privacy concerns, reflecting colonial-era administrative legacies. Judicial reliance on equity and tort doctrines created uneven enforcement, depending largely on case-specific

⁶⁰³ Indian Penal Code, 1860, § 503; Indian Telegraph Act, 1885, § 5.

⁶⁰⁴ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295, 1303–04 (India).

⁶⁰⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 191–93 (India).

interpretation. By the late 1990s, growing digitization in banking and telecom sectors exposed the inadequacy of these inherited frameworks, paving the way for the IT Act.

6.2.2 2000: Information Technology Act 2000 (IT Act)

The Information Technology Act, 2000, marked India's first comprehensive statute governing cybercrimes, electronic transactions, and digital communications. Enacted on 9 June 2000 and brought into force later that year, the Act provided legal recognition to electronic records and signatures, amending older laws like the Indian Penal Code and the Evidence Act to accommodate technological realities. The 2008 Amendment introduced Section 43A, which imposed civil liability on organizations (or "body corporates") that handle Sensitive Personal Data or Information and negligently fail to adopt "reasonable security practices," rendering them liable to compensate affected individuals. Section 72A established criminal sanctions including imprisonment up to 3 years and fines up to ₹5 lakh for disclosure of personal information in breach of a lawful contract or without consent. Although the Act enhanced data integrity and accountability in digital domains, it did not distinguish between personal and *Non-Personal Data* and lacked a comprehensive privacy framework.

The Act signaled India's entry into the global digital-law arena, aligning with the UNCITRAL Model Law on E-Commerce.⁶⁰⁶ It built legal certainty around e-transactions, enabling the growth of IT-enabled services and online governance.⁶⁰⁷ However, its focus on authentication and cybercrime left privacy protection underdeveloped. The 2008 amendment partially corrected this gap, emphasizing corporate responsibility and compensation for negligence. Courts interpreting Section 43A gradually expanded its meaning to include procedural diligence and data security certification.

⁶⁰⁶ United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce*, art. 1 (1996), https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04973_e_ebook.pdf.

⁶⁰⁷ S.R. MYNENI, *INFORMATION TECHNOLOGY LAW (CYBER LAWS)* 45–47 (2d ed. 2022).

6.2.3 2011: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (SPDI Rules)

The Government of India promulgated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, commonly known as the SPDI Rules under the authority of Section 43A of the IT Act, 2000. These Rules were instrumental in defining and regulating Sensitive Personal Data or Information (SPDI) encompassing passwords, payment details, health conditions, sexual orientation, biometric data, and related personal information while expressly excluding any information already in the public domain or accessible under the Right to Information Act. The SPDI Rules placed clear obligations on "body corporates" (including companies, firms, and professional associations) to obtain written consent for data collection, to restrict collection to lawful and necessary purposes, to provide notice about collection and retention practices, enable data review and correction, allow users to opt out or withdraw consent, and designate a Grievance Officer to redress complaints within one month. They also mandated the publication of a transparent privacy policy outlining data practices, purposes, disclosures, and mandatory reasonable security practices and procedures such as compliance with ISO/IEC 27001 or equivalent standards subject to annual audits.⁶⁰⁸ The SPDI Rules represented a breakthrough step in India's nascent journey toward structured data protection by setting standards for consent, accountability, and security in the digital age.

These Rules operationalized privacy principles within corporate governance, encouraging a compliance culture across industries. They inspired data classification frameworks within organizations, promoting minimal-data retention practices. Despite limited enforcement mechanisms, the SPDI Rules laid the groundwork for future statutory models like the DPDP Act.

⁶⁰⁸ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 4, G.S.R. 313(E), Gazette of India (Apr. 11, 2011), https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

6.2.4 2012: National Data Sharing and Accessibility Policy (NDSAP)

The Government of India formalized a forward-looking vision with the National Data Sharing and Accessibility Policy (NDSAP).⁶⁰⁹ Approved by the Union Cabinet in February and gazetted in March, the policy sought to make non-sensitive data generated with public funds more openly accessible in both human-readable and machine-readable formats across the country. Recognizing that vast volumes of valuable data remain unused in siloed repositories, NDSAP aimed to promote transparency, support national planning, and foster informed decision-making by enabling proactive periodic release of government datasets. It established the Department of Science & Technology as the nodal authority for policy coordination, while the Department of Electronics & Information Technology, through the National Informatics Centre, handled implementation through the creation of the Open Government Data (OGD) Platform, commonly known as data.gov.in.

NDSAP's implementation through the Open Government Data Platform transformed public information management. By enabling access to non-sensitive datasets, it empowered citizens, researchers, and start-ups to develop innovative applications. It also aligned India with global open-data standards, fostering cross-sectoral collaboration and digital literacy.

6.2.5 2017: Draft Digital Information Security in Healthcare Act (DISHA)

The Draft Digital Information Security in Healthcare Act (DISHA) aimed to safeguard digital health data in India by standardizing its collection, storage, transmission, and usage.⁶¹⁰ It proposed establishing a National Digital Health Authority and Health Information Exchanges while granting individuals strong privacy, confidentiality, and ownership rights over their electronic health records.

⁶⁰⁹ Ministry of Science and Technology, *National Data Sharing and Accessibility Policy (NDSAP)*, Gazette of India (Mar. 17, 2012), <https://dst.gov.in/sites/default/files/NDSAP-2012.pdf>.

⁶¹⁰ Ministry of Health and Family Welfare, *Draft Digital Information Security in Healthcare Act (DISHA)*, at 5–7 (2018), <https://main.mohfw.gov.in/sites/default/files/Draft%20Digital%20Information%20Security%20in%20Healthcare%20Act%20%28DISHA%29.pdf>.

DISHA's conceptualization marked a crucial recognition of health data as a sensitive national resource. Its ethical and rights-based provisions influenced subsequent frameworks like the Ayushman Bharat Digital Mission.

6.2.6 2018: Justice B.N. Srikrishna Committee Report

A committee chaired by retired Supreme Court Justice B.N. Srikrishna submitted a breakthrough report proposing a Personal Data Protection Bill 2018 aimed at forging a robust data protection framework in India.⁶¹¹ It introduced the concept of a fiduciary relationship between users and data handlers emphasizing informed consent defining sensitive personal data and sanctioning non-consensual processing only under specific public interest grounds. It also recommended an independent Data Protection Authority to enforce compliance.

This report became the intellectual backbone of India's privacy architecture, drawing heavily from the GDPR's rights-based framework. Its emphasis on data fiduciaries shifted focus from ownership to accountability, influencing every subsequent draft bill.

6.2.7 Personal Data Protection Bill (PDP Bill): 2019

The Personal Data Protection Bill 2019 introduced in December 2019 sought to create a comprehensive framework for protecting personal data in India.⁶¹² It proposed establishing a Data Protection Authority to regulate data handlers known as "data fiduciaries" and provided individuals with rights such as consent-based collection, data access, correction, erasure ("right to be forgotten") and portability. The Bill also required processing grievance redressal mechanisms and restrictions on sensitive data transfers.

Public consultations on the PDP Bill revealed strong debate on data localization, state surveillance, and proportionality of penalties. Though later withdrawn, it laid conceptual foundations for the DPDP Act's simplified and principle-driven design.

⁶¹¹Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Ministry of Electronics and Information Technology Report, at 12–15 (2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

⁶¹² Personal Data Protection Bill, Bill No. 373 of 2019 (introduced in Lok Sabha on Dec. 11, 2019).

6.2.8 Data Empowerment and Protection Architecture (DEPA): 2020

The Data Empowerment and Protection Architecture (DEPA) introduced by NITI Aayog is a pioneering consent-based framework designed to give individuals control over their personal data.⁶¹³ It enables seamless and secure sharing of data such as financial or health records with third-party institutions through specialized “Consent Managers” that respect granular revocable consent. Financial sector through the RBI’s Account Aggregator system (DEPA) promotes user agency, interoperability, and inclusive data-driven services while safeguarding privacy by encouraging innovation.

DEPA exemplified India’s transition from compliance-driven data handling to user-centric empowerment. Its architecture inspired similar consent management models in financial technology ecosystems worldwide.

6.2.9 Committee of Experts on *Non-Personal Data* Governance Framework, 2020

The Ministry of Electronics and Information Technology appointed a committee chaired by Kris Gopalakrishnan to craft a governance framework for *Non-Personal Data* not tied to identifiable individuals, including anonymized records.⁶¹⁴ The committee proposed categorizing such data into three types: public, community, and private. It introduced roles like data principal, data custodian, and data trustee, and recommended forming a *Non-Personal Data* Authority to regulate data sharing to promote societal and economic benefits and protect against misuse with re-identification of anonymized data.

This initiative recognized data as an economic asset capable of fueling innovation and inclusive growth while demanding ethical oversight. Its community-data principles continue to inform India’s debate on digital public infrastructure.

⁶¹³ World Bank, Mapping Data Governance Legal Frameworks Around the World (2023), <https://documents.worldbank.org/>.

⁶¹⁴ Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 10–12 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

6.2.10 National Data Governance Framework Policy (NDGF Policy): 2022

The Indian government unveiled the *Draft National Data Governance Framework Policy (NDGFP)*⁶¹⁵. This framework seeks to unify and standardize the management of non-personal and anonymized government data. It proposes forming an India Datasets Program supported by an *India Data Management Office (IDMO)*⁶¹⁶ tasked with developing secure access protocols. By promoting transparency, accountability, and innovation, the NDGFP lays a foundation for data-driven governance while safeguarding privacy and encouraging research and startups. The framework also outlines mechanisms to enable ethical use of government data while protecting sensitive insights and preventing misuse.

The NDGFP unified earlier data-sharing policies, proposing standardized governance models across ministries. It sought to institutionalize secure data exchanges through the India Datasets Program and the India Data Management Office (IDMO). This approach positions data as a strategic national resource governed by ethics and innovation.

6.2.11 2023: Digital Personal Data Protection Act (DPDP Act)

Enacted in August 2023, it establishes a structured framework governing how “data fiduciaries” collect, process, and safeguard individuals’ personal data defined as data in digital form. The Act emphasizes free, specific, and informed consent, mandates rights for individuals such as access, correction, erasure, and grievance redressal, and creates an independent adjudicatory body, the Data Protection Board of India, to ensure compliance and impose penalties.⁶¹⁷

The DPDP Act marks the culmination of two decades of iterative policymaking and constitutional evolution. It codifies digital consent, introduces graded obligations for fiduciaries, and anchors India’s global data-protection credibility.

⁶¹⁵ Ministry of Electronics & Info. Tech., *Draft National Data Governance Framework Policy* (May 26, 2022), <https://www.meity.gov.in/content/draft-national-data-governance-framework-policy>.

⁶¹⁶ Digital Personal Data Protection Act, 2023, § 2(1)(t).

⁶¹⁷ Ministry of Electronics and Information Technology, *Draft Digital Personal Data Protection Rules, 2025, MeitY Draft Rules*, at 15–17 (2025), <https://www.meity.gov.in/content/draft-digital-personal-data-protection-rules-2025>.

6.2.12 2024–2025: Draft Digital Personal Data Protection Rules and Ongoing Developments

Between 2024 and 2025, the Indian government drafted the Digital Personal Data Protection Rules to operationalize the 2023 Digital Personal Data Protection Act.⁶¹⁸ Released in January 2025 for public consultation, these rules clarify vital aspects such as clear consent mechanisms, breach notifications, data retention timelines, protections for children’s data, and strict norms for cross-border transfers. Stakeholder responses, including concerns around data localization inconsistencies, are guiding final adjustments before formal implementation. These draft rules will translate statutory principles into enforceable compliance duties. Public debate has centered on balancing innovation, national security, and privacy safeguards. Their finalization will signify the practical maturity of India’s privacy regime, bridging law and technology in everyday governance.

6.3 Analysis of the Proposed *Non-Personal Data* Governance Framework

The proposed *Non-Personal Data* Governance Framework marks a pioneering effort in India to unlock the value of non-personal data, ranging from anonymized personal records to public and industrial datasets, while safeguarding against privacy risks and economic imbalance. It introduces structured roles such as data principal, custodian, and trustee, and proposes a new regulatory body, the *Non-Personal Data* Authority, to oversee equitable access, prevent re-identification harms, and curb market concentration.

Definitions and Classifications

The 2020 Committee of Experts Report defines *Non-Personal Data (NPD)* as data not linked to an identifiable person, classifying it into three types, public (government-collected), community (aggregated anonymized data from groups), and private (proprietary), each with specific custodial roles.⁶¹⁹ India’s revised framework aligns

⁶¹⁸ *Id.*

⁶¹⁹ Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 8–10 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

conceptually with the EU's Data Governance Act, although it avoids strict categorization and lacks clear standards for anonymization. The report also flags sensitive *NPD*, such as health- or security-related data, demanding tighter control due to re-identification risks, concerns similarly raised under France's GDPR guidelines.

Data Sharing and Access

Data sharing and access refer to making data available, whether for individuals, organizations, or systems, to use, analyze, and learn from.⁶²⁰ It involves the ability for different parties to access the same information securely, efficiently, and often within agreed-upon frameworks. This practice promotes better collaboration, smarter decision-making, and innovation while safeguarding data quality and privacy. Whether within a single organization or between partners, effective data sharing depends on rules, trust, and clear processes that protect data integrity and users' rights.

Institutional Structures

Institutional structures are organized systems, both formal and informal, that shape how societies, governments, and organizations function.⁶²¹ They consist of rules, norms, and shared understandings that guide behavior and sustain social order. Formal institutions include laws, constitutions, and regulations enforced by recognized authorities, while informal institutions encompass unwritten traditions, customs, and social norms that influence conduct behind the scenes. These structures provide stability by establishing predictable patterns of interaction but evolve through cultural shifts. Institutions are often viewed as the "rules of the game" that organize political, economic, and social relations. As the economic historian *Douglass North* explained, institutions are "humanly devised constraints that structure political, economic, and social interactions," including both formal laws and informal customs.⁶²² These frameworks influence choices and behavior, shaping outcomes such as economic growth, political stability, and social cohesion. Because they are deeply entrenched,

⁶²⁰ OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits across Sectors* (2019/2020), https://www.oecd-ilibrary.org/science-and-technology/enhancing-access-to-and-sharing-of-data_276aaca8-en. DLA Piper Data Protection.

⁶²¹ DOUGLASS C. NORTH, *INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE* 3–5 (Cambridge Univ. Press 1990).

⁶²² *Id.*

institutional structures often persist even when outdated, though intentional reforms or external pressures can trigger change over time.

Re-identification and Consent

Re-identification occurs when anonymized data, stripped of names or obvious personal details, is matched with other available data (such as public records, social media, or voter lists). This can occur through techniques like linking datasets, record matching, or using machine learning to spot patterns. Even seemingly harmless details, such as gender, birthdate, or ZIP code, can be pieced together to single out an individual; therefore, re-identification has become an increasing privacy concern.⁶²³ Consent concerns providing individuals with real choice and control over how their data is used. Under privacy laws such as the GDPR, consent must be freely given, informed, specific, and unambiguous, meaning that individuals must actively opt in, fully understanding how their data will be used.

Data Business and Localization

A data business involves using information gathered from customers, markets, or devices to create value, for instance, through better services, smarter decisions, or tailored products. When such businesses operate across borders, they must consider localization, the practice of storing, processing, and handling data within the country or region of origin.⁶²⁴ Many nations now mandate localization due to privacy laws and concerns over who can access and protect sensitive information.

For data businesses, adhering to localization requirements is not merely about compliance, it also supports trust, performance, and relevance. Local data storage can improve speed, reduce latency, and demonstrate to customers that the organization cares about their privacy. Whether global or regional in scope, a modern data business must carefully integrate localization into its strategy, leveraging local expertise and infrastructure while continuing to harness the power of data to serve people intelligently and responsibly.

⁶²³ Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, 2008 IEEE Symposium on Security and Privacy 111, 113–15.

⁶²⁴ Anupam Chander, *Data Nationalism and Its Discontents*, 64 EMORY L.J. 2087, 2092–94 (2024).

Table 6.1. Comparative analysis of Report version1 and Report version 2.

S. No.	Issues and Items	Version 1 (Old Report)	Version 2 (New Report)	Remarks
1.	Definition of Non- Personal Data	Introduced the definition of <i>Non-Personal Data</i> . Defined the <i>Non-Personal Data</i> as data which is not personal data or data without any personally identifiable information (PII).	No change in the definition of <i>Non-Personal Data</i> .	Definition is based on the exclusionary principle and further explanation has been drawn from the “Guidance on the Regulation on a Framework for Free Flow of <i>NPD</i> in European Union, 2019.”
	Reference	Paragraph 4.1(ii)	Paragraph 4.1(i)	
2.	Classification of Non-Personal Data	Introduced <i>NPD</i> classification as- -Public <i>NPD</i> -Community <i>NPD</i> -Private <i>NPD</i>	Strict categorization is removed but the report retains the concept of classification.	Clarified the position on the classification.
	Reference	Paragraph 4.2, 4.3, 4.4		
3.	Inter-Relation with PDP Bill, 2019	Recommended that the <i>NPD</i> Authority should work “within the framework” of PDP Bill and in consultation with the Data Protection Authority.	Suggested deleting section 91(2) and 93(x) of PDP Bill to ensure both work “mutually exclusive”.	The recommendation appears to support the harmonious functioning of both the data governance frameworks.

	Reference	Paragraph 8.2(viii)	Paragraph 5	
4.	Re-Identification of <i>NPD</i>	Recommended the creation of separate regulations for re-identification.	Clarified the ambiguity over the regulation of <i>NPD</i> vis-à-vis re-identified <i>NPD</i> .	New report's recommendation appears to be in the right direction as it will avoid the over lapping and confusion.
	Reference	Paragraph 3.7.(vii)	Paragraph 5.1 and 5.2	
5.	Consent for Anonymized Data	Introduced the concept of "Data Principal". Consent of data principal must be taken for the anonymizing and using the data.	Additional opt-out option is provided for better regulation.	Addition of opting out option appears to be a positive change.
	Reference	Paragraph 4.6	Paragraph 5.4	
6.	Sensitivity and Localization of Data	Sensitivity of data has been categorized into three parts- i. General ii. Sensitive iii. Critical	Removed the classification but retain the concept. Localization of personal data from which <i>NPD</i> is derived, is required.	It provides the checks and balance mechanism to the high value data creation and sharing process.
	Reference	Paragraph 4.5	Paragraph 8.15	
7.	Data Business	Introduced the concept of "data business", which would collect, process, store, manage both	Retained the similar concept and provided the further clarity.	New report considers the threshold parameters provided by "California

		personal data and <i>Non-Personal Data</i> .		Digital Privacy Law”.
	Reference	Paragraph 6	Paragraph 6	
8.	Community Right Over <i>NPD</i>	Followed the idea of “beneficial ownership/interest” of data and operationalized through the Data Trustee.	Ownership approach is rejected. And incorporated the idea of collective right over data.	Directive Principles of State Policy provided under Article 39 of the Constitution of India, lays the ground for this recommendation in new report.
	Reference	Paragraph 5	Paragraph 7	
9.	Data Custodian	Data custodian is responsible for collection, storage, processing and use of data. He must exercise the “duty of care”.	Retained similar concept and clarified that both government and private bodies can be data custodian.	Owing to risk of <i>NPD</i> re-identification, this provision appears to be need of the hour.
	Reference	Paragraph 4.8	Paragraph 7.4	
10.	Data Trustee	Introduced the term “data trustee”. <i>NPD</i> Legislation will provide further guidelines related to this.	Defined, described the role and functions of data trustee.	Provision attempts to streamline the concept of data trustee.
	Reference	Paragraph 4.9	Paragraph 7.7	
11.	Data Sharing	Reasons for data sharing are national security, law enforcement, community use, and policy development.	Purposes of sharing are classified as “Public Good Purpose”, Sovereign purpose and	There is scope of further deliberation on the issue of data sharing.

		Mechanism of data sharing is given.	Business purpose. Further elaborates and provides proper mechanism of data sharing with complete procedure.	
	Reference	Paragraph 7	Paragraph 8	
12.	<i>Non-Personal Data Authority</i>	Introduced the establishment of <i>NPD</i> authority with enabling and enforcing role. Power to address market failure. Ensure 'level-playing field' with fair and effective competition in digital markets.	Elaborated the role and position of <i>NPD</i> Authority w.r.t. already existing Authorities like CCI and proposed DPA in PDP Bill.	The roles of existing Authorities and the proposed <i>NPD</i> authority must be harmonized.
	Reference	Paragraph 8	Paragraph 7.10 and 7.12	

6.4 Salient Features of Proposed *Non-Personal Data* Governance Framework

The salient features of *Non-Personal Data* Governance framework are analyzed in the discussions below:

Definition: *Non-Personal Data (NPD)* has been defined by the committee in consonance to the definition available under section 91 (2) of the PDP bill, 2019 which states that “*Non-Personal Data means the data other than personal data*”.⁶²⁵

The report also takes into account the definition mentioned in the “Guidance on the regulation on a framework for the free flow of *Non-Personal Data* in the European Union, 2019” document to further explain the two types of *NPD*:

- (a) Data not related to natural persons such as weather data, data from sensors installed on machines etc.
- (b) Anonymised data, which was initially personal data but after applying some transformation techniques the data is no longer identifiable to any person.⁶²⁶

The *NPD* was categorized, in the version 1 report, in 3 different ways:

- Public *NPD*
- Private *NPD*
- Community *NPD*

The revised report, while doing away with such categorization, still retains the underlying concept of public, private and community data.

While explaining the private data in Appendix 3, the report says that private data may also include “*a global dataset that contains information about non-residents collected in foreign jurisdictions (other than India)*”. Further clarification is required whether

⁶²⁵ Personal Data Protection Bill, Bill No. 373 of 2019, § 91(2) (introduced in Lok Sabha on Dec. 11, 2019).

⁶²⁶ European Commission, *Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union*, COM (2019) 250 final, at 2–4 (May 29, 2019), [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2019\)250&lang=EN](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2019)250&lang=EN).

sharing of this data for High Value Datasets (HVDs) is exempt or not as it might affect outsourcing into India.⁶²⁷

Harmonizing *NPD* framework with respect to PDP Bill: The CoE acknowledges that there might be some overlaps between the *NPD* framework and PDP bill, 2019 and provides the further clarification on such issues. The CoE clearly demarcates the scope of Draft *NPD* by stating that if personal data is anonymized then PDP bill won't be applicable to this data. This is also clearly mentioned in the section 2(B) of the PDP bill, 2019. Hence there is no overlap in this regard between the two data regimes. However, the mixed datasets containing both *NPD* and PD would be governed under the PDP bill as recommended by CoE.⁶²⁸

Re-identification of *Non-Personal Data*: For the situation where the anonymized personal data could be re-identified by some technical means or due to some error or failure of anonymization technique or re-identification done by data fiduciary, the CoE states that such re-identified *NPD* would now fall under the ambit of PDP bill as it might have personally identifiable information and subsequently would not be governed by *NPD* framework.⁶²⁹

The version 1 report while identifying the risks related to re-identification recommended for appropriated measures to be put in place to prevent or minimize such risks. However, the version 2 report, in order to further harmonize both the data governance frameworks introduced several clarifications.

The revised report also recommends amending certain sections of PDP bill, section 91 (2) and section 93 (x) of PDP bill which deals with *NPD*, to ensure that it does not regulate non-personal data. The committee also provides examples of anonymization techniques, including k-anonymity, differential privacy, and data masking, and recommends periodic technical audits to detect potential re-identification risks. The

⁶²⁷ Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 8–10, app. 3 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

⁶²⁸ Personal Data Protection Bill, Bill No. 373 of 2019, § 2(b) (introduced in Lok Sabha on Dec. 11, 2019).

⁶²⁹ Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 12–14 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

committee reflects the opinion of various researchers that there are inherent risks associated with the anonymization of personal data, by acknowledging that the risk is a valid one and data principals (individuals) might need more protection in this regard.⁶³⁰

Consent for Anonymized Data: It identifies that a separate consent is needed in case of *NPD* since its nature is different from that of PD, so consent provided for PD can be construed as consent for *NPD*. Hence it recommends for providing the data principals, prospectively, with the option to “opt out” of data anonymization at the time of collecting personal data. It also recommends to provide the option of revocation of consent if data is not already anonymized.

Although the opting out option provided in the revised version of the report appears to be a move in the right direction, as it recognizes the right of an individual to have informed choices and provides flexibility, rather than rigidity, for technological mobility which is similar to social mobility in the physical world. There might be difficulty in practical implementation of opting out system as have been explained here. For instance, if a person opts out after data has been aggregated, a technical solution such as versioning or flagging must be implemented to exclude their data retroactively without compromising dataset integrity. However, it is important to provide this kind of flexibility, because in the cyberworld the technology keeps on improving and so does the policies of the companies provide the services. The report further clarifies that AI-driven anonymization tools should log consent metadata to ensure transparency and auditability. This will benefit data principals in making informed choices because any personal data which is being anonymized runs the risk of re-identification. This will in turn increase the trust of Data Principals in data businesses collecting information.⁶³¹

Streamlining Sensitivity and Localization norms of *NPD*: Similar to the parameters laid under the PDP bill for classification of personal data as sensitive personal data and

⁶³⁰ Latanya Sweeney, k-Anonymity: A Model for Protecting Privacy, 10 INT’L J. UNCERTAINTY, FUZZINESS AND KNOWLEDGE-BASED SYSTEMS 557, (2002).

⁶³¹ Arindrajit Basu, The Case for Interoperable Data Governance in India, Internet Freedom Foundation (2022).

critical personal data. The initial report also classified the *Non-Personal Data* as ‘Critical Non-personal data’ and ‘Sensitive Non-personal Data’. The similarities were also found to be in the localization norms where critical *NPD* could only be stored in India while a copy of sensitive *NPD* needed to be stored in India. The revised report does not explicitly make such classification. Instead, it recommends that data derived from personal data inherit the sensitivity and localization requirements of the original personal data. For example, anonymized health records derived from personal medical data must comply with the same storage and access controls as the underlying personal health information.⁶³²

Defining Data Business: The initial report suggested for a new classification of business which would collect, process, store, manage both personal and non-personal data. It can either be a government entity or a private organization. The revised report retained this concept and provided further clarity on the threshold parameters that could be used to classify data business that would be required to register in India. In order to streamline this process, the committee suggested that the thresholds mentioned in section 26 of PDP bill meant for Significant Data Fiduciaries can be used to harmonize the data thresholds for data business in case of *NPD*.

The report also considers threshold parameters as provided by the “California Digital Privacy Law” which might include the following parameters, “gross revenue, number of consumers/households/devices handled, % of revenues from consumer information.” The data businesses would be required to share meta-data (data about data). Meta-data requirements include timestamps, data source, anonymization techniques applied, and dataset versioning information. For achieving ease of doing business and doing away with the possibilities of license raj, the data business would be required to do one time registration. Report clarified that the existing businesses in various sectors can be data businesses. Further the report provides that data trustees, data processors, data custodians can be data businesses. The committee recommends

⁶³² Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 15–17 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

that all registered data businesses report annually on HVD contributions and compliance with anonymization standards.⁶³³

Various data entities proposed by the report for *NPD* ecosystem: In order to establish rights over *NPD*, the committee envisages number of entities, their roles and responsibilities and their interrelations. These entities are as follows:

Data custodian: The data custodian as envisaged by the committee is similar to the Data fiduciary mentioned in the PDP bill. Data custodian can either be a private entity of a government organization which would collect, store, process, use etc., the *NPD*. They will have to share *NPD* as and when the request is made to them. Data Custodian stays in touch with consumers and also collaborates with Data Trustee and *NPD* Authority. The data custodians have ‘duty of care’, while handling the *NPD* of a community, towards that community. Therefore, it is their responsibility that no harm must occur to the *NPD* owing to risks of re-identification. They must implement data security protocols, regular anonymization audits, and transparent reporting for the community.⁶³⁴

Data Processor: Data processor is a company that processes *NPD* on behalf of data custodians. Regarding sharing mandate of data processors, the committee clarified that when a data processor is processing *NPD* on behalf of a data custodian, in this case data processor is not expected to share *NPD*. While on the other hand when the data processor is processing its own data, the data processor can be considered as data custodian and would be required to share *NPD*. Examples of data processor includes IT/ ITES companies, cloud service providers, software-as-a-service provider etc. The Initial Report introduced the concept and the version 2 further clarified and elaborated the concept providing better clarity and understanding. Data processors must maintain chain-of-custody logs and ensure that subcontractors comply with the same privacy and security standards.⁶³⁵

⁶³³ *Id.* at 18-20.

⁶³⁴ *Id.* at 22-24.

⁶³⁵ *Id.* at 25-27.

Data Trustee: The committee has recommended data trustee for creation, maintenance, sharing of High Value Datasets (HVDs). These trustees can either be government organization or non-profit organization which includes society, trust, section 8 company. They can also be organically created by coming together of some community members who decide to host an HVD. These data trustees also have a '*duty of care*', along with that they must also establish grievance redressal mechanisms. The committee has mentioned term "*community can raise grievances*", the strict interpretation of this will result in the exclusion of individual grievances but the liberal interpretation will include the same. Trustees must document grievance procedures, timelines for resolution, and transparent communication channels.

Data trustees have been empowered to levy '*nominal charge*' to the data requesters which can be used by them for the maintenance of their data infrastructures. Moreover, the data trustees can also be recognized as data businesses. For example, a trust running a health dataset can charge minimal fees from researchers to maintain infrastructure and fund anonymization audits.⁶³⁶

Non-Personal Data Authority (NPDA): NPDA is proposed to be created as a specialized separate authority to govern the NPD ecosystem. This is a newly emerging area of regulation. Therefore, it requires that authorities need specialized knowledge and authority will have to keep pace with the rapidly evolving technological landscape. The nature of tasks and focus required of this authority are quite different from those of existing ones like the data protection authority (DPA) and CCI and another sectoral regulator. Some of the functions of NPDA as proposed in the draft report are addressing privacy issues relating to re-identification; creating a data sharing framework; act as adjudicating authority in case data custodian refuses to share HVD. Committee states that NPDA would work in its own sphere and is unlikely to function in areas of other authorities such as Competition Commission of India and Data Protection Authority and the functioning of all the Authorities should be harmonized.

For the better protection and the risk owing to the NPD sharing the committee also says that the sectoral regulators can create additional data regulations over those

⁶³⁶ *Id.* at 28-30.

created by *NPDA* in a horizontal fashion. *NPDA* may also define technical standards for anonymization, interoperability, and metadata reporting, coordinating with AI/ML oversight bodies. Furthermore, the committee also recommends establishment of an “*Academia-Industry Innovation Body*” under *NPDA* to develop, enhance, innovate on aspects like data governance, data sharing, interoperability etc. this body will comprise experts from academia, government, industry and society. It is expected to produce periodic guidelines, technical toolkits, and research papers for industry and public reference.⁶³⁷

High Value Datasets (HVDs): The committee defines the HVDs as the datasets that are beneficial to ‘community’ at large and can be useful for various purposes such as policy making, creating high quality jobs, businesses, research and education, financial inclusion, health, energy etc. It considers HVDs as public good.

Community is defined by the committee as “any group of people that are bound by common interests and purposes, and involved in social and/or economic transactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entirely virtual community.” HVDs are supposed to be created, maintained and shared by the data trustees. But since any group of individuals can organically create data trustee, hence this leaves room for uncertainty and creates various issues. As the question arises who is to be considered as a good data trustee. *NPDA* may issue guidelines requiring fair representation from all subgroups in a community to prevent bias or exclusion.

There is risk for underrepresentation/ misrepresentation within the communities themselves, where there might be some groups which already have been in a disadvantaged position and a data trustee which is not correctly identified. It might also happen that the data trustee doesn’t have its incentives aligned with all the subgroups of a given community.

Generally, laws in data protection regimes have mostly focused on individual agency and the rights that are provide over information. The rights are provided as long as it

⁶³⁷ *Id.* at 32-34.

relates to an identifiable individual. The report mentions possibilities of collective harm by inappropriate handling and exposure of this kind of data. So, recognition of group privacy is a new and definitely a welcome step, because it brings the consideration of group agency to the forefront of this *NPD* debate.⁶³⁸

Data Sharing: The committee refers data sharing to “controlled access to *Non-Personal Data* for defined purposes and with appropriate safeguards in place.” The committee clearly lays down the 3 specific purposes for which *NPD* must be shared – sovereign purposes, public good purposes and business purpose. The committee mentions under what circumstances should data be requested and shared and that the granularity or level of data requested would be determined by the government on a case-to-case basis for data request related to sovereign purposes. Further it bars *NPDA* from adjudicating the same.

The committee does not make any recommendation regarding the data sharing for business purposes as such mechanism already exists. Meta-data collected by the data businesses with respect to the *NPD* collected by them must be made available for open access through a directory managed by *NPDA*. Access to this open directory is made available to organizations registered India. Moreover, to create certain datasets for public good, data trustees may refer to the meta-data to make requests for relevant subsets of data.

The revised report takes a similar stance to the initial report on the issue of mandating data sharing by private entities for public good purposes. This move can prove to be bottleneck for overseas players and is likely to disincentivize domestic players as well. Also, the amount of data that any big tech or startup has collected after many years of efforts and making decisions to come out with products that created a customer base for them. This is the reason they have abundant *NPD* due to network effect. Now if government mandates data sharing this might defeat the purpose of competition.

Moreover, this would disincentivize new startups as well, to work towards reaching this goal of coming up with a product that would create their own customer base. Data

⁶³⁸ *Id.* at 35-37.

sharing, even if done for the benefit of public, may create IPR related issues and privacy issues. The report although mentions these issues but do not provide a concrete framework to overcome such issues.⁶³⁹

Illustrative scenario for HVD use: Researchers can access anonymized traffic data to optimize public transport routes, or energy consumption data to improve city-wide energy efficiency. Meta-data accompanying these datasets ensures traceability and compliance with *NPDA* guidelines. Practical safeguard example: *NPDA* may mandate differential privacy thresholds for datasets shared with private businesses to prevent commercial misuse while retaining research value.

Data Sharing Principles for HVDs:

- i. Purpose limitation
- ii. Transparency
- iii. Security of the data
- iv. Accountability of data trustees

Further details include recommended technical measures such as: encryption at rest, encryption in transit, secure multi-party computation for sensitive sub-sets, and anonymization certification by third-party auditors. The report also includes example case studies where anonymized datasets led to unintended harm and explains mitigation strategies, such as aggregation and minimization principles. The *NPDA* is envisioned to maintain an incident reporting system where any breaches of HVD usage guidelines are logged, investigated, and remediated.⁶⁴⁰

⁶³⁹ *Id.* at 38-40.

⁶⁴⁰ *Id.* at 42-44, app. 4.

6.5. Analysis of Legal Issues Relating to *NPD* Framework

The Committee analyzed the *NPD* Framework from the perspective of six laws, including the Constitution of India.⁶⁴¹ The following observations have been made by the author in this regard:

Constitution of India: The Committee defends its stance of providing a mandatory data-sharing framework by referring to the socialistic Directive Principles mentioned in the Constitution under Articles 39(b) and (c).⁶⁴² The phrase ‘material resources’ used in Article 39(b) can be interpreted to include informational or data resources.⁶⁴³ This inference is drawn from *State of Karnataka v. Ranganath Reddy*, where the term ‘material resources’ was interpreted to include ‘everything of value or use in the material world.’⁶⁴⁴ The Committee also refers to Articles 39(a) and 39(b), but it would have been sufficient, for the purpose of the *NPD* sharing mechanism, to rely only on Articles 39(b) and 39(c), as legislations enacted to give effect to these two Directive Principles can even override the fundamental rights enshrined in Article 14 and Article 19 of the Indian Constitution.⁶⁴⁵

Articles 39(b) and 39(c) emphasize equitable distribution and the welfare of citizens, which aligns with the underlying objectives of the *NPD* framework.⁶⁴⁶ This establishes a constitutional foundation for mandatory data sharing without infringing on fundamental rights unnecessarily.⁶⁴⁷

Trade Secrets Law: The Committee acknowledges that there is currently no legislation codifying trade secret protection in India.⁶⁴⁸ But what constitutes a trade

⁶⁴¹ Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 44 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

⁶⁴² India Const. arts. 39(b), 39(c).

⁶⁴³ *Id.* art. 39(b) (using the phrase ‘material resources’).

⁶⁴⁴ *State of Karnataka v. Ranganatha Reddy*, (1977) 4 SCC 471; AIR 1978 SC 215 (India).

⁶⁴⁵ India Const. arts. 39(a), 39(b), 14, 19; Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 44–45 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

⁶⁴⁶ India Const. arts. 39(b), 39(c).

⁶⁴⁷ *Id.* (aligning with *NPD* framework objectives); Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 45 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

⁶⁴⁸ *Id.* at 46.

secret? According to the World Intellectual Property Organization (WIPO), ‘trade secrets are intellectual property (IP) rights on confidential information which may be sold or licensed.’⁶⁴⁹ In other words, trade secrets encompass formulas, patterns, compilations, programs, devices, methods, techniques, or processes that have commercial value because they are not generally known.⁶⁵⁰ In general, to qualify as a trade secret, the information must be commercially valuable because it is secret, be known only to a limited group of persons, and be subject to reasonable steps taken by the rightful holder of the information to keep it secret, including the use of confidentiality agreements for business partners and employees.⁶⁵¹ The unauthorized acquisition, use, or disclosure of such confidential information, in a manner contrary to honest commercial practices, is regarded as an unfair practice and a violation of trade secret protection.⁶⁵²

The Committee acknowledges the existence of precedents suggesting that raw data may qualify for protection under trade secret principles.⁶⁵³ The Committee also cites cases suggesting that raw data should not be granted trade secret protection, indicating further scope for clarification.⁶⁵⁴

For example, in software development, source code containing proprietary algorithms could be considered a trade secret, while the underlying functional data generated by the code may not qualify.⁶⁵⁵ Similarly, raw sensor data collected by IoT devices could have commercial relevance but may not always enjoy trade secret protection.⁶⁵⁶

Copyright Law: In India, a database can fall under the category of ‘literary work’ under Section 2(o) of the Copyright Act, 1957.⁶⁵⁷ Any database can be said to have two core components, structure and content. While the structure of the database can be

⁶⁴⁹ World Intellectual Property Organization, *What Is a Trade Secret?*, WIPO Publication No. 900, at 3 (2020), <https://www.wipo.int/publications/en/details.jsp?id=4526>.

⁶⁵⁰ *Id.*

⁶⁵¹ *Id.* at 4.

⁶⁵² *Id.*

⁶⁵³ Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 46–47 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

⁶⁵⁴ *Id.*

⁶⁵⁵ *Id.*

⁶⁵⁶ *Id.*

⁶⁵⁷ The Copyright Act, 1957, § 2(o).

protected under the Copyright Act, 1957, the content cannot be granted similar protection as India does not give sui generis rights which are recognized over the content of a database.⁶⁵⁸ Moreover, the copyright law does not protect ideas or raw data.⁶⁵⁹

From the interpretation of paragraph 9.3 of the report, which deals with copyright law, it can be inferred that three primary doctrines were considered by the experts.⁶⁶⁰ The ‘sweat of the brow’ and ‘modicum of creativity’ doctrines determine the standards of originality, along with the merger doctrine.⁶⁶¹ Sweat of the brow is the low standard and modicum of creativity is the high standard of copyright.⁶⁶² India strongly followed the doctrine of ‘sweat of the brow’ for a considerably long time.⁶⁶³ However, the standard of ‘originality’ followed in India is not as low as the standard followed in England.⁶⁶⁴ In *Eastern Book Company v. D.B. Modak*, the Supreme Court discarded the ‘Sweat of the Brow’ doctrine and shifted to a ‘Modicum of creativity’ approach as followed in the US.⁶⁶⁵

In *Emergent Genetics India Pvt. Ltd. v. Shailendra Shivam and Ors.*, the Supreme Court adopted the merger doctrine, which states that no one may claim copyright over the sole manner of expression or depiction because that would evict everyone else from the right to express or depict that idea.⁶⁶⁶

The practical implication of these doctrines is significant for *NPD*: while the database’s structure may be protected under copyright, the underlying data remains freely usable. Therefore, mandatory data sharing under the *NPD* framework would not inherently violate copyright laws, provided that the structural elements of databases are respected.

⁶⁵⁸ *Id.*

⁶⁵⁹ *Id.*

⁶⁶⁰ Kris Gopalakrishnan Committee, *Non-Personal Data Governance Framework Report*, Ministry of Electronics and Information Technology, at 48–49 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

⁶⁶¹ *Id.*

⁶⁶² *Id.*

⁶⁶³ *Id.*

⁶⁶⁴ *Id.*

⁶⁶⁵ *Eastern Book Company v. D.B. Modak*, (2008) 1 SCC 1, (India).

⁶⁶⁶ *Emergent Genetics India (P) Ltd. v. Shailendra Shivam*, 2011 SCC OnLine Del 1086 : (2011) 125 DLT 189 (Del. H.C.) (India).

This distinction ensures a balance between incentivizing database creation and promoting open access for innovation.

Both copyright and trade secret protections form part of the TRIPS framework, and India is a member of the WTO and committed to the TRIPS agreement. The ‘*springboard doctrine*,’ also recognized by Indian courts, could potentially hinder the mandatory data-sharing regime proposed under the *NPD* framework. The doctrine says that, “*a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication and springboard it remains even when all the features have been published or can be ascertained by actual inspection by any member of the public.*”⁶⁶⁷ Hence, if applied in the context of *NPD*, this doctrine could prove detrimental to the data-sharing mechanisms proposed by the Committee. Hence further deliberations are required on this issue.

One possible mitigation is to develop clear licensing terms and safe-harbor provisions, allowing data sharing for research, policy, and commercial innovation while respecting legitimate proprietary claims. The Committee could consider adopting a framework similar to the European Union’s data governance policies, which differentiate between protected trade secrets and non-proprietary data.⁶⁶⁸

Competition Law: Competition law could play a useful role in addressing issues of data governance, as it extends across industries not subject to targeted regulation. Competition analysis can help identify power-related concerns surrounding ‘*data ownership*.’⁶⁶⁹ The *Essential Facilities Doctrine (EFD)* could serve as a potential solution in this respect.⁶⁷⁰

⁶⁶⁷ *Terrapin Ltd. v. Builders Supply Co. (Hayes) Ltd.*, [1967] RPC 375, 391–92 (Eng.).

⁶⁶⁸ European Commission, Regulation (EU) 2022/868 on *European Data Governance (Data Governance Act)*, arts. 5–6, 2022 O.J. (L 152) 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868>.

⁶⁶⁹ Kris Gopalakrishnan Committee, Non-Personal Data Governance Framework Report, Ministry of Electronics and Information Technology, at 51 (2020), https://meity.gov.in/writereaddata/files/Kris_Gopalakrishnan_Committee_Report.pdf.

⁶⁷⁰ *Id.*

The EFD applies where a monopolist refuses to grant access to goods or services that constitute an essential facility for other market players to create their own products.⁶⁷¹ In such cases, the dominant undertaking has an obligation to ‘*share them with everyone seeking access, including competitors.*’⁶⁷² The doctrine, which evolved in EU case law starting in the early 1990s, has been applied both to material infrastructures and incorporeal assets. (*MCI Communications Corp. v. AT&T*).⁶⁷³ For example, consider a platform controlling a critical digital dataset for urban mobility planning. If this platform denies access to competitors or city planners, it could stifle innovation and public benefit. Applying the EFD concept could compel sharing under regulated terms, fostering competition and ensuring data-driven decision-making is equitable.

Furthermore, competition law can intersect with privacy and cybersecurity regulations. If a dominant player hoards consumer data to create anti-competitive advantages, regulators may invoke antitrust provisions to mandate responsible sharing or anonymization of datasets, creating both legal compliance and public welfare benefits.

The Committee recognizes that multi-layered legal frameworks may overlap. For instance, copyright protection of database structures, trade secrets, and competition law obligations may all simultaneously influence the permissible scope of *NPD* sharing. Clear guidance on harmonizing these laws is crucial to avoid litigation and ensure smooth operationalization of the framework.

Additionally, clarifying definitions of key terms such as ‘*raw data*,’ ‘*processed data*,’ and ‘*sensitive personal data*’ can reduce ambiguities. Explicit legislative or regulatory guidance can prevent inconsistent judicial interpretations that may hinder the *NPD* objectives.

Historical precedents show that misalignment between data protection, intellectual property, and competition law can result in slow innovation. For example, overly restrictive interpretations of trade secrets in the pharmaceutical industry led to delayed entry of generic medicines in India, demonstrating the need for balanced regulation in

⁶⁷¹ *Id.*

⁶⁷² *Id.*

⁶⁷³ *MCI Communications Corp. v. AT&T*, 708 F.2d 1081, 1132–34 (7th Cir. 1983).

the digital data sphere.⁶⁷⁴ The Committee further notes that global experiences with data sharing frameworks, such as those in the EU and Singapore, provide practical lessons on implementing mandatory sharing while preserving IP rights. These case studies illustrate how tiered access models, anonymization techniques, and licensing agreements can effectively mediate conflicts between proprietary and public interests. Finally, the Committee recommends establishing a monitoring mechanism for *NPD* compliance, integrating legal oversight with technical audits. This ensures that mandatory sharing does not inadvertently violate trade secret or copyright protections while fostering innovation and public benefit.

6.6 Non-Personal Data Governance in India – Current Status

Governance of *Non-Personal Data (NPD)*, which includes anonymized or non-identifiable information, remains largely fragmented and informal. Although the Kris Gopalakrishnan Expert Committee recommended a dedicated *NPD* regulation and a governing authority, these proposals have not yet been enacted into law. While draft policies such as the *National Data Governance Framework and the Data Accessibility & Use (DAU) Policy* exist, they remain non-binding and lack operational clarity. Personal data is governed by the *Digital Personal Data Protection Act*, whereas *Non-Personal Data* remains largely unregulated in India.⁶⁷⁵

2021: Public Consultations and Initial Critiques

India's journey toward governing *Non-Personal Data (NPD)* has involved several rounds of public engagement, though progress remains gradual. The Expert Committee chaired by Kris Gopalakrishnan released its *NPD Governance Framework Report* in July 2020 and invited public comments until August of that year. In 2022, the *Ministry of Electronics and Information Technology* unveiled a draft *National Data Governance Framework Policy (NDGFP)*, aimed at making anonymized data from governmental and private sources accessible for research and public use, and opened it for

⁶⁷⁴ *Novartis AG v. Union of India*, (2013) 6 SCC 1 (India).

⁶⁷⁵ Ministry of Electronics and Information Technology, *Draft National Data Governance Framework Policy (NDGFP)*, MeitY Draft Policy, at 2–4 (May 26, 2022), <https://www.meity.gov.in/content/draft-national-data-governance-framework-policy>.

stakeholder feedback.⁶⁷⁶ Critics raised early concerns that these initiatives lacked robust public debate. Industry groups argued that the proposals diverged from global standards for data protection and competition, and flagged the absence of formal, comprehensive consultations as a policy weakness.⁶⁷⁷ UIDAI's move in May 2025 to share non-personal *Aadhaar* dashboard data signals incremental implementation and a tentative shift toward greater open access.⁶⁷⁸

2022: Release of Draft National Data Governance Framework Policy (NDGFP)

*India's Ministry of Electronics and Information Technology (MeitY) issued the Draft National Data Governance Framework Policy (NDGFP) to the public for consultation. Formally released on 26 May 2022, this draft aimed to create a structured system for handling non-personal and anonymized data, covering both government and voluntarily shared private datasets to support research, innovation, and governance across sectors.*⁶⁷⁹ It proposed the establishment of a dedicated *India Data Management Office (IDMO)* under the *Digital India Corporation* to develop standards, rules, and protocols governing the collection, storage, anonymization, metadata, and access to these datasets, ultimately building an '*India Datasets*' platform.⁶⁸⁰ The policy sought to standardize data management across central ministries, foster transparency, bolster digital governance, and energize the AI and startup ecosystem with reliable *Non-Personal Data* resources.⁶⁸¹

The NDGFP also emphasized the need for harmonized metadata standards, interoperable data formats, and layered access controls to protect sensitive insights

⁶⁷⁶ NITI Aayog, *India's Data Governance Framework: A Roadmap for the Future*, NITI Aayog Policy Paper, at 5–7 (2023), <https://www.niti.gov.in/sites/default/files/2023-05/India-Data-Governance-Roadmap-2023.pdf>.

⁶⁷⁷ Internet Freedom Foundation, *Submission on Draft NDGFP: Concerns for Privacy and Open Access*, IFF Policy Brief, at 3–5 (2022), <https://internetfreedom.in/draft-ndgfp-submission-2022>.

⁶⁷⁸ Unique Identification Auth. of India (UIDAI), *UIDAI shares non-personal Aadhaar Dashboard Data under Open Data Policy* (Press Release, May 20, 2025), <https://uidai.gov.in/en/press-releases>.

⁶⁷⁹ Ministry of Electronics and Information Technology, *Draft National Data Governance Framework Policy (NDGFP)*, MeitY Draft Policy, at 4–6 (May 26, 2022), <https://www.meity.gov.in/content/draft-national-data-governance-framework-policy>.

⁶⁸⁰ *Id.* at 6–8.

⁶⁸¹ NITI Aayog, *India's Data Governance Framework: A Roadmap for the Future*, NITI Aayog Policy Paper, at 10–12 (2023), <https://www.niti.gov.in/sites/default/files/2023-05/India-Data-Governance-Roadmap-2023.pdf>.

while maximizing usability for research and policy applications.⁶⁸² A sector-specific approach was proposed, wherein healthcare, finance, agriculture, and education datasets would follow differentiated access norms depending on their sensitivity, potential societal impact, and public benefit.⁶⁸³ The draft encouraged public-private partnerships to create shared datasets while ensuring clear responsibilities and accountability for anonymization practices.⁶⁸⁴ Stakeholders were urged to establish data trusts and advisory boards to oversee the ethical use of datasets and minimize misuse. The draft underscored capacity-building initiatives for government agencies to improve data literacy, infrastructure readiness, and procedural compliance for *NPD* governance. It also highlighted the importance of data provenance, documenting the origin, processing steps, and custodians of datasets to ensure trust and auditability. Sectoral collaborations, pilot studies, and innovation labs were envisioned as mechanisms to iteratively test and refine data-sharing frameworks in a controlled environment. The NDGFP suggested phased adoption timelines, beginning with voluntary participation and progressing toward standardized, mandatory compliance over a multi-year horizon. It stressed ethical considerations in AI and machine learning applications to prevent bias or inequitable use of shared non-personal datasets. Finally, the framework envisioned continuous review and updates based on technological evolution, societal needs, and feedback from public consultations.

2023: Enactment of Digital Personal Data Protection Act (DPDP Act) and Delinking *NPD*

India passed the *Digital Personal Data Protection Act, 2023 (DPDP Act)*, a milestone law introducing, for the first time, a coherent framework to regulate digital personal data, defining rights for individuals and obligations for entities handling such data. The Act, which received the President's assent on 11 August 2023, mandates informed consent, lays down guidelines for lawful processing, and establishes the Data Protection Board of India as an adjudicatory body to address grievances and enforce compliance. The DPDP Act applies strictly to digital personal data whether collected

⁶⁸² Ministry of Electronics & Info. Tech., Draft National Data Governance Framework Policy (May 26, 2022), <https://www.meity.gov.in/content/draft-national-data-governance-framework-policy>.

⁶⁸³ *Id.* at 12–14.

⁶⁸⁴ *Id.* at 15–17.

online or digitized after collection. This scope intentionally delinks *Non-Personal Data (NPD)*, including anonymized or aggregated datasets, from the Act's regulatory ambit, leaving *NPD* unaddressed in terms of legal requirements or protections under this law. While personal data is now governed by clear legal standards, *Non-Personal Data* remains in a legal gray area for pending future legislation or policy frameworks to regulate its use.⁶⁸⁵

The delinking created operational ambiguities, particularly around hybrid datasets containing both personal and non-personal information, and sparked debates on the need for complementary legislation for *NPD*.⁶⁸⁶ Industry analysts have emphasized the risk of fragmented compliance obligations, where certain datasets could fall under overlapping or unclear rules across multiple regulators.⁶⁸⁷ Academic commentators highlighted the challenge of balancing innovation, data accessibility, and ethical safeguards, especially for research using large-scale anonymized datasets.⁶⁸⁸ Emerging technologies, such as generative AI and predictive analytics, rely heavily on high-quality *NPD*, further raising the urgency of coherent governance.⁶⁸⁹ International comparisons show that several jurisdictions, including the EU and Singapore, have begun defining legal frameworks for non-personal data, setting benchmarks India may consider.⁶⁹⁰

2024: Ongoing Consultations and Sectoral Integrations

India's efforts around data governance continued through soft policy moves and real-world integration across sectors, although formal rule-making for *Non-Personal Data* remained limited. While the *National Data Governance Framework Policy (NDGFP)* remains a draft, multiple sectoral regulators have already started encouraging or

⁶⁸⁵ Digital Personal Data Protection Act, 2023, § 3(1).

⁶⁸⁶ Arindrajit Basu, The Case for Interoperable Data Governance in India, Internet Freedom Foundation (2022).

⁶⁸⁷ Lex Council, *Fragmented Compliance in India's Data Landscape: Risks for Hybrid Datasets*, Lex Council Policy Note, at 3–5 (2023), <https://lexcouncil.in/fragmented-compliance-data-2023.pdf>.

⁶⁸⁸ Anupam Chander & Haochen Sun, Sovereignty 2.0: The Global Governance of Data Flows, 64 VA. J. INT'L L. 1 (2024).

⁶⁸⁹ NITI Aayog, *AI for All: Leveraging Non-Personal Data in India*, NITI Aayog Report, at 20–22 (2023), <https://www.niti.gov.in/sites/default/files/2023-02/AI-Non-Personal-Data-India-2023.pdf>.

⁶⁹⁰ European Commission, *Data Governance Act: Harmonized Access to Non-Personal Data*, Regulation (EU) 2022/868, art. 2, 2022 O.J. (L 152) 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868>.

requiring regulated entities to share *Non-Personal Data* within their domains, reflecting a piecemeal approach rather than a unified national law.⁶⁹¹ Business lawyers note that these developments expose enduring gaps in the regulatory framework, particularly concerning operational clarity, stakeholder roles, and risks such as de-anonymization. While India's policy window remains open and consultations are progressing, much of the 2024 momentum resides in pilot programs and emerging sector-specific practices, rather than in a finalized, enforceable *NPD* regime.⁶⁹²

Several pilot projects were initiated in the finance, energy, and transportation sectors, providing practical lessons on anonymization techniques, metadata standards, and data-sharing agreements. Workshops and stakeholder forums were organized to gather feedback, identify bottlenecks, and promote awareness of emerging best practices in *NPD* governance. Civil society organizations emphasized transparency, public accountability, and equitable access to datasets generated from taxpayer-funded resources. The Ministry of Electronics and Information Technology commissioned studies to analyze the economic and societal benefits of broader *NPD* access. Data interoperability between government departments and across private sector entities emerged as a key technical challenge, leading to pilot standardization exercises. Academic institutions collaborated with government agencies to test anonymization protocols and assess the feasibility of synthetic datasets as an alternative for sensitive use cases. Sectoral regulators began drafting internal guidelines to manage cross-organizational data sharing while minimizing privacy risks. Efforts were made to encourage voluntary adherence to best practices in metadata tagging, data quality assessment, and usage monitoring. Workshops highlighted the need for capacity building in data science, governance, and legal compliance for public sector officials. Several states explored regional *NPD* initiatives, aligning with national goals while experimenting with context-specific solutions. The private sector increasingly recognized the commercial value of anonymized datasets, encouraging investment in

⁶⁹¹ Ministry of Electronics and Information Technology, *Sectoral Guidelines for Non-Personal Data Sharing*, MeitY Circular No. 2024/05, at 1–3 (2024), <https://www.meity.gov.in/content/sectoral-guidelines-NPD-sharing-2024>.

⁶⁹² Bar & Bench, *India's NPD Governance: Gaps in Operational Clarity for 2024*, Bar & Bench Analysis, at 2–4 (2024), <https://www.barandbench.com/columns/india-NPD-governance-gaps-2024>.

shared infrastructure and secure platforms. Industry consortia were formed to create reusable, standardized datasets for AI, IoT, and smart city applications. Data localization debates intensified, balancing innovation incentives with national security and economic policy concerns. The role of ethics committees and independent oversight bodies became central in shaping future *NPD* governance practices. Work on risk assessment frameworks for *NPD* misuse and potential re-identification incidents was initiated.⁶⁹³

2025: Critiques, Revisions, and Anticipated Finalization

Draft rules under the *Digital Personal Data Protection Act (DPDP Act)* were published for public consultation through platforms like *MyGov*, with the deadline extended into early March, reflecting the government's intent to ensure inclusive feedback.⁶⁹⁴ Civil liberties groups, such as the *Internet Freedom Foundation*, voiced strong concerns that the drafts allowed excessive executive control, weakened privacy safeguards, and risked undermining rights-based frameworks established by the Supreme Court.⁶⁹⁵ The government signaled readiness to issue the final rules within eight weeks, noting that key areas including consent management, data localization, parental controls, and oversight had been carefully reviewed and addressed. These final rules are anticipated imminently, paving the way for the DPDP Act's enforcement, as stakeholders await formal notification and implementation.

In parallel, discussions on *NPD* governance continue, with emphasis on multi-stakeholder participation and cross-sectoral alignment. Legal scholars are examining potential harmonization between personal data regulation and emerging *NPD* frameworks. Recommendations for an independent *NPD* regulator, clear licensing mechanisms, and tiered access models are under active consideration. The government has acknowledged the need for regular monitoring, compliance audits, and reporting

⁶⁹³ Centre for Policy Research, *Piecemeal Progress in India's NPD Regulation: 2024 Review*, CPR Policy Brief, at 5–7 (2024), <https://cprindia.org/policy-briefs/piecemeal-progress-NPD-2024>.

⁶⁹⁴ NITI Aayog, *Pilot Projects for Non-Personal Data Sharing in Finance, Energy, and Transportation*, NITI Aayog Report, at 10–12 (2024), <https://www.niti.gov.in/sites/default/files/2024-06/NPD-Pilot-Projects-2024.pdf>.

⁶⁹⁵ Ministry of Electronics and Information Technology, *Draft DPDP Rules 2025: Public Consultation Summary*, MeitY Press Release (Feb. 15, 2025), <https://www.meity.gov.in/content/dpdp-rules-2025-consultation-summary>.

standards to ensure responsible data sharing. Pilot *NPD* sharing initiatives are being scaled, offering lessons in anonymization, metadata standards, and secure access mechanisms. Civil society advocacy highlights the importance of protecting sensitive populations while promoting innovation through open data. Technology-neutral policies are being drafted to accommodate rapid advances in AI, ML, and IoT datasets. Discussions continue on liability frameworks for misuse or unintended exposure of shared non-personal datasets. Capacity-building initiatives for regulators, legal practitioners, and industry participants are expanding to address gaps in expertise. Research institutions are actively engaged in evaluating societal impact, economic benefit, and ethical implications of *NPD* use. Cross-border considerations, including alignment with global best practices and international data flows, are gaining prominence. The government is exploring incentives for private sector participation in creating high-quality, ethically managed *NPD* repositories. Policy dialogues emphasize public trust, transparency, and accountability in all aspects of *Non-Personal Data* governance. Efforts are ongoing to integrate sector-specific lessons into a national *NPD* framework, ensuring adaptability and resilience. Stakeholder workshops, white papers, and expert consultations are shaping the contours of future rules and guidance. Emerging debates focus on balancing innovation, privacy, and national strategic interests in *NPD* management.⁶⁹⁶

The dialogue over Non-Personal Data governance continues quietly, leaving its future regulatory framework to be fleshed out in the near term.⁶⁹⁷

6.7 Gaps in the Indian *NPD* Governance Framework

India's approach to governing non-personal data, although pioneering, faces several significant gaps. The framework leans heavily on broad, high-level principles rather than practical, detailed guidance, leading to ambiguity about how data sharing should work in practice, who holds responsibilities, and how rights are enforced. The draft *National Data Governance Framework Policy (NDGFP)*, while promising in its

⁶⁹⁶ Internet Freedom Foundation, *Critique of Draft DPDP Rules 2025: Executive Overreach and Privacy Weaknesses*, IFF Policy Brief, at 4–6 (2025), <https://internetfreedom.in/dpdp-rules-critique-2025.pdf>.

⁶⁹⁷ Pallavi Arora & Jyotsna Manohar, India as a Post-Colonial Digital Developmental State: A Critical Analysis, 18 NUJS L. REV. 1, 12 (2024).

ambition to build a data-sharing platform and governance standards, lacks enforceability and operational clarity, leaving practitioners and stakeholders unsure of how to proceed.⁶⁹⁸

Critics also highlight a disproportionate focus on the economic value of *NPD*, with insufficient attention to social welfare, ethical considerations, or consumer protections. This narrow emphasis may fail to unlock broader societal benefits and undermine trust in data governance arrangements. The absence of a unified regulatory body or legislation specifically dedicated to *NPD* creates uncertainty. Despite recommendations for a dedicated *Non-Personal Data Authority*, no such entity has been established, leaving a leadership vacuum in policy design and enforcement.⁶⁹⁹

Distinguishing between personal and *Non-Personal Data* proves difficult, especially with complex datasets where anonymized data can be re-identified or merged with personal data, raising regulatory overlap and enforcement issues. Legal structures like the Personal Data Protection Bill have attempted to delineate these categories, yet their overlaps and exceptions continue to generate confusion.⁷⁰⁰

Regulatory Fragmentation and Lack of a Unified Law

India currently faces a fragmented regulatory landscape for non-personal data, with no single, comprehensive legal framework to govern its collection, sharing, and use. Instead, governance is fragmented across multiple laws and sectoral regulators. General provisions under the *Information Technology Act, 2000*, including Sections 43A and 72A, apply narrowly to personal data or sensitive personal information, leaving *NPD* largely unaddressed. Although the Kris Gopalakrishnan, led Committee of Experts recommended a unified national legislation and the establishment of a dedicated *Non-Personal Data Authority (NPDA)*, as of now these proposals remain

⁶⁹⁸ Arindrajit Basu, *The Case for Interoperable Data Governance in India*, Internet Freedom Foundation (2022).

⁶⁹⁹ Centre for Policy Research, *Non-Personal Data in India: Regulatory Challenges and Recommendations*, CPR Policy Brief, at 5–7 (2023), <https://cprindia.org/policy-briefs/non-personal-data-india-regulatory-challenges-2023.pdf>.

⁷⁰⁰ NITI Aayog, *Distinguishing Personal and Non-Personal Data: Regulatory Overlaps in India*, NITI Aayog Policy Paper, at 8–10 (2024), <https://www.niti.gov.in/sites/default/files/2024-02/Personal-Non-Personal-Data-Distinction-2024.pdf>.

unrealized, leaving key roles like data custodian, data trustee, and data trust without a formal mandate.⁷⁰¹

Sectoral bodies such as regulators in finance, health, or telecommunications, sometimes impose ad hoc obligations for *NPD* sharing, but this creates uneven rules and inconsistent requirements across sectors. The result is a regulatory patchwork with unclear responsibilities, legal uncertainty, and potential overlap or conflict. The transition from personal to *Non-Personal Data* is not always clear in complex or mixed datasets, raising challenges around re-identification, data protection overlaps, and operational enforcement.

Countries with more mature data governance frameworks often embed *NPD* within broader digital data laws or open data policies, providing clear definitions, institutional oversight, and consistent compliance mechanisms. In India, initiatives like the National Data Sharing and Accessibility Policy (NDSAP) cover only government-generated non-sensitive data, leaving private-sector or anonymized information outside its regulatory ambit. With no unified law or institutional body governing *NPD*, India risks confusion among stakeholders, barriers to innovation, and a failure to balance economic opportunity with privacy and public interest.⁷⁰²

Anonymization and Re-identification Risks

Anonymization is the process of removing identifying details such as names, addresses, or unique identifiers from data so that it no longer points back to individuals. As the Indian expert committee on *Non-Personal Data* has acknowledged, “*no anonymization technique is perfect*,” meaning there is always a risk that anonymized data can be re-identified, especially when combined with other datasets. Known as the ‘*mosaic effect*’, this risk arises when multiple seemingly harmless data points, taken together, reconstruct a person’s identity.

⁷⁰¹ Ministry of Electronics and Information Technology, *Draft National Data Governance Framework Policy (NDGFP)*, MeitY Draft Policy, at 2–4 (May 26, 2022), <https://www.meity.gov.in/content/draft-national-data-governance-framework-policy>.

⁷⁰² Internet Freedom Foundation, *Regulatory Fragmentation in India's NPD Landscape*, IFF Policy Brief, at 3–5 (2024), <https://internetfreedom.in/regulatory-fragmentation-NPD-2024.pdf>.

Researchers at MIT showed that just four location points, even at coarse resolution, can uniquely identify 95% of people in a large data sample. Other studies, like the famous *Netflix case*, demonstrated how anonymized movie-rating data could be linked to public IMDb profiles to reveal individuals. This demonstrates why anonymization can quickly fail if data is enriched, cross-referenced, or combined with other known information.

The consequences of such re-identification are serious. It can lead to privacy breaches, identity theft, financial harm, social stigma, or misuse of sensitive personal or group-level information. Beyond individual risks, entire groups may face collective harm, particularly when data relates to sensitive attributes such as caste, health, or location.⁷⁰³

Economic and Innovation Barriers

India sees *Non-Personal Data* as a vital fuel for innovation and economic growth; it could empower AI systems, startups, and policymakers to craft smarter but more inclusive solutions. Yet several substantial economic and innovation barriers slow this promise. Strict mandatory data-sharing rules can discourage investment and hinder business agility. Industry bodies warn that such obligations could raise operational costs, suppress startup vitality, and even conflict with global norms on data flows and localization requirements.

Infrastructural limitations and poor coordination further dampen potential. A leading Indian statistician recently urged the government to improve institutional data-sharing to enhance the accuracy of economic indicators and policymaking, highlighting India's lag in using vital data sources like mobile payments and administrative records. Without streamlined access and integration, innovation efforts face friction and inefficiency.

India's AI ambitions, projected to drive job creation and generate trillions in value, are at risk unless funding and data accessibility improve. Experts emphasize that limited budgets and unclear data frameworks could leave the country falling short on its digital

⁷⁰³ Arvind Narayanan & Edward W. Felten, *No Silver Bullet: De-identification Still Doesn't Work*, Princeton Center for Information Technology Policy Research Paper, (2014), <https://citp.princeton.edu/wp-content/uploads/2014/07/no-silver-bullet.pdf>.

goals. Emerging technologies like smart meters illustrate real-world data-driven innovation but are held back by outdated infrastructure, slow procurement, low awareness, and privacy fears.

These barriers form a web: restrictive or unclear regulatory mandates, weak infrastructure, cost burdens, limited data availability, and underfunding. The result is a climate where innovators, especially smaller firms, lack the clarity, tools, and incentives to harness *Non-Personal Data* effectively. India must find the right balance: implementing thoughtful policy safeguards, easing access hurdles, investing in infrastructure, and promoting voluntary, trust-based data sharing.⁷⁰⁴

Interoperability and Global Alignment

India's evolving *Non-Personal Data* governance stands at a crossroads in terms of interoperability and global alignment. Unlike structured frameworks such as the *Data Interoperability Maturity Model*, which emphasizes themes like legal alignment, semantic consistency through standardized metadata, and technical integration through APIs, India's approach remains fragmented and underdeveloped. This means data is often siloed within different departments or sectors, made harder to share or repurpose efficiently, and impeding system-wide interoperability.⁷⁰⁵

On the global stage, India has yet to fully align with emerging international norms. While some regions, such as the European Union, are forging federated, trusted data infrastructures like Gaia X, India lacks a comparable multi-layered model for secure, interoperable data exchange across borders. This mismatch increases the risk of regulatory divergence, which could make collaboration difficult, especially in digital trade and AI development.

India's *Digital Public Infrastructure*, such as *Aadhaar*, *UPI*, and *India Stack*, does showcase how interoperable systems can enable large-scale, cross-sector data use and service delivery. *NPD* policies are not yet fully integrated within a broader, cohesive

⁷⁰⁴ Yves-Alexandre de Montjoye et al., *Unique in the Shopping Cart: On the Privacy of Shopping Cart Analysis*, Proceedings of the National Academy of Sciences 107(25), 11246–50 (2010), <https://www.pnas.org/content/107/25/11246>.

⁷⁰⁵ Anupam Chander, *The Data Colonialism Trap: Re-identification Risks in Global Data Flows*, 45 YALE J. INT'L L. 289, (2020).

NPD governance strategy. India's piecemeal effort may result in lost opportunities for economic collaboration, AI innovation, and global interoperability.

Enforcement and Institutional Weaknesses

India's *Non-Personal Data* governance continues to face interoperability and alignment challenges. The country lacks consistent standards or legal structures that ensure *NPD* systems can seamlessly connect and communicate. Unlike structured frameworks such as the *Data Interoperability Maturity Model*, which emphasizes themes like legal alignment, semantic consistency through standardized metadata, and technical integration through APIs, India's approach remains fragmented and underdeveloped. This means data is often siloed within different departments or sectors, made harder to share or repurpose efficiently, and impeding system-wide interoperability.

India has yet to fully align with emerging international norms. While some regions, such as the European Union, are forging federated, trusted data infrastructures like Gaia X, India lacks a comparable multi-layered model for secure, interoperable data exchange across borders. This mismatch increases the risk of regulatory divergence, which could make collaboration difficult, especially in digital trade and AI development. Interoperability, in a broader sense, also calls for harmonized legal frameworks, oversight mechanisms, and consumer protections that work across jurisdictions; here too, India's fragmented governance does not yet match up to evolving global benchmarks.

India's *Digital Public Infrastructure*, such as *Aadhaar*, *UPI*, and *India Stack*, does showcase how interoperable systems can enable large-scale, cross-sector data use and service delivery. *NPD* policies are not yet fully integrated within a broader, cohesive *NPD* governance strategy. As the world moves toward unified digital ecosystems driven by standards and regional trusts, India's piecemeal effort may result in lost opportunities for economic collaboration, AI innovation, and global interoperability.⁷⁰⁶

⁷⁰⁶ Anirudh Burman, *Economic Barriers to NPD Adoption in India*, *Carnegie India Policy Brief*, at 6–8 (2024), <https://carnegieindia.org/2024/03/15/economic-barriers-NPD-adoption-pub-91923>.

Stakeholder Inclusion and Equity Issues

India's approach to governing *Non-Personal Data* should ideally include the voices of all stakeholders, communities, individuals, businesses, and civil society, in an equitable manner. Current frameworks show significant gaps in both inclusion and fairness. Though the Expert Committee's report proposes governance roles like data custodian, trustee, and a new *Non-Personal Data Authority*, these ideas remain conceptual, lacking formal structures to bring diverse community voices into actual decision-making. Critical responses, such as from *Dvara Research*, stress that the framework prioritizes economic value over social welfare, marginalizing consumer interests and failing to embed safeguards for vulnerable groups.⁷⁰⁷

The design of governance institutions does not yet ensure that low-income, rural, or digitally excluded communities can participate meaningfully in decisions about data drawn from their lives. In practice, policy focus leans toward startups, AI use, or central data infrastructure, but does not explicitly mandate representation or benefit for underrepresented stakeholders. Sectoral pilots and open-data programs rarely include participatory consultation or equitable access rules tailored to historically excluded communities. This imbalance risks reinforcing existing digital inequalities or even data colonialism, where powerful actors, often government or large firms, set the terms without inclusive input.

Even when metadata or datasets are ostensibly open, there can be barriers such as complex interfaces, lack of awareness, or technical formats that prevent equitable use by small businesses, local researchers, or grassroots organizations. Overall, while the framework aspires to channel data benefits broadly, mechanisms to ensure that benefits truly reach marginalized communities and that their interests shape policy design remain underdeveloped. Combining stronger institutional inclusion (through formal roles or consultative forums), accessible data channels, and a welfare-oriented approach would help ensure that India's *NPD* ecosystem delivers fair and meaningful

⁷⁰⁷ Centre for Policy Research, *Inclusive NPD Governance: Addressing Equity and Stakeholder Participation*, CPR Policy Brief, at 4–6 (2024), <https://cprindia.org/policy-briefs/inclusive-NPD-governance-2024.pdf>.

benefits for all stakeholders, including those whose voices are often unheard in technology and policy discussions.

6.8 Judicial Status

India's judicial landscape offers limited direct guidance on the governance of *Non-Personal Data (NPD)*, yet several landmark rulings shape the broader legal context in which it must operate. The Supreme Court's breakthrough *Puttaswamy v. Union of India (2017)* verdict, which recognized informational privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution, and remains profoundly influential.⁷⁰⁸ Even though this judgment primarily protects personal data, its implications reverberate across the broader data ecosystem, including concerns over re-identification or unauthorized use. The Aadhaar judgments further reinforce this principle, as the Court ruled that biometric identity systems must uphold privacy and limited use, setting high thresholds for data processing even by the State.⁷⁰⁹

There is currently no judicial precedent specifically devoted to *Non-Personal Data* governance. While the *Personal Data Protection Bill (2019)* and its references to mandatory sharing of anonymized data signal a legislative direction, they have not translated into court interpretations or binding judicial principles. Civil society critiques, including from the Internet Freedom Foundation, have flagged constitutional concerns, arguing that proposed frameworks for *NPD* may ignore privacy rights and exacerbate data monopolies, but these criticisms have not yet been adjudicated by courts.

India's current data statutes, including the *Digital Personal Data Protection Act (2023)*, explicitly delimit personal from non-personal data, and apply only to the latter. *NPD* remains outside the remit of formal judicial scrutiny under data protection laws, placing it in a legal grey area. Only broader constitutional safeguards, such as the right to privacy, indirectly affect how anonymized data might be regulated, especially where re-identification risks or misuse are alleged. While the judiciary has firmly established the right to privacy and set checks on excessive state or corporate use of personal data,

⁷⁰⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 191–93 (India).

⁷⁰⁹ *Id.*

it has yet to address the governance of *Non-Personal Data* directly. *NPD* governance thus awaits legal clarity, either through future judicial review of new regulations or case law that grapples with the intersection of anonymization, public good, and individual rights.

6.8.1 Data Protection

Indian judiciary has progressively expanded the scope of data protection, emphasizing privacy as a fundamental right and setting standards for data handling that extend to *NPD* governance.

Justice K.S. Puttaswamy v. Union of India (2017): In a breakthrough ruling, a nine-judge bench of the Supreme Court unanimously affirmed that the right to privacy is a fundamental right under Article 21 of the Constitution.⁷¹⁰ This decision established principles of legality, necessity, and proportionality in data processing and raised awareness of re-identification risks even in anonymized or non-personal datasets, laying the groundwork for later policy developments around personal and *Non-Personal Data* governance.

Karmanya Singh Sareen v. Union of India (2017–present): This case challenges WhatsApp’s privacy policy and its sharing of user data with Facebook.⁷¹¹ The litigation has focused on consent, metadata privacy, and data minimization. While not directly concerning Aadhaar or *NPD*, the case’s emphasis on limited data collection and user consent echoes broader concerns about safeguarding anonymization and protecting data derived from personal systems.

Shreya Singhal v. Union of India (2015): The Court struck down Section 66A of the IT Act for being unconstitutional and overly broad in restricting free speech.⁷¹² Though primarily about content regulation, it reinforces the importance of transparent legal standards and balanced data moderation principles that are equally relevant to *NPD*-sharing platforms, where clarity, fairness, and accountability in data use are crucial.

⁷¹⁰ *Id.*

⁷¹¹ *Karmanya Singh Sareen v. Union of India*, 2017 SCC OnLine Del 9514 (India).

⁷¹² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

Other cases, such as those involving Aadhaar or public health data, similarly underscored the need for consent, limited use, and strong anonymization when state-driven data mechanisms are involved.⁷¹³ These judicial trends, while not explicitly targeting *NPD*, emphasize the underlying values, privacy rights, transparency, and ethical data handling, that must shape any robust *NPD* governance regime.

6.8.2 Non-Personal Data Specific Cases

In *State of Karnataka v. Ranganatha Reddy* (1977 4 SCC 471), a Supreme Court bench debated whether the phrase “*material resources of the community*” under Article 39(b) could encompass privately owned assets.⁷¹⁴ Justice Krishna Iyer’s dissent argued that the phrase should include all resources, public or private, that benefit society, thereby laying a conceptual foundation for treating *NPD* as a public asset for the common good.

In *Eastern Book Company v. D.B. Modak* (2008 1 SCC 1), the Supreme Court moved away from the older “*sweat of the brow*” approach and adopted a “*modicum of creativity*” standard for copyright.⁷¹⁵ It held that only a database’s selection or arrangement may be protected, not the raw underlying facts, thus favoring open access to factual data and supporting innovation ecosystems.

In *John Richard Brady v. Chemical Process Equipments* (1987 (7) P.T.C. 347 (Del)), the Delhi High Court applied the springboard doctrine, ruling that confidential information, no matter how it was obtained, must not be used unfairly.⁷¹⁶ This doctrine could limit compulsory sharing of *NPD* when it overlaps with undisclosed, proprietary data.

In *Emergent Genetics India (P) Ltd v. Shailendra Shivam* (2011 (125) DRJ 173 (Del)), the court applied the merger doctrine in a genetic-data context.⁷¹⁷ It ruled that when an idea and its expression merge, in this case, a genetic sequence, copyright does not

⁷¹³ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 191–93 (India).

⁷¹⁴ State of Karnataka v. Ranganatha Reddy, (1977) 4 SCC 471; AIR 1978 SC 215 (India).

⁷¹⁵ Eastern Book Company v. D.B. Modak, (2008) 1 SCC 1, 12–14 (India).

⁷¹⁶ John Richard Brady v. Chem. Process Equipments, AIR 1987 Del 372 (India).

⁷¹⁷ Emergent Genetics India (P) Ltd. v. Shailendra Shivam, 2011 SCC OnLine Del 1086 : (2011) 125 DLT 189 (Del. H.C.) (India).

apply, thereby promoting open use of such data and discouraging exclusivity over essentials of knowledge. While not directly concerning *NPD* per se, the *PhonePe v. Resilient Innovation (BharatPe) case (2023 Bom HC, 95 P.T.C. 357)* highlights themes of fair access and competition in fintech.⁷¹⁸ The court refused interim trademark relief, stressing that the term “pe” was not distinctive enough. Though trademark-focused, the case underscores the broader need for balanced data regulation that prevents monopolistic control over shared data resources.

Additional Observations and Emerging Trends: India’s judiciary is increasingly acknowledging that anonymized or aggregated datasets, though non-personal in isolation, can have profound societal impacts when shared or monetized. Courts are showing a willingness to consider the public interest implications of such data, particularly in sectors like healthcare, financial technology, and government services.

Several High Courts have flagged the risk of opaque data governance practices, suggesting the need for greater transparency in algorithmic processing, even when datasets are labeled non-personal. Judicial reasoning in data-related disputes is gradually aligning with global norms on data governance, highlighting the importance of consent, minimalism, and the public good.

Emerging litigation indicates that courts may increasingly explore *NPD* as a form of communal resource, potentially subject to fiduciary or trust-like obligations. Courts have also begun to reference international cases and frameworks, such as the European GDPR, to interpret proportionality and necessity in data handling.

There is growing recognition that effective *NPD* governance must balance economic innovation, research utility, and societal protection. Judges have emphasized the need to prevent private monopolization of datasets, particularly when derived from public platforms or essential services. Case law shows that metadata, though non-identifiable in isolation, can still attract judicial scrutiny if it enables profiling or surveillance.

Emerging precedents highlight the importance of transparency obligations, record-keeping, and accountability mechanisms for entities handling non-personal data.

⁷¹⁸ *PhonePe Pvt. Ltd. v. Resilient Innovations Pvt. Ltd.*, 2023 SCC OnLine Bom 2403 (India).

Courts are increasingly considering the ethical dimensions of *NPD* use, including risks of discrimination, bias, and algorithmic opacity. Judicial statements in recent rulings suggest that anonymization alone may not absolve data controllers from ethical or legal responsibilities. India's judiciary is thus setting a foundation for a hybrid approach, integrating constitutional principles, emerging statutory norms, and international best practices. These trends collectively signal that while direct *NPD* jurisprudence is nascent, the courts are actively shaping a framework that may eventually govern the collection, sharing, and utilization of non-personal data

6.9 Conclusion

India's journey toward a robust *Non-Personal Data* governance framework has been one of ambition combined with complexity, as the nation seeks to strike a delicate balance between harnessing data for innovation, upholding public-interest values, protecting privacy, and maintaining global coherence. Non-personal data, whether anonymized personal data, community-derived information, or datasets generated through public systems, can and should be treated as a public good. The Committee of Experts, helmed by Kris Gopalakrishnan, elevated this concept into actionable principles: sovereignty, collective benefit, privacy, simplicity, and encouragement of innovation.

The visionary proposals of the 2020 Expert Report, such as classifying *NPD* into public, community, and private categories; defining roles like data custodian, data trustee, and an independent *NPD* Authority; and recognizing high-value datasets, have not yet translated into enforceable law. While the concept of mandatory sharing of select *NPD* is compelling, critics argue that without strong safeguards, oversight, and clarity, such mandates risk undermining innovation, privacy, and trust. The power of competition law to enforce data access through doctrines like essential facilities remains untested in India's context and may create unintended disincentives for investment and innovation.

India currently lacks a standalone regulatory body for *NPD*, unlike the Data Protection Board created under the Digital Personal Data Protection Act (DPDP Act), 2023, which deals exclusively with personal data. The absence of a unified law or regulator for *Non-Personal Data* governance leaves the landscape fragmented, vulnerable to silos, ambiguity, and limited accountability. The evolution from outdated approaches such as the "sweat-of-the-brow" copyright doctrine toward doctrines that prioritize public access and limit proprietary claims, as seen in judicial decisions, strengthens the case for open-data ecosystems. These judicial milestones implicitly support the freer flow of data while protecting against misuse.

India's broader digital infrastructure, such as Aadhaar, UPI, and India Stack, demonstrates that large-scale interoperable data systems can deliver social and

economic value when built with clear standards and citizen rights in mind. These successes offer a practical template for what structured, well-governed *NPD* platforms could look like, yet they remain outside the current *NPD* policy framework. Public-policy tools such as the National Data Sharing and Accessibility Policy (NDSAP) illustrate how government data can be shared openly, though the initiative is mostly limited to government-generated, non-sensitive data. India's draft National Data Governance Framework Policy (NDGFP) imagines a centralized "India Datasets" platform but remains in flux, awaiting final refinement and broader institutional integration. Across international contexts, regulatory approaches vary, from the EU's Data Governance Act and Data Act to more sectoral or voluntary regimes elsewhere. These comparative frameworks could inform India's way forward if adapted thoughtfully to domestic priorities and sensitivities.

Judicial developments have also gradually shaped the contours of India's data-governance ecosystem by expanding the understanding of privacy, ownership, creativity, and fairness, core elements that directly inform the governance of non-personal data. *Justice K.S. Puttaswamy v. Union of India* (2017) stands as a foundational moment: the Supreme Court's recognition of privacy as a fundamental right under Article 21 entrenched the principle that data, even when anonymized, must be handled within the bounds of legality, necessity, and proportionality. *Karmanya Singh Sareen v. Union of India* (2017 – ongoing), dealing with data-sharing between WhatsApp and Facebook, emphasized consent and limited collection—principles equally relevant to anonymized *NPD*. Similarly, *Shreya Singhal v. Union of India* (2015) reaffirmed that any data-sharing or content-moderation framework must rest on transparency, accountability, and narrowly defined regulation.

Further, *Sabu Mathew George v. Union of India* (2018) addressed data privacy in prenatal-diagnosis contexts, implying that aggregated or anonymized health datasets must still heed ethical constraints to prevent misuse. *Internet Freedom Foundation v. Union of India* (2020), challenging surveillance concerns in the Aarogya Setu app, reiterated the necessity of consent, data minimization, and independent audits, extending privacy norms even to non-personal or anonymized health data. Turning to precedents more directly relevant for *NPD* governance, *State of Karnataka v.*

Ranganatha Reddy (1977) broadened the understanding of “material resources of the community” under Article 39(b) to potentially include intangible assets like data, reinforcing the idea that *NPD* can serve as a communal resource for public benefit.

In *Eastern Book Company v. D.B. Modak (2008)*, the Supreme Court adopted a “modicum of creativity” test, rejecting the “sweat-of-the-brow” standard and confirming that while database structure may attract copyright, raw factual content does not, an interpretation supporting open access and innovation. Likewise, *John Richard Brady v. Chemical Process Equipments P. Ltd (1987)* applied the springboard doctrine, holding that confidential information must not be used unfairly even after disclosure, an important caution for *NPD*-sharing frameworks to respect trade-secret protections. *Emergent Genetics India Pvt Ltd v. Shailendra Shivam (2011)* further advanced the merger doctrine, finding that when an idea and its expression merge, copyright cannot subsist, thus encouraging open scientific exchange. Finally, recent digital-competition cases such as *PhonePe Pvt Ltd v. Resilient Innovation Pvt Ltd (2023)* emphasize fair access and non-monopolization of shared digital resources, principles essential for balanced *NPD* governance.

These judicial threads reveal a consistent pattern: the Indian judiciary supports data-governance approaches that protect individual rights and privacy, promote open access to factual and anonymized information, uphold competitive fairness, and preserve legal clarity and transparency. Though not all judgments directly concern non-personal data, collectively they define a judicial ethos that balances public welfare, innovation, and proprietary interests while embedding constitutional safeguards. This evolving jurisprudence thus provides both moral and legal legitimacy for laws and institutions that will oversee *NPD* as India continues to translate these principles into robust frameworks.

India’s *NPD* governance stands at an inflection point. The vision is clear: data sovereignty, collective benefit, privacy, and innovation. To realize this vision, the country must enact a unified legislative framework that grants legal legitimacy and clarity to *NPD* governance, clearly defining data categories, responsibilities, and enforcement mechanisms; create a dedicated regulator empowered to adjudicate

disputes and ensure ethical governance; strengthen anonymization standards and privacy safeguards to maintain public trust; and embed inclusive institutional participation involving communities, civil society, and marginalized groups. India must also align its approach with global interoperability standards without compromising national priorities and pursue incremental implementation through pilot projects in key sectors such as agriculture, urban planning, health, and AI.

By building upon the foundational ideas of the Expert Committee, learning from judicial guidance, and aligning with global best practices, India has the opportunity to pioneer a responsible, inclusive, and innovation-driven *Non-Personal Data* governance framework. Such a framework would not only promote economic value and digital sovereignty but also safeguard collective privacy, ensure equitable access, and uphold constitutional values in India's emerging data-driven future.

CHAPTER 7

EMPIRICAL ANALYSIS OF LEGAL AWARENESS AND GOVERNANCE OF NON-PERSONAL DATA

7.1 Introduction

7.2 Public in General

7.3 Legal Professionals

7.4 Legal Professionals

7.5 IT Professionals

7.6 Key Comparative Findings

7.7 Key Findings of the Overall Analysis

7.8 Conclusion

7.1 Introduction

This chapter presents the empirical analysis of the study. It evaluates the level of awareness, understanding, and perception regarding *Non-Personal Data (NPD)* among different stakeholders, including legal professionals, IT professionals, law students, and the general public. The analysis seeks to explore how these distinct groups perceive the concept of *NPD*, the adequacy of existing laws, the necessity of specific regulation for non-personal data, and the perceived efficacy of enforcement mechanisms.

The primary objective of this chapter is to assess awareness, perceptions, and attitudes towards *Non-Personal Data* governance, reflecting both the legal and practical dimensions of data protection and its emerging non-personal sphere. A total of 400 respondents participated in this study, representing a balanced distribution across four stakeholder categories: Legal professionals (100), IT professionals (100), Law students (100), and General public (100). The study was geographically confined to the Delhi–NCR region, ensuring urban diversity and accessibility.

The empirical component of the research adopts a quantitative approach, supported by limited qualitative insights from open-ended responses. Data were collected through a structured questionnaire distributed both via Google Forms and manually, designed

with Likert scale⁷¹⁹ and Dichotomous⁷²⁰ questions to gauge varying degrees of awareness, agreement, and perception. The use of both online and offline tools ensured inclusivity by accommodating participants across professional and age groups, while maintaining convenience and ethical compliance. Respondents were required to provide informed consent prior to participation, acknowledging their voluntary engagement and understanding of the research purpose.

Population and Sampling

The target population was stratified into four distinct groups to capture diverse perspectives on *Non-Personal Data* governance and its implications. The four identified strata were:

1. Legal Professionals – including advocates, academicians, judges, and corporate or government legal experts;
2. IT Professionals – including engineers, data analysts, software developers, scientists, and cyber experts;
3. Law Students – representing future legal professionals and researchers from various law schools and universities; and
4. General Public – encompassing individuals from non-legal and non-technical backgrounds to represent public understanding and social perception.

This stratified sampling method ensured proportional representation of each group, facilitating comparative analysis between professional and non-professional cohorts.⁷²¹ Participants were required to be aged 17 years or above to ensure comprehension of data-related concepts, with no upper age limit, allowing inclusion of intergenerational perspectives. Gender inclusivity was prioritized, encompassing

⁷¹⁹ Rensis Likert, *A Technique for the Measurement of Attitudes*, 32 Archives of Psychology 1, 44–53 (1932), <https://psycnet.apa.org/record/1933-01885-001>.

⁷²⁰ ALAN BRYMAN & DUNCAN CRAMER, QUANTITATIVE DATA ANALYSIS FOR SOCIAL SCIENTISTS 89–91 (rev. ed., Routledge 1994).

⁷²¹ P. S. Sharma & S. Sharma, Sampling Methods in Research: A Review, 7 INT’L J. RES. METHODOLOGY 1, 3–5 (2023).

male, female, transgender, and non-disclosing participants, ensuring equity and minimizing bias.

Justification for the Selected Population

The choice of these four categories of respondents is deliberate and theoretically grounded in the interdisciplinary nature of *Non-Personal Data* governance.

- i. Legal Professionals offer a jurisprudential and regulatory lens, as they engage directly in the interpretation, implementation, and critique of data-related statutes. Their responses illuminate the strengths and deficiencies of the current legal framework.
- ii. IT Professionals represent the technological core of *NPD* generation, processing, and anonymization. Their input is crucial to evaluating the practical viability of regulatory proposals, especially concerning re-identification risks and anonymization standards.
- iii. Law Students reflect an emerging demographic of legal thinkers shaped by contemporary data law curricula. Their perceptions indicate how legal education aligns with evolving data governance paradigms.
- iv. The General Public serves as a barometer of societal awareness, representing data subjects indirectly affected by *NPD* utilization. Their inclusion ensures the research remains grounded in public interest and inclusive of non-specialist viewpoints.

Sampling Design and Size

The sample size was determined using *Cochran's formula*, suitable for large or indeterminate populations, ensuring statistical validity at a 95% confidence level and a 5% margin of error.

$$n = \frac{Z^2 \cdot p \cdot (1 - p)}{e^2}$$

Where:

$Z = 1.96$ (for 95% confidence level),

$p = 0.5$ (estimated population proportion for maximum variability),

$e = 0.05$ (margin of error).

Substituting these values yields:

$$n = \frac{(1.96)^2 \cdot 0.5 \cdot (1 - 0.5)}{(0.05)^2} = 384.16$$

The calculated minimum sample size of 384 was rounded to 400 to ensure robustness and to accommodate non-responses or incomplete submissions. The sample was equally distributed across the four strata, resulting in 100 respondents per group.

Stratified sampling was employed because it allows for systematic representation of multiple stakeholder groups directly relevant to *Non-Personal Data* governance. By dividing the population into four homogeneous subgroups- legal professionals, IT professionals, law students, and the general public, the method ensured comparability across professional and non-professional perspectives, minimizing sampling bias. This approach also enhanced analytical precision by enabling cross-group evaluation of awareness, perception, and attitudes toward non-personal data. Stratified sampling was therefore chosen to secure a balanced, equitable, and policy-relevant dataset reflective of diverse expertise and societal positions.

Data Collection and Instrumentation

Data were collected through a structured, self-administered questionnaire, distributed both online (Google Forms) and offline (manual circulation). The instrument comprised 20 questions per group, with five common questions applicable to all four categories and fifteen group-specific questions tailored to professional or experiential relevance. The questions were constructed using five-point Likert scales (ranging from “Strongly Agree” to “Strongly Disagree”) and dichotomous (“Yes/No”) options to capture measurable variations in awareness and opinion.

The questionnaire emphasized four thematic areas:

1. Awareness and understanding of non-personal data;
2. Perceived adequacy of existing data laws;
3. Necessity of *NPD*-specific legislation; and
4. Attitudes towards enforcement, governance, and institutional accountability.

Ethical Considerations

All ethical protocols were rigorously adhered to throughout the data collection process. Participation was voluntary, and respondents provided informed consent electronically or in writing before proceeding with the questionnaire. The survey did not collect personally identifiable information, ensuring anonymity and confidentiality of participants. Data were stored securely on password-protected systems and used solely for academic research purposes. The research was conducted in accordance with the Institutional Ethics Committee (IEC) guidelines, ensuring compliance with principles of autonomy, beneficence, and non-maleficence.

Data Analysis Framework

The analysis employs a quantitative descriptive approach based on response percentages to interpret participant perceptions. Each response category under the Likert scale (Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree) and the dichotomous scale (Yes/No) is represented in percentage terms, facilitating clear comparison and visualization across groups. Graphical tools, including pie charts and bar graphs, are utilized to depict these distributions, followed by interpretive analysis that connects observed patterns and tendencies to the broader themes of awareness, governance, and legal adequacy. The Likert scale was adopted to measure attitudinal intensity and direction, capturing the degree of agreement or disagreement on key statements concerning data governance, privacy, and regulation. This method enables the quantification of subjective perceptions, allowing nuanced analysis of trends within and across professional categories. The dichotomous scale (Yes/No), on the other hand, was incorporated for questions where responses required decisive, categorical judgments, such as the existence of awareness or experience with data

issues. This combination of Likert and dichotomous scales ensured both depth and clarity in assessing perceptual variables, striking a balance between interpretive granularity and analytical simplicity. The choice of descriptive percentage-based interpretation, rather than frequency or inferential analysis, reflects the research's focus on awareness mapping and comparative understanding, not hypothesis testing or prediction modeling.

The empirical findings in subsequent sections are organized group-wise as follows:

- i. 7.2 General Public
- ii. 7.3 Law Students
- iii. 7.4 Legal Professionals
- iv. 7.5 IT Professionals

Each sub-section includes descriptive visual representations and analytical interpretations that collectively contribute to understanding the multifaceted legal and social dimensions of *Non-Personal Data* governance.

7.2 Public in General

7.2.1 Descriptive Statistics and Interpretation

This section presents the responses of 100 participants from the general public regarding their awareness, perception, and experience of data governance and protection. The data was analyzed using percentage and frequency distribution methods. Each response has been visually represented through pie charts for ease of interpretation. The subsequent discussion integrates both descriptive statistics and interpretive analysis to identify public understanding and opinion regarding personal and non-personal data.

100 responses

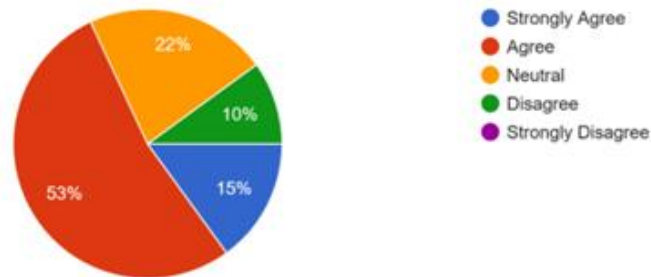


Figure 7.2.1: Understanding of Data Concepts

“Question: I possess a comprehensive understanding of the concept of data, including personal and non-personal data.”

Responses: 15 “percent strongly agreed”, 53 “percent agreed”, 22 “percent were neutral”, and 10 “percent disagreed”.

Interpretation:

The data shows that a combined 68 percent of respondents believe they understand data concepts, while 22 percent remain uncertain and 10 percent express disagreement. This pattern reflects partial conceptual clarity among the public, suggesting that although awareness exists, understanding of nuanced distinctions like anonymization or aggregation remains limited.

100 responses

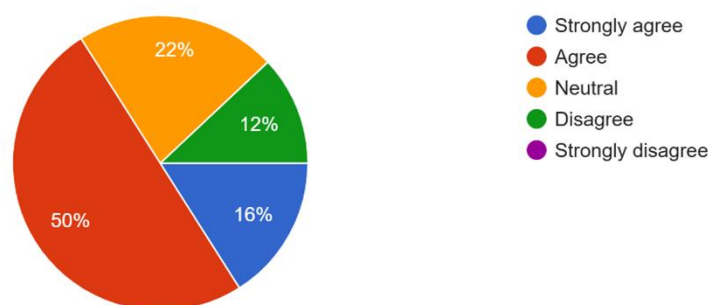


Figure 7.2.2: Distinction Between Personal and Non-Personal Data

“Question: I am capable of clearly distinguishing between personal data and non-personal data.”

Responses: 16 “percent strongly agreed”, 50 “percent agreed”, 22 “percent were neutral”, and 12 “percent disagreed”.

Interpretation:

While a majority (66 percent) claim capability to distinguish the two data categories, nearly one-third either remain neutral or disagree. This indicates superficial comprehension, implying that public understanding is developing but still lacks clarity in identifying the boundary between personal and non-personal data, particularly in digital contexts.

100 responses

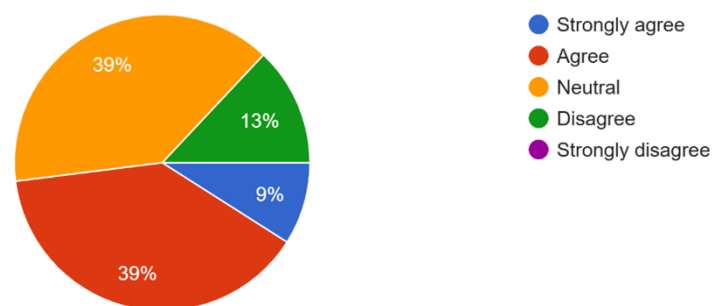


Figure 7.2.3: Awareness of Indian Legal Framework

“Question: I am well-informed about the existing Indian legal framework governing data protection.”

Responses: 9 “percent strongly agreed”, 39 “percent agreed”, 39 “percent were neutral”, and 13 “percent disagreed”.

Interpretation:

The responses suggest a general lack of familiarity with India’s data protection laws, including the Digital Personal Data Protection Act (2023). With 78 percent either neutral or uncertain, the findings reveal low public awareness of statutory provisions and underline the need for enhanced legal literacy initiatives.

100 responses

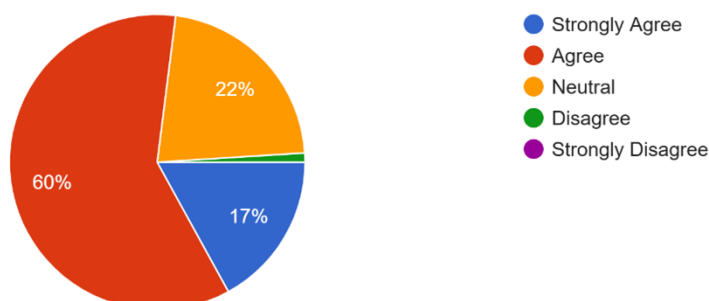


Figure 7.2.4: Need for Legal Provisions on Non-Personal Data

“Question: In my view, the formulation of specific legal provisions for Non-Personal Data is necessary.”

Responses: 17 “percent strongly agreed”, 60 “percent agreed”, 22 “percent were neutral”, and 1 “percent disagreed”.

Interpretation:

An overwhelming 77 percent believe that separate legal provisions for *Non-Personal Data* are necessary. The negligible dissent reflects a strong public perception that current data laws are insufficient and that *NPD* requires independent governance frameworks for ethical and economic balance.

100 responses

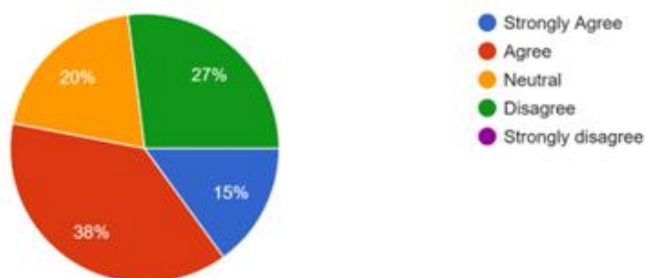


Figure 7.2.5: Effectiveness of Global Uniform Laws

“Question: I consider global uniform data protection laws to be more effective than national laws in addressing data-related challenges.”

Responses: 15 “percent strongly agreed”, 38 “percent agreed”, 20 “percent were neutral”, and 27 “percent disagreed”.

Interpretation:

The division in responses reveals competing policy preferences: 53 percent favor global uniformity, while 27 percent emphasize national sovereignty. This demonstrates public awareness of global governance debates but also highlights ambivalence toward universal frameworks due to contextual differences between jurisdictions.

100 responses

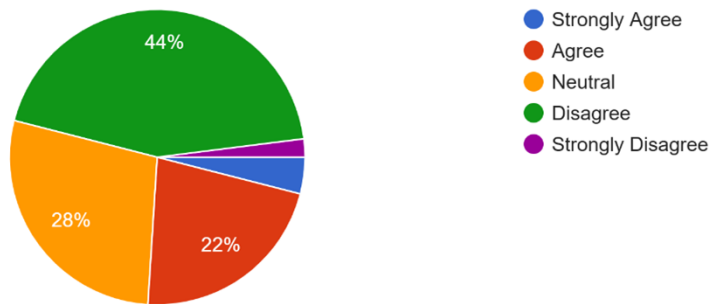


Figure 7.2.6: Adequacy of Indian Law for Personal Data Protection

Question: I am confident that Indian law provides adequate protection for my personal data.

Responses: 5 “percent strongly agreed”, 22 “percent agreed”, 28 “percent were neutral”, 44 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

A substantial 45 percent of respondents disagree with the adequacy of Indian data protection mechanisms. With only 27 percent expressing confidence, public trust appears limited, suggesting that existing enforcement structures may lack transparency or efficiency in implementation.

100 responses

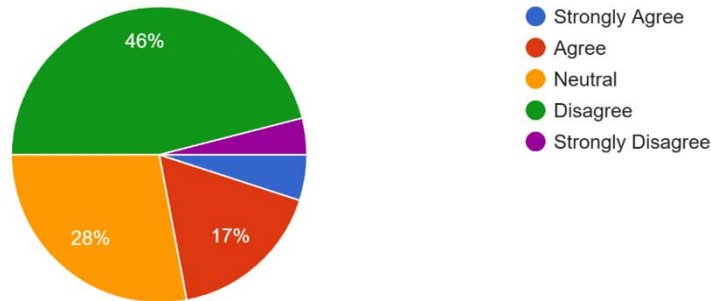


Figure 7.2.7: Sufficiency of Indian Regulations for Non-Personal Data

Question: I believe that existing Indian regulations are sufficient to safeguard non-personal data.

Responses: 5 “percent strongly agreed”, 17 “percent agreed”, 28 “percent were neutral”, 46 “percent disagreed”, and 4 “percent strongly disagreed”.

Interpretation:

The combined 50 percent disagreement underscores public concern over regulatory gaps in *NPD* governance. The low level of agreement (22 percent) highlights the absence of institutional clarity and statutory recognition for *NPD* within India’s broader data governance ecosystem.

100 responses

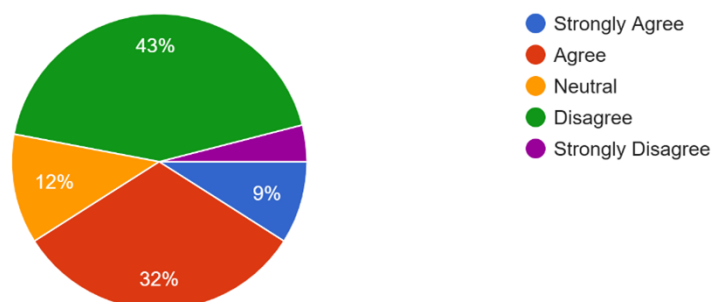


Figure 7.2.8: Awareness of Organizational Use of Non-Personal Data

Question: I am well-informed about how organizations collect and utilize non-personal data.

Responses: 9 “percent strongly agreed”, 32 “percent agreed”, 12 “percent were neutral”, 43 “percent disagreed”, and 4 “percent strongly disagreed”.

Interpretation:

A combined 47 percent disagreement reveals that most respondents lack visibility into organizational data practices. The limited affirmative responses suggest transparency gaps in how anonymized or aggregated data are collected, stored, or monetized by public and private entities.

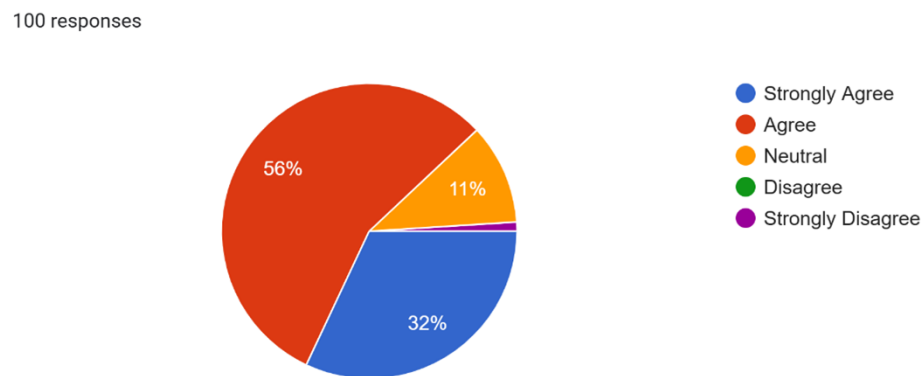


Figure 7.2.9: Need for Legal Protection of Non-Personal Data

Question: I believe that Non-Personal Data should be explicitly protected under legal frameworks.

Responses: 32 “percent strongly agreed”, 56 “percent agreed”, 11 “percent were neutral”, and 1 “percent disagreed”.

Interpretation:

An overwhelming 88 percent support explicit legal protection for non-personal data. This consensus indicates growing public recognition that anonymized and aggregated datasets possess both economic and ethical significance, requiring legislative intervention to ensure responsible use and privacy safeguards.

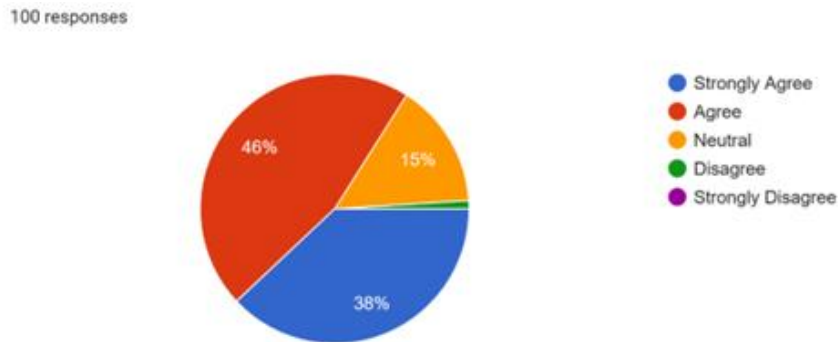


Figure 7.2.10: Concern Over Data Usage by Organizations

Question: I am concerned about the ways in which my personal and Non-Personal Data are utilized by organizations.

Responses: 38 “percent strongly agreed”, 46 “percent agreed”, 15 “percent were neutral”, and 1 “percent disagreed”.

Interpretation:

The high level of concern (84 percent) reflects rising public anxiety regarding surveillance, data profiling, and misuse. These perceptions indicate a growing demand for stronger corporate accountability, clearer consent processes, and transparency in organizational data practices.

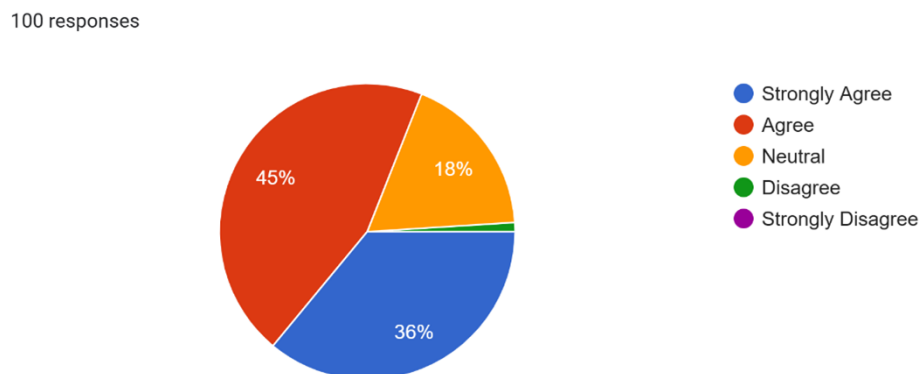


Figure 7.2.11: Need for Uniform Global Data Protection Laws

Question: Uniform global laws for data protection are necessary to ensure comprehensive data security.

Responses: 36 “percent strongly agreed”, 45 “percent agreed”, 18 “percent were neutral”, and 1 “percent disagreed”.

Interpretation:

With 81 percent of respondents supporting global frameworks, the findings emphasize the perceived importance of international cooperation in achieving consistent data-protection standards. The minimal disagreement highlights the globalized nature of data ecosystems and the necessity of cross-border policy alignment.

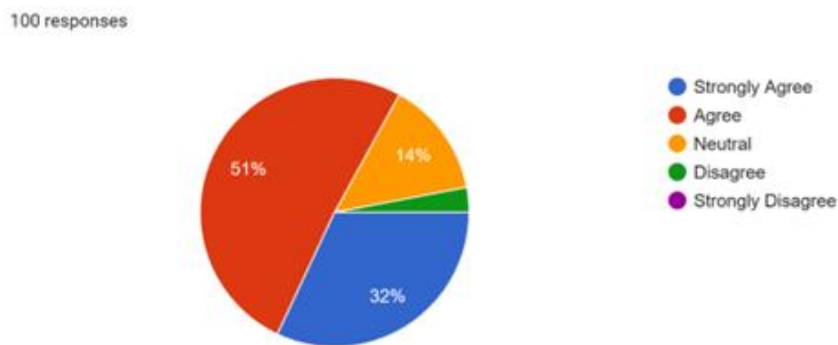


Figure 7.2.12: Support for Stronger National Laws

Question: I support the implementation of more stringent national laws governing personal and Non-Personal Data usage.

Responses: 32 “percent strongly agreed”, 51 “percent agreed”, 14 “percent were neutral”, and 3 “percent disagreed”.

Interpretation:

The 83 percent agreement demonstrates strong public endorsement for stricter national legislation. The findings indicate public confidence in domestic policymaking, coupled with expectations for institutional reforms that balance innovation and privacy protection.

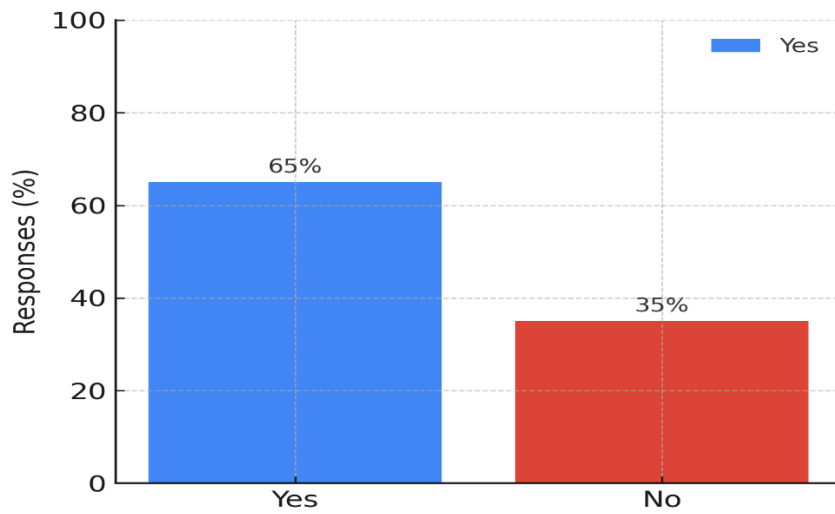


Figure 7.2.13: Personal Experience with Data Privacy Issues

Question: Have you personally experienced issues related to data privacy or misuse, such as identity theft or data breaches?

Responses: 65 percent Yes, 35 percent No.

Interpretation:

The 65 percent affirmative response reveals that data breaches and privacy violations are common experiences. This underscores the urgent need for effective grievance redressal mechanisms and organizational compliance with legal obligations.

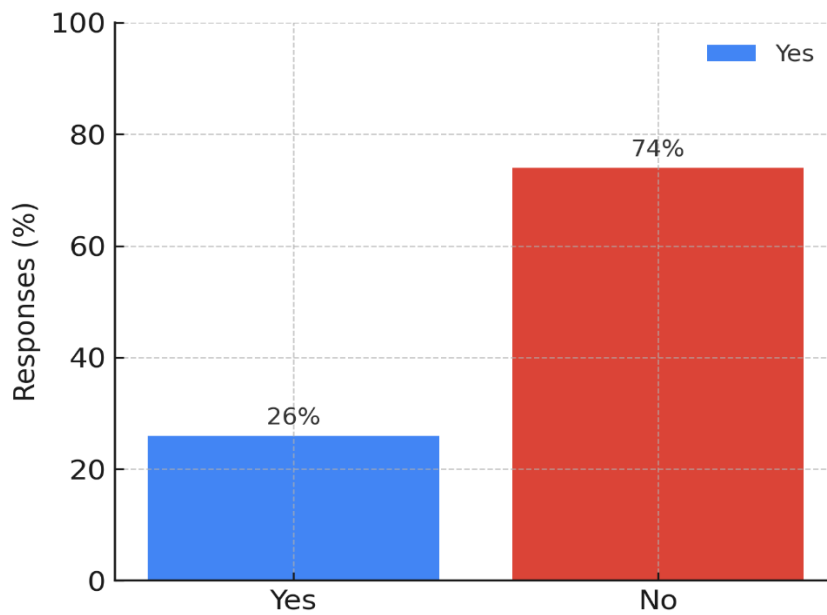


Figure 7.2.14: Action Taken After Data-Related Issues

Question: Did you take any action (e.g., filed a complaint) when faced with data-related issues?

Responses: 26 percent Yes, 74 percent No.

Interpretation:

Despite frequent exposure to privacy violations, only 26 percent acted upon them. This indicates limited trust in institutional processes, lack of awareness of complaint mechanisms, or procedural challenges that deterred reporting.

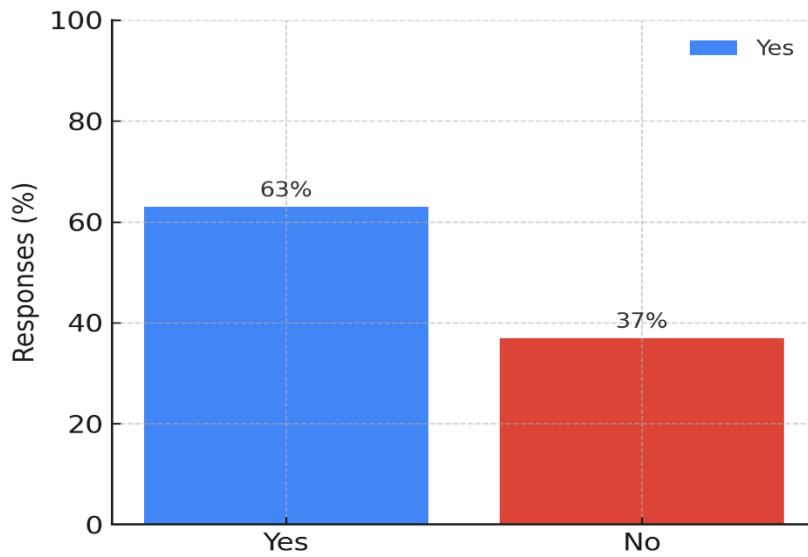


Figure 7.2.15: Reasons for Inaction

Question: If no action was taken, was it due to unclear or insufficient legal provisions?

Responses: 63 percent Yes, 37 percent No.

Interpretation:

The 63 percent affirmative responses show that legislative ambiguity and procedural gaps are key deterrents to seeking remedies. This reinforces the argument that legal clarity and accessible procedures are prerequisites for effective enforcement.

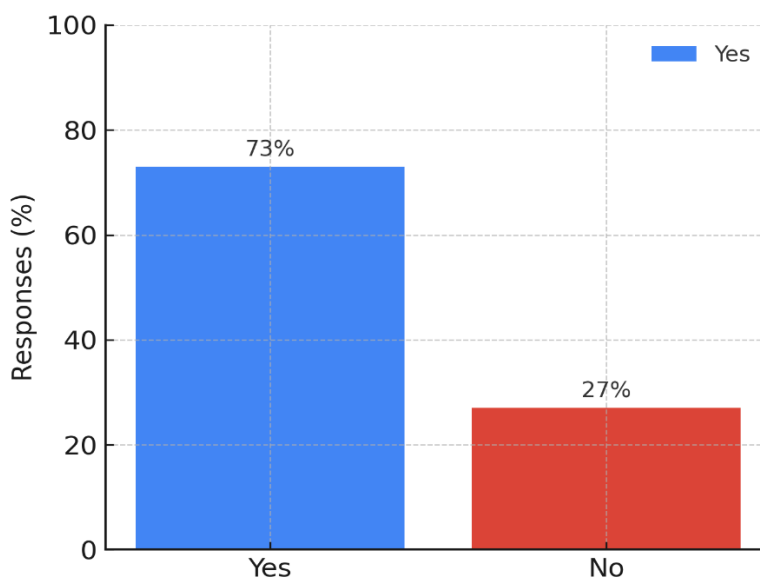


Figure 7.2.16: Awareness of Privacy as a Fundamental Right

Question: Are you aware that personal privacy is recognized as a fundamental right under Indian law?

Responses: 73 percent Yes, 27 percent No.

Interpretation:

The 73 percent awareness reflects moderate public understanding of the *Puttaswamy* (2017) judgment, though the remaining 27 percent unaware indicates continued need for civic legal education on fundamental rights related to data privacy.

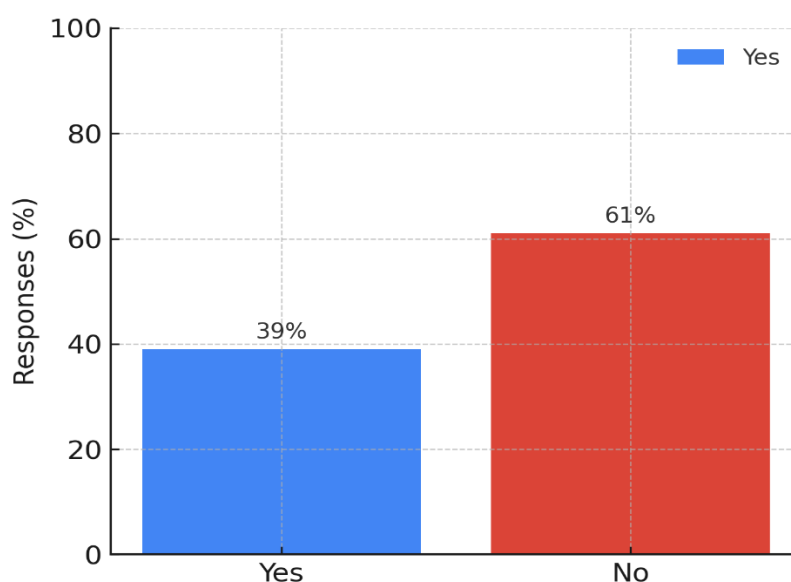


Figure 7.2.17: Awareness of Legal Remedies for Privacy Breach

Question: Do you know the legal remedies available to you if your personal privacy is breached?

Responses: 39 percent Yes, 61 percent No.

Interpretation:

While the right to privacy is widely known, understanding of remedies remains limited. The 61 percent lack of knowledge highlights the gap between formal rights and practical accessibility, underscoring the importance of procedural literacy and outreach initiatives.

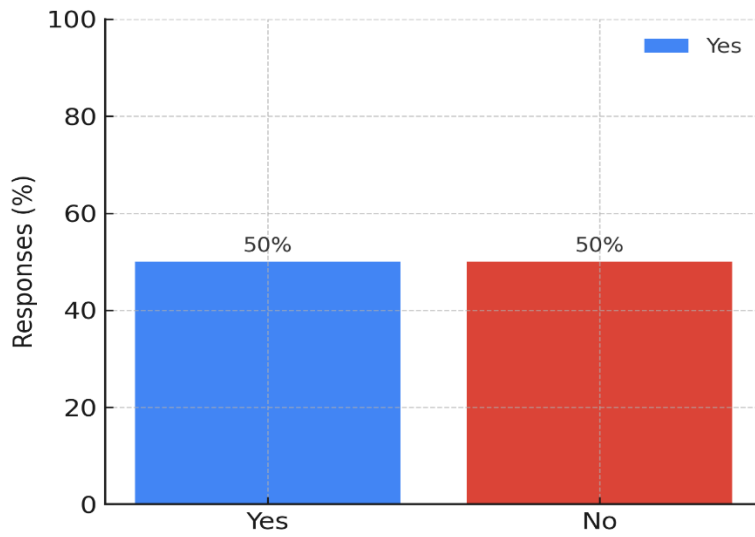


Figure 7.2.18: Knowledge of Relevant Authorities

Question: Are you aware of the relevant authorities (e.g., police, consumer courts, cyber cells) to approach if your data privacy is violated?

Responses: 50 percent Yes, 50 percent No.

Interpretation:

Equal division among respondents demonstrates uneven awareness of institutional mechanisms. This suggests the absence of a unified public-facing authority or centralized platform guiding victims of data breaches.

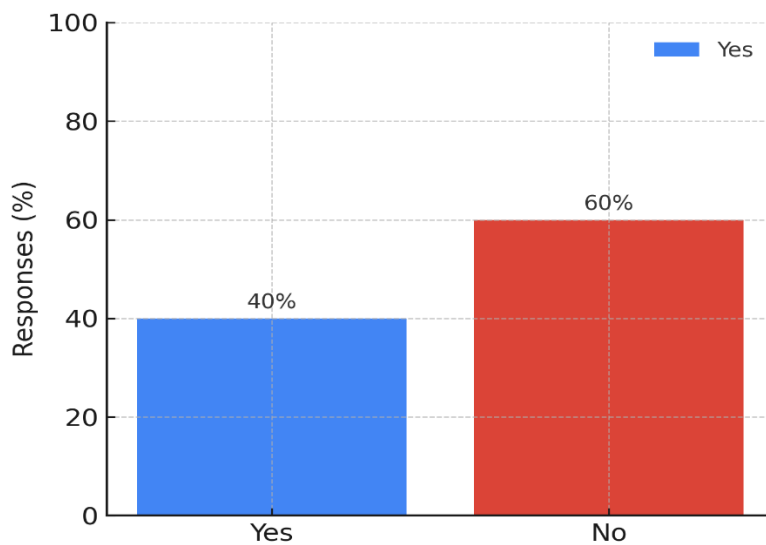


Figure 7.2.19: Understanding of Complaint Process

Question: Do you understand the process of filing a complaint regarding the misuse of personal data?

Responses: 40 percent Yes, 60 percent No.

Interpretation:

The 60 percent negative responses confirm that procedural opacity persists in privacy enforcement. Simplified digital complaint systems and clear communication by regulators are essential to bridge this gap.

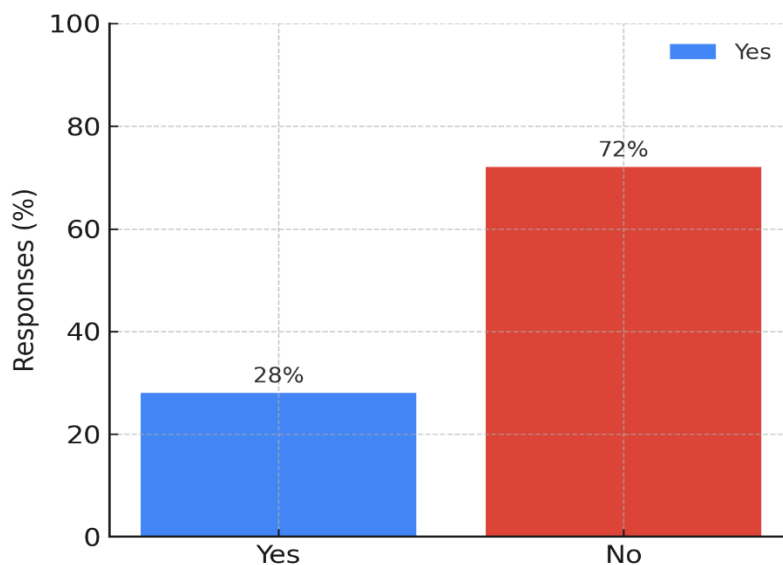


Figure 7.2.20: Disclosure by Organizations or Government

Question: Have you ever been informed by any organization or government agency about how your personal or Non-Personal Data is used?

Responses: 28 percent Yes, 72 percent No.

Interpretation:

The 72 percent negative responses reveal low transparency in data handling. The absence of proactive disclosure undermines accountability and public trust, suggesting the necessity of mandatory notification standards and public transparency measures.

7.2.3 Summary of Key Findings

The analysis of responses from the general public reveals a multifaceted understanding of data concepts, legal awareness, and perceptions regarding the adequacy of current data governance frameworks. The findings highlight both encouraging trends of awareness and significant gaps in legal literacy, procedural familiarity, and trust in institutional mechanisms. These results offer a critical reflection on the readiness of the public to engage effectively with emerging data governance regimes.

The descriptive data indicates that a majority of respondents possess a foundational understanding of the concept of data and demonstrate awareness of the distinction between personal and non-personal data. This awareness, however, remains primarily conceptual rather than practical. While most participants affirm general familiarity with data-related terms, their ability to distinguish, apply, and interpret these categories in legal or technological contexts appears limited. The prevalence of neutral responses across questions concerning definitional clarity and the Indian legal framework underscores that conceptual understanding has not yet evolved into substantive legal or procedural comprehension.

A clear consensus emerges regarding the necessity for specific legal provisions addressing non-personal data. Respondents overwhelmingly favor the establishment of an independent regulatory framework to manage anonymized, aggregated, and machine-generated datasets. This sentiment reflects a growing recognition of the economic and societal value of *Non-Personal Data* and the public's expectation that it should be governed by transparent and accountable mechanisms. The inclination toward stronger national legislation and simultaneous support for global harmonization reflects an understanding that data governance is inherently transnational yet must remain contextually adaptable. Participants' preference for stringent domestic laws suggests trust in localized policy implementation, while their endorsement of global uniformity acknowledges the need for international cooperation to combat cross-border risks such as data misuse and cybercrime.

The perception of the adequacy of existing Indian data protection laws remains cautious. A significant portion of respondents express limited confidence in the

effectiveness of current statutory instruments, indicating skepticism about enforcement capacity and institutional responsiveness. Public opinion reflects that while India's legislative framework, particularly the Digital Personal Data Protection Act, 2023, marks an essential step toward protecting individual rights, gaps persist in regulating non-personal and anonymized datasets. Respondents also convey concern over the lack of transparency among organizations in disclosing data collection and usage practices, suggesting a need for statutory mandates on disclosure and audit obligations.

Experience-based responses reveal that data privacy concerns are not abstract but widely encountered in daily digital interactions. A substantial majority of respondents have personally faced issues related to data breaches, misuse, or identity theft. Despite this, a large proportion of those affected did not pursue any formal action, highlighting a pronounced enforcement and awareness deficit. The primary reason cited for inaction, unclear or insufficient legal provisions, illustrates a gap between the existence of laws and their accessibility to the average citizen. This points to an urgent need for public-facing mechanisms that translate complex legal provisions into actionable pathways for grievance redressal.

The responses concerning legal and institutional awareness show mixed results. While most respondents recognize that personal privacy is a constitutionally protected right following the landmark *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) judgment, fewer are familiar with the remedies or authorities available in the event of a privacy breach. Half of the respondents remain unaware of which institutional channels, such as cyber cells, data protection boards, or consumer forums, can be approached for assistance. This evidences the absence of a unified institutional framework and demonstrates that awareness of substantive rights has not been matched by procedural understanding. The majority's limited familiarity with the complaint process further emphasizes the need for simplified, digitalized, and accessible grievance mechanisms.

Transparency and accountability emerged as critical areas of public concern. A significant proportion of participants reported never being informed by any

organization or government agency regarding the collection or use of their personal or non-personal data. This lack of disclosure represents an asymmetry between data controllers and data subjects, undermining the principles of informed consent and participatory governance. It reflects the public's growing demand for proactive transparency obligations, periodic data audits, and stronger accountability mechanisms to restore trust in both public and private data custodians.

In summary, the general public exhibits a developing but incomplete awareness of data governance concepts, an increasing demand for specific legal instruments governing non-personal data, and a pronounced need for institutional clarity. Respondents show alignment with both domestic and international reform trajectories, suggesting that public sentiment favors a hybrid governance model, one that balances national sovereignty with global cooperation. However, the findings also reveal that the effectiveness of any such regime depends on the public's ability to understand, access, and utilize legal remedies. The results thus substantiate the hypothesis that public awareness of data protection remains in a formative stage, requiring comprehensive legal literacy initiatives, institutional transparency, and procedural simplification to bridge the gap between legal frameworks and societal engagement.

Table 7.2.1 Summary of Key Responses from the General Public on Awareness and Perceptions of Non-Personal Data

Statement Number	Statement (Shortened)	Raw Response Data (Exact %)	Key Metric (% Agreement/Yes)	Main Insight
1	Comprehensive understanding of data concepts	Strongly Agree: 15%, Agree: 53%, Neutral: 22%, Disagree: 10%	53% Agree + 15% Strongly Agree	Majority indicate understanding, though 22% neutral shows uncertainty.
2	Can distinguish personal vs non-personal data	Strongly Agree: 16%, Agree: 50%, Neutral: 22%, Disagree: 12%	50% Agree + 16% Strongly Agree	Most claim ability, but 34% neutral/disagree indicates conceptual ambiguity.

		Disagree: 12%		
3	Well-informed about Indian legal framework	Strongly Agree: 9%, Agree: 39%, Neutral: 39%, Disagree: 13%	39% Agree + 9% Strongly Agree	Low legal awareness; 78% not confident or unsure of laws like DPDP Act 2023.
4	Need legal provisions for Non-Personal Data	Strongly Agree: 17%, Agree: 60%, Neutral: 22%, Disagree: 1%	60% Agree + 17% Strongly Agree	Strong public demand for a separate NPD legal framework.
5	Global uniform laws more effective than national laws	Strongly Agree: 15%, Agree: 38%, Neutral: 20%, Disagree: 27%	38% Agree + 15% Strongly Agree	Respondents divided; concerns over feasibility of global harmonization.
6	Indian law protects personal data adequately	Strongly Agree: 5%, Agree: 22%, Neutral: 28%, Disagree: 44%, Strongly Disagree: 1%	22% Agree + 5% Strongly Agree	Low confidence; 45% disagree indicates lack of trust in enforcement.
7	Indian regulation sufficient for Non-Personal Data	Strongly Agree: 5%, Agree: 17%, Neutral: 28%, Disagree: 46%, Strongly Disagree: 4%	17% Agree + 5% Strongly Agree	Majority believe NPD governance is insufficient.
8	Aware of how organizations use Non-Personal Data	Strongly Agree: 9%, Agree: 32%, Neutral: 12%,	32% Agree + 9% Strongly Agree	Low visibility into organizational data practices and transparency issues.

		Disagree: 43%, Strongly Disagree: 4%		
9	NPD should be legally protected	Strongly Agree: 32%, Agree: 56%, Neutral: 11%, Disagree: 1%	56% Agree + 32% Strongly Agree	Very strong support for explicit legal protection.
10	Concerned about organizational data usage	Strongly Agree: 38%, Agree: 46%, Neutral: 15%, Disagree: 1%	46% Agree + 38% Strongly Agree	High public concern regarding surveillance and misuse.
11	Need for uniform global data protection laws	Strongly Agree: 36%, Agree: 45%, Neutral: 18%, Disagree: 1%	45% Agree + 36% Strongly Agree	Strong support for global alignment and interoperability.
12	Support stronger national laws	Strongly Agree: 32%, Agree: 51%, Neutral: 14%, Disagree: 3%	51% Agree + 32% Strongly Agree	Public strongly endorses tougher domestic laws.
13	Experienced data privacy/misuse issues	Yes: 65%, No: 35%	65% Yes	Data misuse is widely experienced among respondents.
14	Took action after data misuse	Yes: 26%, No: 74%	26% Yes	Most take no action due to lack of trust or awareness of remedies.
15	Inaction due to unclear legal provisions	Yes: 63%, No: 37%	63% Yes	Legal ambiguity is a major reason for lack of redressal.
16	Aware privacy is a fundamental right	Yes: 73%, No: 27%	73% Yes	Majority aware of constitutional right, though 27% remain unaware.
17	Know legal remedies for privacy breach	Yes: 39%, No: 61%	39% Yes	Public lacks practical knowledge of remedies despite formal rights.

18	Aware of relevant authorities	Yes: 50%, No: 50%	50% Yes	Evenly divided, showing uncertainty in enforcement pathways.
19	Understand complaint process	Yes: 40%, No: 60%	40% Yes	Complaint procedures unclear for most respondents.
20	Ever informed by any entity about data use	Yes: 28%, No: 72%	28% Yes	Very low transparency by organizations/government.

7.3 Legal Professionals

7.3.1 Descriptive Statistics and Interpretation

This section presents responses from 100 legal professionals (judges, advocates, and legal officers) regarding their understanding, awareness, and perception of data governance, including personal and non-personal data. The analysis uses descriptive statistics based on percentage distribution and corresponding interpretations to capture both the level of awareness and the perceived adequacy of existing legal frameworks.

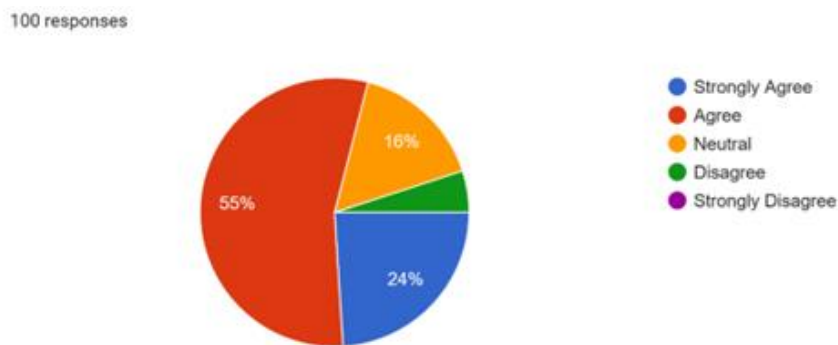


Figure 7.3.1: Understanding of Data Concepts

Question: I possess a comprehensive understanding of the concept of data, including personal and non-personal data.

Responses: 24 “percent strongly agreed”, 55 “percent agreed”, 16 “percent were neutral”, and 5 “percent disagreed”.

Interpretation:

The data indicates that a combined 79 percent of legal professionals acknowledge having a comprehensive understanding of data concepts. The presence of 16 percent neutral responses suggests that a small segment is yet to develop full conceptual clarity. The 5 percent disagreement points to the need for continued sensitization among practitioners regarding evolving classifications such as anonymized or aggregated data.

100 responses

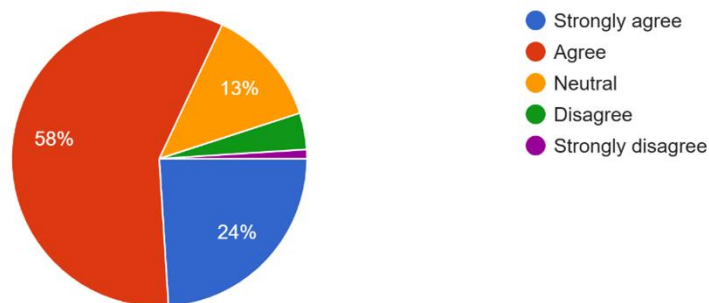


Figure 7.3.2: Capability to Distinguish Between Personal and Non-Personal Data

Question: I am capable of clearly distinguishing between personal data and non-personal data.

Responses: 24 “percent strongly agreed”, 58 “percent agreed”, 13 “percent were neutral”, 4 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

A majority (82 percent) of respondents affirm their ability to distinguish between personal and non-personal data. However, the 13 percent neutral and 5 percent dissenting responses imply that even within the legal community, there remains ambiguity regarding the precise legal boundary between these categories, particularly given the evolving nature of anonymization and re-identification standards.

100 responses

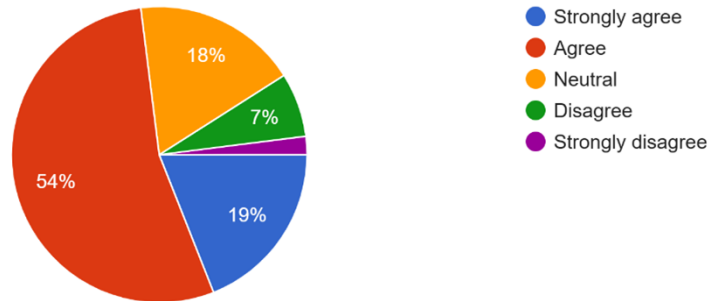


Figure 7.3.3: Awareness of Indian Legal Framework on Data Protection

Question: I am well-informed about the existing Indian legal framework governing data protection.

Responses: 19 “percent strongly agreed”, 54 “percent agreed”, 18 “percent were neutral”, 7 “percent disagreed”, and 2 “percent strongly disagreed”.

Interpretation:

The data reveals that 73 percent of legal professionals are aware of India’s data protection framework, including the Digital Personal Data Protection Act, 2023. However, 27 percent either remain uncertain or uninformed, reflecting that while general awareness exists, comprehensive understanding of procedural and regulatory details requires strengthening through targeted continuing legal education.

100 responses

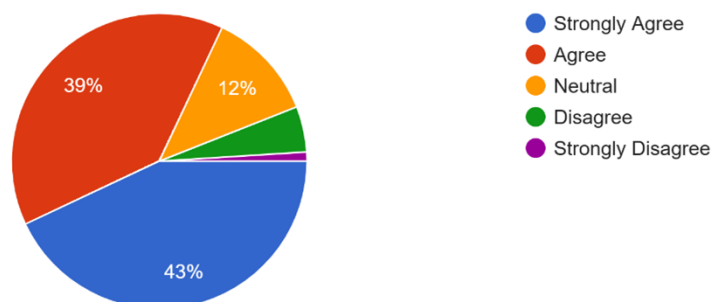


Figure 7.3.4: Necessity for Specific Legal Provisions on Non-Personal Data

Question: In my view, the formulation of specific legal provisions for Non-Personal Data is necessary.

Responses: 43 “percent strongly agreed”, 39 “percent agreed”, 12 “percent were neutral”, 4 “percent disagreed”, and 2 “percent strongly disagreed”.

Interpretation:

An overwhelming 82 percent of respondents advocate for dedicated legal provisions on non-personal data. This consensus underscores recognition within the legal community that current laws primarily address personal data, leaving a gap in the governance of anonymized or industrial datasets. The limited disagreement indicates near-universal endorsement of a separate legislative framework.

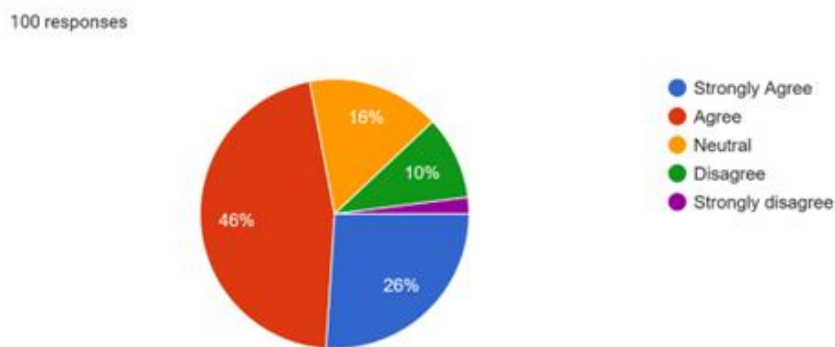


Figure 7.3.5: Preference for Global Uniform Data Protection Laws

Question: I consider global uniform data protection laws to be more effective than national laws in addressing data-related challenges.

Responses: 26 “percent strongly agreed”, 46 “percent agreed”, 16 “percent were neutral”, 10 “percent disagreed”, and 2 “percent strongly disagreed”.

Interpretation:

A total of 72 percent of legal professionals favor global uniform data protection frameworks. The remaining 28 percent reflect either neutrality or resistance, possibly grounded in the belief that national laws should retain flexibility to address jurisdiction-specific challenges. The overall result highlights the recognition of globalization’s impact on data movement and cross-border privacy concerns.

100 responses

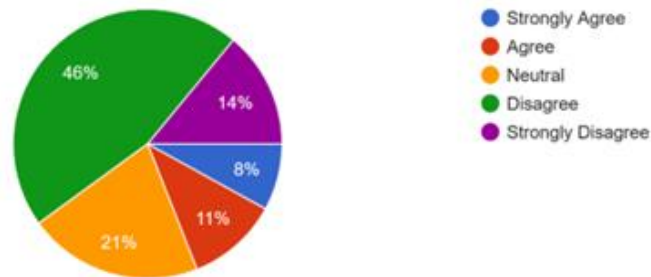


Figure 7.3.6: Adequacy of Indian Legal Framework for Personal Data

Question: I believe the current Indian legal framework adequately addresses challenges related to personal data.

Responses: 8 “percent strongly agreed”, 11 “percent agreed”, 21 “percent were neutral”, 46 “percent disagreed”, and 14 “percent strongly disagreed”.

Interpretation:

The 60 percent disagreement reflects skepticism regarding the adequacy of India’s current legal framework for personal data protection. This could stem from perceived enforcement weaknesses or procedural delays. The 19 percent agreement demonstrates limited confidence in the DPDP Act’s ability to address emerging digital threats, while 21 percent neutrality suggests cautious optimism pending implementation outcomes.

100 responses

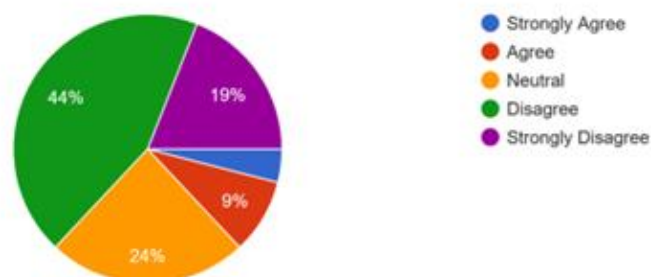


Figure 7.3.7: Sufficiency of Indian Legal Provisions for Non-Personal Data

Question: I consider the existing Indian legal provisions sufficient to regulate Non-Personal Data usage and protection.

Responses: 4 “percent strongly agreed”, 9 “percent agreed”, 24 “percent were neutral”, 44 “percent disagreed”, and 19 “percent strongly disagreed”.

Interpretation:

With 63 percent disagreement, respondents largely reject the sufficiency of current legal mechanisms for regulating non-personal data. Only 13 percent express satisfaction, reflecting an understanding that India lacks a comprehensive framework for anonymized datasets. The findings reveal a strong perceived need for new legislative or regulatory instruments.

100 responses

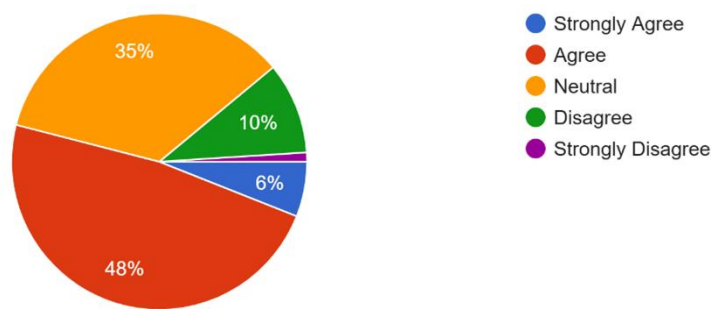


Figure 7.3.8: Confidence in Applying Data Protection Laws

Question: I am confident in effectively applying Indian data protection laws within legal proceedings.

Responses: 6 “percent strongly agreed”, 48 “percent agreed”, 35 “percent were neutral”, and 10 “percent disagreed”.

Interpretation:

The 54 percent who express confidence demonstrate moderate professional readiness to apply data protection laws in litigation. However, 35 percent neutrality reveals that procedural and interpretive uncertainties persist, possibly due to the recent enactment of relevant laws and the limited availability of judicial precedents.

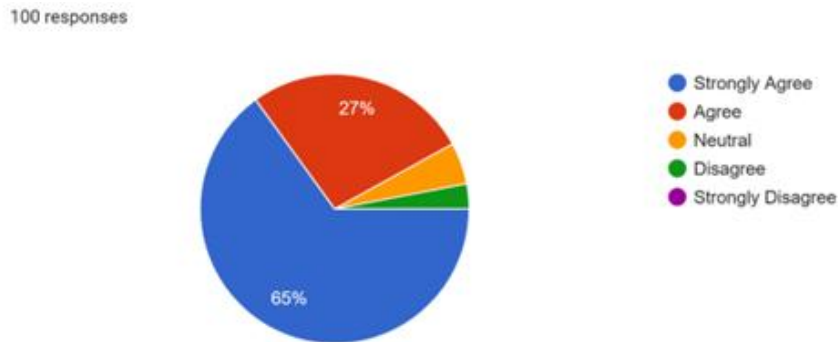


Figure 7.3.9: Need for Specialized Legal Training

Question: There is a substantial need for specialized legal training for law enforcement agencies in handling data-related cases.

Responses: 65 “percent strongly agreed”, 27 “percent agreed”, 5 “percent were neutral”, 2 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

An overwhelming 92 percent consensus underscores the recognized need for specialized legal training for law enforcement and judicial officers. This finding aligns with the broader observation that technological complexity in data cases often outpaces current legal and procedural capabilities, necessitating targeted capacity-building initiatives.

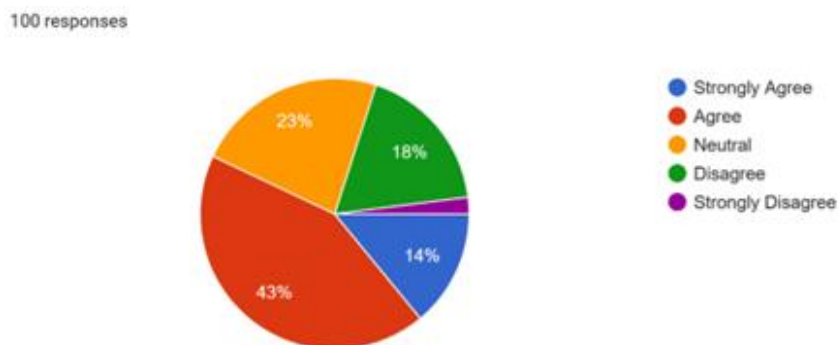


Figure 7.3.10: Knowledge of International Data Protection Laws

Question: I am knowledgeable about international data protection laws, including regulations such as the GDPR.

Responses: 14 “percent strongly agreed”, 43 “percent agreed”, 23 “percent were neutral”, 18 “percent disagreed”, and 2 “percent strongly disagreed”.

Interpretation:

A cumulative 57 percent of respondents claim knowledge of international data protection laws, suggesting moderate global legal awareness. The 23 percent neutral and 20 percent dissenting responses imply that while exposure to frameworks such as the GDPR is common, detailed comparative understanding remains limited among practitioners primarily engaged in domestic law.

100 responses

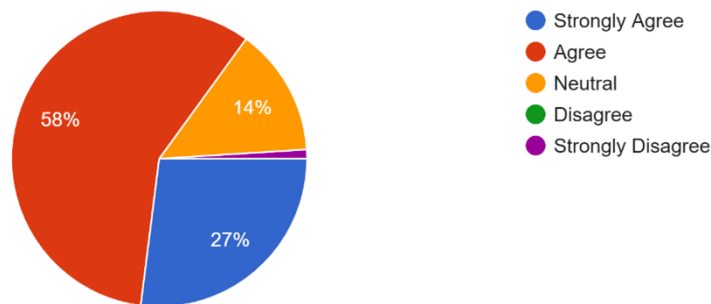


Figure 7.3.11: Amendment Necessity in Existing Data Protection Laws

Question: I believe existing Indian data protection laws require amendments to address emerging challenges.

Responses: 27 “percent strongly agreed”, 58 “percent agreed”, 14 “percent were neutral”, and 1 “percent disagreed”.

Interpretation:

A clear majority (85 percent) agree that existing laws such as the Digital Personal Data Protection Act, 2023, require amendments to address evolving technological realities. This consensus among law implementers underscores a demand for continuous legislative updating, particularly concerning artificial intelligence, data monetization, and anonymization safeguards.

100 responses

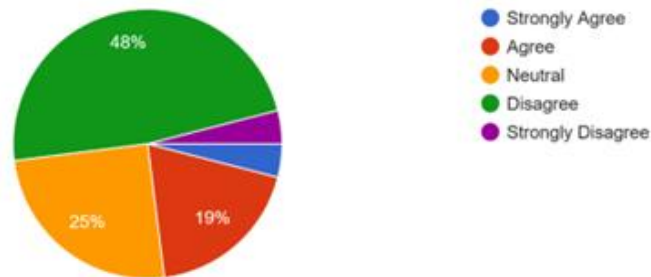


Figure 7.3.12: Clarity of Legal Distinction Between Personal and Non-Personal Data

Question: The legal distinction between personal and Non-Personal Data is sufficiently clear for application in legal contexts.

Responses: 4 “percent strongly agreed”, 19 “percent agreed”, 25 “percent were neutral”, 48 “percent disagreed”, and 4 “percent strongly disagreed”.

Interpretation:

A combined 52 percent disagreement reveals that legal practitioners find the current distinction between personal and *Non-Personal Data* inadequate for clear application in judicial or procedural contexts. This uncertainty indicates that while conceptual definitions exist, their operational clarity is yet to be established in Indian jurisprudence.

100 responses

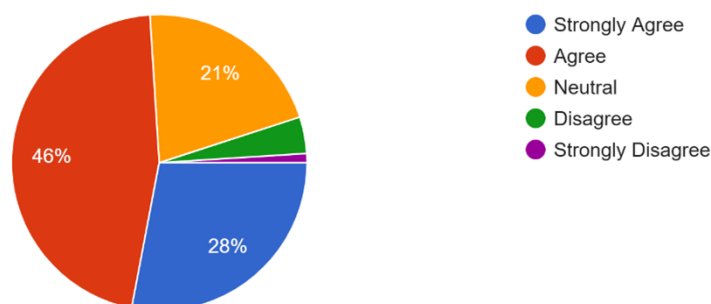


Figure 7.3.13: Need for Comprehensive Non-Personal Data Regulations

Question: In my opinion, Non-Personal Data necessitates a distinct and comprehensive set of legal regulations.

Responses: 28 “percent strongly agreed”, 46 “percent agreed”, 21 “percent were neutral”, 4 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

An overwhelming 74 percent of respondents support the need for a separate, comprehensive legal regime for non-personal data. This reflects growing recognition among legal professionals that existing frameworks, focused on personal data, are insufficient to manage collective or industrial datasets that possess both economic and societal implications.

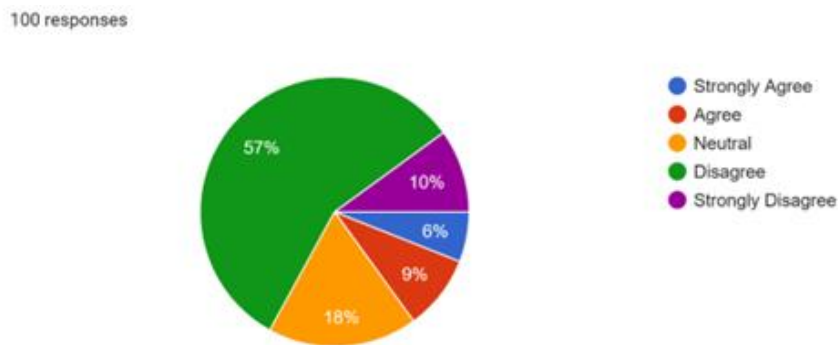


Figure 7.3.14: Awareness of Non-Personal Data Regulations in Legal Community

Question: I believe that the legal community in India is adequately informed about Non-Personal Data regulations.

Responses: 6 “percent strongly agreed”, 9 “percent agreed”, 18 “percent were neutral”, 57 “percent disagreed”, and 10 “percent strongly disagreed”.

Interpretation:

A combined 67 percent of respondents disagree that the legal community is adequately informed about *NPD* regulations. This reflects an awareness gap, likely due to the absence of codified law on *NPD* and limited judicial precedents. Continuous legal training and inclusion of *NPD* in professional curricula appear necessary to bridge this gap.

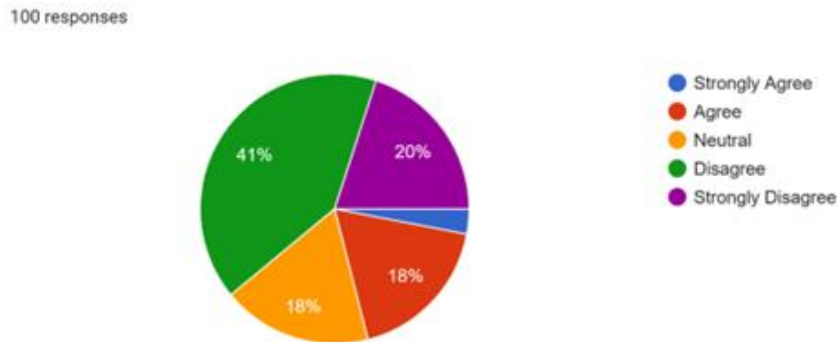


Figure 7.3.15: Sufficiency of National Legal Frameworks

Question: National legal frameworks are sufficient to address issues arising from Non-Personal Data in the Indian context.

Responses: 3 “percent strongly agreed”, 18 “percent agreed”, 18 “percent were neutral”, 41 “percent disagreed”, and 20 “percent strongly disagreed”.

Interpretation:

A combined 61 percent of respondents believe national legal frameworks are insufficient to address *NPD*-related issues. This highlights a lack of confidence in India’s ability to independently manage cross-border data challenges without referencing international standards or collaboration.

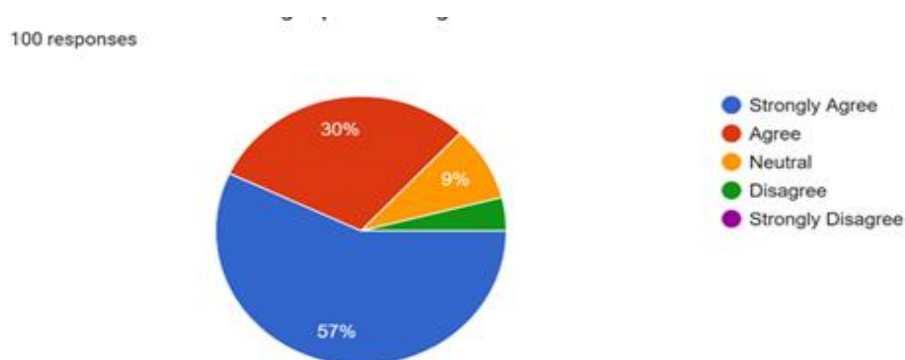


Figure 7.3.16: Need for Collaboration Between Law Enforcement and Cyber Experts

Question: Enhanced collaboration between law enforcement agencies and cyber experts is essential for effective data-related legal proceedings.

Responses: 57 “percent strongly agreed”, 30 “percent agreed”, 9 “percent were neutral”, and 4 “percent disagreed”.

Interpretation:

A near-unanimous 87 percent support demonstrates the legal community’s recognition of interdisciplinary cooperation as a cornerstone of data governance. This finding underscores the need for integrated investigation models and expert-assisted adjudication in cyber and data-related litigation.

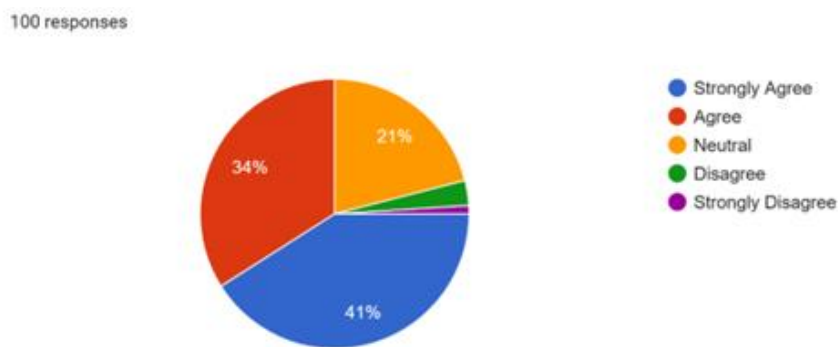


Figure 7.3.17: Relevance of International Frameworks

Question: I believe adopting international frameworks on Non-Personal Data governance would enhance the effectiveness of Indian legal systems.

Responses: 41 “percent strongly agreed”, 34 “percent agreed”, 21 “percent were neutral”, 3 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

With 75 percent agreement, there is strong professional support for incorporating global best practices such as the EU’s Data Governance Act and OECD privacy standards. Respondents recognize that convergence with international frameworks could improve consistency, interoperability, and enforcement of data protection norms.

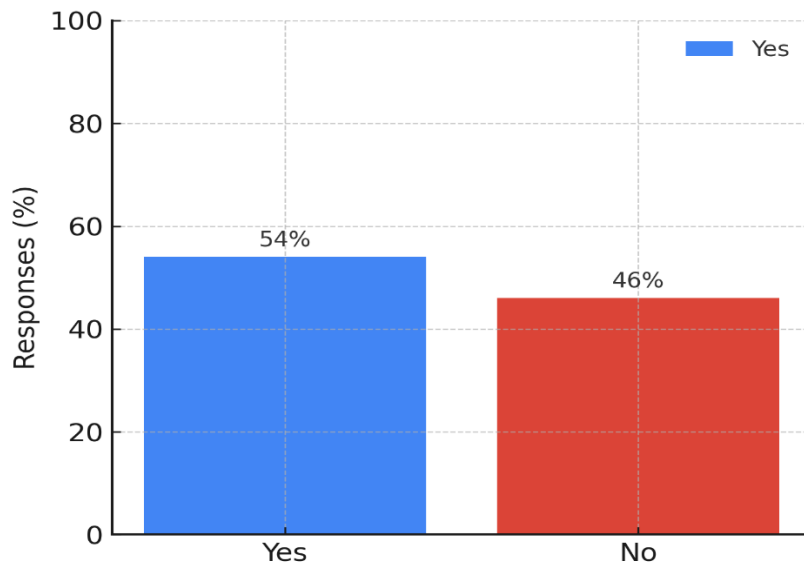


Figure 7.3.18: Exposure to Data Misuse or Breach Cases

Question: Have you encountered cases involving data misuse or breaches in your professional capacity?

Responses: 54 percent Yes, 46 percent No.

Interpretation:

The 54 percent affirmative responses confirm that data misuse cases are increasingly entering the legal domain. This experiential insight suggests that data-related disputes are no longer peripheral but are becoming a regular feature in both civil and criminal litigation.

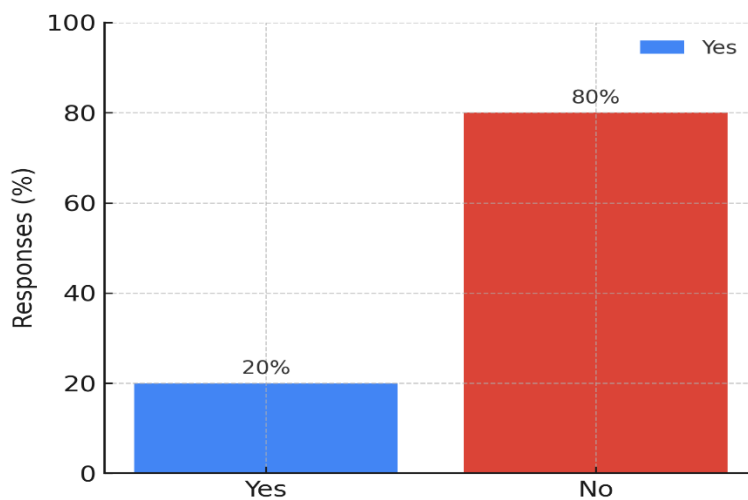


Figure 7.3.19: Pursuit of Legal Action in Data-Related Issues

Question: In instances of data-related issues, did you pursue any legal action?

Responses: 20 percent Yes, 80 percent No.

Interpretation:

Despite encountering violations, only 20 percent of respondents reported pursuing formal legal action. This low engagement reflects systemic barriers—such as procedural complexity, evidentiary difficulty, or limited client initiative—that hinder effective legal recourse in data-related cases.

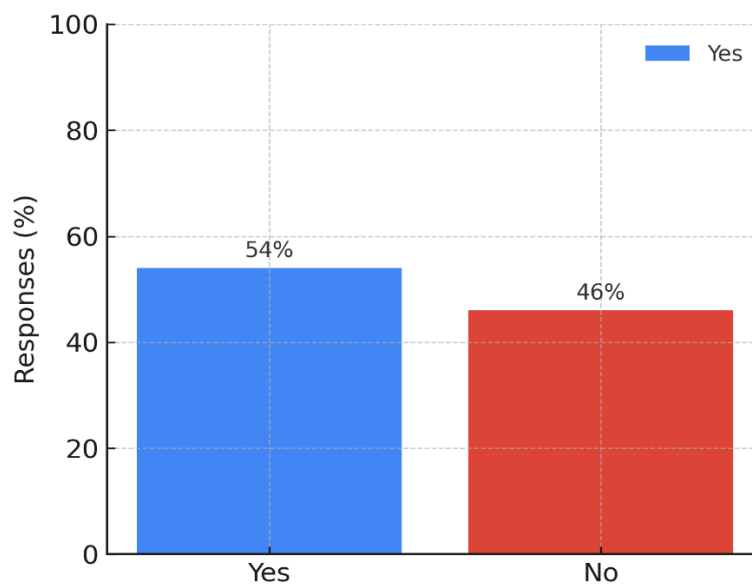


Figure 7.3.20: Reasons for Non-Pursuit of Legal Action

Question: If no legal action was taken, was it due to perceived inadequacies or ambiguities in existing laws?

Responses: 54 percent Yes, 46 percent No.

Interpretation:

A majority (54 percent) attribute their inaction to legal ambiguity, reinforcing the earlier finding that current laws lack sufficient clarity and procedural direction. This outcome indicates the need for legislative refinement to enhance accessibility and precision in enforcement mechanisms for both personal and *Non-Personal Data* cases.

7.3.2 Summary of Key Findings

The responses from the community of legal professionals, comprising judges, advocates, and legal officers, reveal an intricate understanding of data governance coupled with discernible gaps in legislative clarity, institutional preparedness, and procedural awareness. The findings collectively portray the Indian legal ecosystem as being conceptually aligned with contemporary data protection principles but operationally underprepared for the complexities associated with *Non-Personal Data* governance.

The descriptive analysis establishes that a substantial majority of legal professionals (79 percent) claim to possess a comprehensive understanding of the concept of data, including personal and non-personal dimensions. However, when probed further, only 82 percent indicated confidence in distinguishing between the two categories, revealing that definitional comprehension exists largely at a theoretical level rather than through judicial application. The persistence of 13 percent neutral and 5 percent dissenting responses underscores the continued conceptual ambiguity surrounding anonymized, aggregated, and pseudonymized datasets, categories that frequently blur the boundary between personal and non-personal domains in legal practice.

Awareness of the existing Indian legal framework, particularly the Digital Personal Data Protection Act, 2023, was affirmed by 73 percent of respondents, but the remaining 27 percent either expressed uncertainty or admitted limited familiarity. This suggests that while the legal fraternity is broadly aware of the existence of statutory norms, the depth of engagement with procedural or regulatory specifics remains uneven. Such disparities are concerning given that the interpretive burden of new data protection law will primarily rest on legal practitioners and adjudicators.

An overwhelming 82 percent of respondents advocate the formulation of a dedicated legal framework for non-personal data, reflecting near-universal acknowledgment that the current regulatory environment inadequately addresses anonymized and industrial datasets. This viewpoint aligns with international trends wherein jurisdictions such as the European Union, Japan, and Singapore have already institutionalized governance mechanisms for non-personal data. Similarly, 72 percent support the establishment of

global uniform data protection standards, demonstrating a recognition that national frameworks alone cannot effectively manage transnational data flows and cross-border misuse.

Despite moderate familiarity with international instruments such as the *General Data Protection Regulation (GDPR)*, only 57 percent reported confidence in their knowledge of these regimes. This limited global awareness, juxtaposed with the 92 percent endorsement of specialized training for enforcement agencies, points to an institutional recognition of knowledge asymmetry within the Indian legal system. Respondents emphasized the necessity for interdisciplinary capacity building, integrating technological literacy, cyber forensics, and legal interpretation, to handle data-related disputes effectively.

The perceived adequacy of the Indian legal framework yielded mixed responses. A significant 60 percent expressed skepticism about the sufficiency of existing laws in safeguarding personal data, while 63 percent considered current provisions inadequate to regulate non-personal data. This dual deficit perception suggests that the legal community perceives the Digital Personal Data Protection Act, 2023, as a foundational yet incomplete instrument, one that fails to comprehensively address anonymization, data reuse, and industrial data governance. Nearly 85 “percent agreed” that existing data protection statutes require amendments to adapt to emerging technological and policy challenges. These findings collectively highlight the need for legislative expansion toward an integrated data governance framework encompassing both personal and non-personal datasets.

Further, 52 percent of respondents disagreed that the legal distinction between personal and *Non-Personal Data* is sufficiently clear for application in judicial contexts. This finding reveals that while definitional attempts exist, statutory articulation remains abstract, lacking interpretive guidance or precedent. The absence of authoritative jurisprudence on anonymization thresholds and re-identification standards contributes to this uncertainty. Such conceptual opacity risks inconsistent judicial outcomes and could impede the operationalization of data rights.

Another significant insight pertains to the legal community's self-assessed awareness regarding *Non-Personal Data* governance. A combined 67 percent disagreement on adequate information levels indicates that even among practitioners, the discourse on *Non-Personal Data* remains peripheral. The gap between statutory awareness and actionable knowledge suggests an urgent need for continuing legal education programs and the inclusion of *Non-Personal Data* modules in bar and judicial training curricula.

Institutional collaboration and global convergence emerged as dominant priorities. A striking 87 percent consensus recognized the necessity of enhanced collaboration between law enforcement agencies and cyber experts for effective adjudication of data-related cases. This reinforces the understanding that data regulation transcends traditional legal domains, requiring integration with technical, investigative, and policy expertise. Likewise, 75 percent of respondents endorsed adopting international frameworks, such as the EU Data Governance Act, as models to strengthen India's data governance architecture.

The experiential dimension of the survey reveals that 54 percent of legal professionals have encountered cases involving data breaches or misuse, signifying the increasing judicialization of data-related conflicts. However, 80 percent admitted not pursuing legal action, primarily due to perceived ambiguities or inadequacies in the law, as affirmed by 54 percent of respondents. This hesitation reflects a systemic gap between the recognition of harm and the practical ability to seek redress, underscoring deficiencies in procedural mechanisms, evidentiary clarity, and the scope of statutory remedies.

Taken together, the responses portray a legal fraternity that is intellectually receptive but procedurally constrained. There exists strong conceptual endorsement of the need for a robust legal framework governing non-personal data, yet its translation into judicial and administrative practice remains limited. The findings suggest that legislative reform should be accompanied by judicial capacity building, codification of definitional standards, and inter-agency collaboration mechanisms. Additionally, the harmonization of domestic data protection law with international standards would

not only strengthen India’s regulatory credibility but also ensure legal certainty for cross-border data governance.

In conclusion, while law implementers demonstrate commendable awareness and forward-looking attitudes toward data protection, the survey underscores three structural imperatives for reform, first, statutory precision in distinguishing and regulating non-personal data; second, institutional strengthening through specialized training and expert collaboration; and third, procedural transparency to enable effective enforcement and redressal. These elements collectively mark the transition from theoretical alignment to actionable readiness in India’s evolving data governance landscape.

Table 7.3.1 Summary of Key Responses from Legal Professionals on Awareness and Perceptions of Non-Personal Data

Statement Number	Statement (Shortened)	Raw Response Data (Exact %)	Key Metric (% Agreement/Yes)	Main Insight
1	Comprehensive understanding of data concepts	Strongly Agree: 24%, Agree: 55%, Neutral: 16%, Disagree: 5%, Strongly Disagree: 0%	24% Strongly Agree + 55% Agree	Majority demonstrate strong conceptual clarity, with minimal disagreement.
2	Can distinguish personal vs non-personal data	Strongly Agree: 24%, Agree: 58%, Neutral: 13%, Disagree: 4%, Strongly Disagree: 1%	24% Strongly Agree + 58% Agree	High confidence in distinguishing data types; disagreement remains very low.
3	Well-informed about Indian data protection framework	Strongly Agree: 19%, Agree: 54%, Neutral: 18%, Disagree: 7%, Strongly Disagree: 2%	19% Strongly Agree + 54% Agree	Strong familiarity but neutrality and some disagreement show partial awareness gaps.
4	Specific NPD provisions needed	Strongly Agree: 43%, Agree: 39%, Neutral: 12%, Disagree:	43% Strongly Agree + 39% Agree	Clear consensus that dedicated NPD legislation is necessary.

		4%, Strongly Disagree: 2%		
5	Global uniform laws more effective	Strongly Agree: 26%, Agree: 46%, Neutral: 16%, Disagree: 10%, Strongly Disagree: 2%	26% Strongly Agree + 46% Agree	Majority support harmonised global rules; limited resistance.
6	Indian framework sufficient for personal data challenges	Strongly Agree: 8%, Agree: 11%, Neutral: 21%, Disagree: 46%, Strongly Disagree: 14%	8% Strongly Agree + 11% Agree	Very low confidence; majority express dissatisfaction with adequacy.
7	Indian provisions sufficient for NPD	Strongly Agree: 4%, Agree: 9%, Neutral: 24%, Disagree: 44%, Strongly Disagree: 19%	4% Strongly Agree + 9% Agree	Overwhelming disagreement; existing NPD governance seen as insufficient.
8	Confident applying Indian data laws in practice	Strongly Agree: 6%, Agree: 48%, Neutral: 35%, Disagree: 10%, Strongly Disagree: 0%	6% Strongly Agree + 48% Agree	Moderate confidence but high neutrality shows limited procedural experience.
9	Need specialised training for law enforcement	Strongly Agree: 65%, Agree: 27%, Neutral: 5%, Disagree: 2%, Strongly Disagree: 1%	65% Strongly Agree + 27% Agree	Almost unanimous support; clear recognition of enforcement gaps.
10	Knowledgeable about international data laws	Strongly Agree: 14%, Agree: 43%, Neutral: 23%, Disagree: 18%, Strongly Disagree: 2%	14% Strongly Agree + 43% Agree	Moderate knowledge; significant neutrality and disagreement indicate need for training.
11	Indian data laws require amendments	Strongly Agree: 27%, Agree: 58%, Neutral: 14%, Disagree: 2%	27% Strongly Agree + 58% Agree	Very strong consensus that existing laws must be updated.

		1%, Strongly Disagree: 0%		
12	Distinction between personal and NPD is clear	Strongly Agree: 4%, Agree: 19%, Neutral: 25%, Disagree: 48%, Strongly Disagree: 4%	4% Strongly Agree + 19% Agree	Majority disagree; indicates definitional ambiguity.
13	Distinct NPD regulations required	Strongly Agree: 28%, Agree: 46%, Neutral: 21%, Disagree: 4%, Strongly Disagree: 1%	28% Strongly Agree + 46% Agree	Strong endorsement for a standalone NPD regulatory regime.
14	Legal community adequately informed about NPD	Strongly Agree: 6%, Agree: 9%, Neutral: 18%, Disagree: 57%, Strongly Disagree: 10%	6% Strongly Agree + 9% Agree	Very low awareness across legal professionals.
15	National frameworks sufficient for NPD	Strongly Agree: 3%, Agree: 18%, Neutral: 18%, Disagree: 41%, Strongly Disagree: 20%	3% Strongly Agree + 18% Agree	Respondents largely view current frameworks as inadequate.
16	Need collaboration between law enforcement and cyber experts	Strongly Agree: 57%, Agree: 30%, Neutral: 9%, Disagree: 4%, Strongly Disagree: 0%	57% Strongly Agree + 30% Agree	Extremely strong support for integrated governance.
17	International frameworks improve effectiveness	Strongly Agree: 41%, Agree: 34%, Neutral: 21%, Disagree: 3%, Strongly Disagree: 1%	41% Strongly Agree + 34% Agree	Strong preference for aligning with global standards.
18	Encountered cases of data misuse/breach	Yes: 54%, No: 46%	54% Yes	Majority have dealt with misuse cases, indicating prevalence in practice.

19	Pursued legal action in such cases	Yes: 20%, No: 80%	20% Yes	Very few pursue action; indicates procedural and institutional barriers.
20	Inaction due to legal inadequacies	Yes: 54%, No: 46%	54% Yes	Over half attribute inaction to unclear or insufficient laws.

7.4 Law Students

7.4.1 Descriptive Statistics and Interpretation

This section presents and interprets the responses of 100 law students on their understanding, perception, and preparedness regarding data governance—specifically personal and non-personal data. The results reflect academic awareness, conceptual clarity, and readiness to engage with data protection issues in their future professional practice.

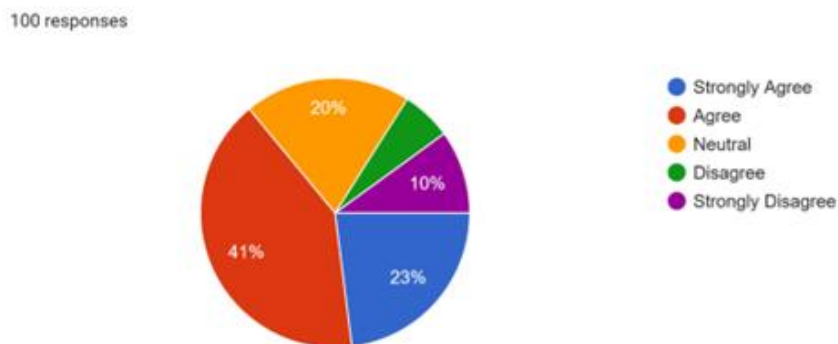


Figure 7.4.1: Understanding of Data Concepts

Question: I possess a comprehensive understanding of the concept of data, including personal and non-personal data.

Responses: 23 “percent strongly agreed”, 41 “percent agreed”, 20 “percent were neutral”, 6 “percent disagreed”, and 10 “percent strongly disagreed”.

Interpretation:

A total of 64 percent of law students affirm a comprehensive understanding of data

concepts. However, the 20 percent neutral and 16 percent disagreement responses reveal that conceptual understanding is not yet uniform, indicating that the study of data and its classifications require deeper integration into law curricula.

100 responses

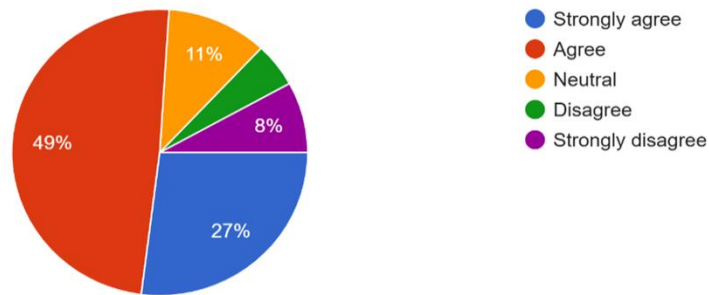


Figure 7.4.2: Distinguishing Between Personal and Non-Personal Data

Question: I am capable of clearly distinguishing between personal data and non-personal data.

Responses: 27 “percent strongly agreed”, 49 “percent agreed”, 11 “percent were neutral”, 5 “percent disagreed”, and 8 “percent strongly disagreed”.

Interpretation:

A strong 76 percent agreement demonstrates satisfactory awareness among law students in distinguishing between data categories. However, 16 percent dissent and 11 percent neutrality highlight the need for clearer pedagogical emphasis on anonymization, pseudonymization, and data re-identification standards.

100 responses

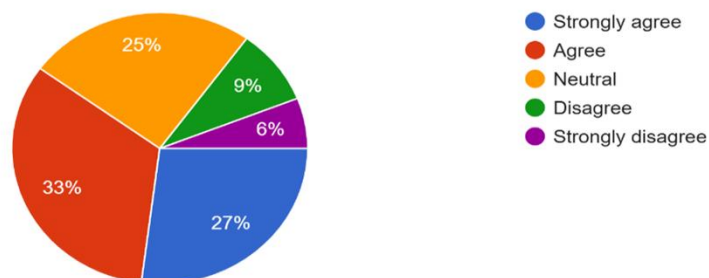


Figure 7.4.3: Awareness of the Indian Legal Framework

Question: I am well-informed about the existing Indian legal framework governing data protection.

Responses: 27 “percent strongly agreed”, 33 “percent agreed”, 25 “percent were neutral”, 9 “percent disagreed”, and 6 “percent strongly disagreed”.

Interpretation:

A cumulative 60 percent of law students reported awareness of the Indian legal framework, notably the Digital Personal Data Protection Act, 2023. The 25 percent neutrality suggests that while awareness exists, depth of understanding and application-based knowledge remain limited, warranting increased academic exposure.

100 responses

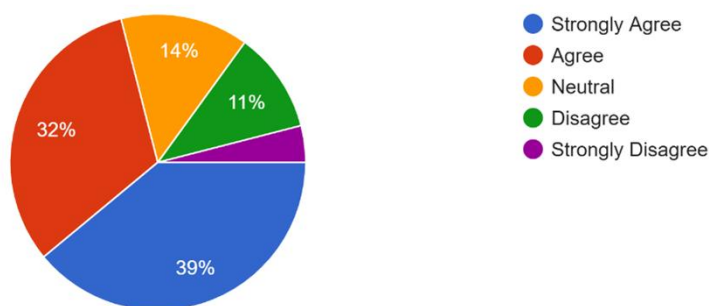


Figure 7.4.4: Need for Legal Provisions on Non-Personal Data

Question: In my view, the formulation of specific legal provisions for Non-Personal Data is necessary.

Responses: 39 “percent strongly agreed”, 32 “percent agreed”, 14 “percent were neutral”, 11 “percent disagreed”, and 4 “percent strongly disagreed”.

Interpretation:

An overwhelming 71 percent of respondents endorse the need for a specialized legal framework governing non-personal data. This consensus reflects growing academic awareness of the limitations of existing laws that primarily focus on personal data protection.

100 responses

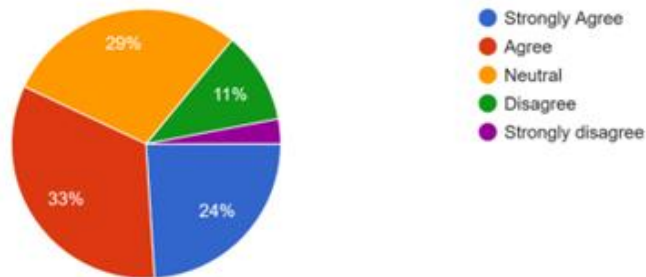


Figure 7.4.5: Preference for Global Uniform Laws

Question: I consider global uniform data protection laws to be more effective than national laws in addressing data-related challenges.

Responses: 24 “percent strongly agreed”, 33 “percent agreed”, 29 “percent were neutral”, 11 “percent disagreed”, and 3 “percent strongly disagreed”.

Interpretation:

A majority (57 percent) favor globally harmonized data protection standards, while 29 percent remain neutral. The trend indicates students’ recognition of international regulatory influence, though a considerable neutral group reflects uncertainty about the practical implementation of global uniformity.

100 responses

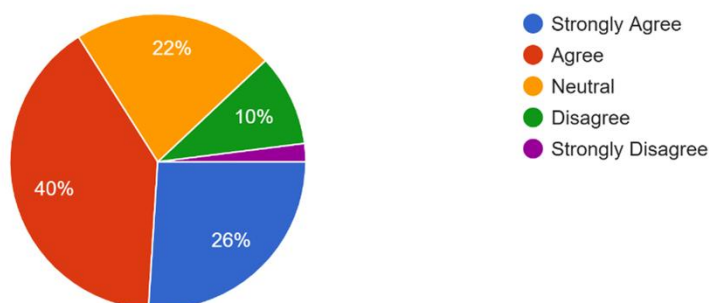


Figure 7.4.6: Inclusion of Non-Personal Data in Legal Education

Question: I believe legal education should include a more comprehensive study of Non-Personal Data laws.

Responses: 26 “percent strongly agreed”, 40 “percent agreed”, 22 “percent were neutral”, 10 “percent disagreed”, and 2 “percent strongly disagreed”.

Interpretation:

A strong 66 percent consensus supports the integration of *Non-Personal Data* law into legal education. The data suggests that students recognize the academic gap and advocate curricular inclusion to ensure readiness for data-centric legal practice.

100 responses

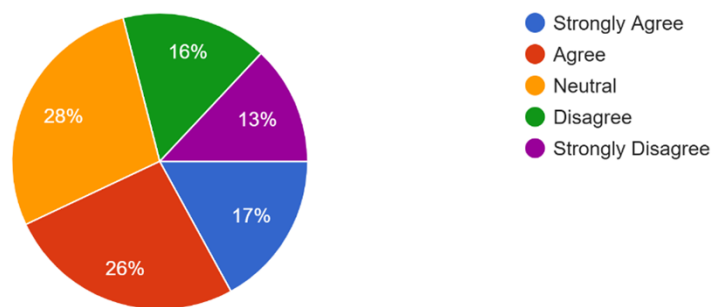


Figure 7.4.7: Confidence in Indian Legislation Regulating Non-Personal Data

Question: I am confident that Indian legislation adequately regulates Non-Personal Data usage.

Responses: 17 “percent strongly agreed”, 26 “percent agreed”, 28 “percent were neutral”, 16 “percent disagreed”, and 13 “percent strongly disagreed”.

Interpretation:

Only 43 percent express confidence in India’s regulatory adequacy for non-personal data, while 29 percent disagree and 28 percent remain neutral. The responses reveal skepticism regarding existing provisions, underscoring perceived legislative insufficiency and the need for a dedicated statutory framework.

100 responses

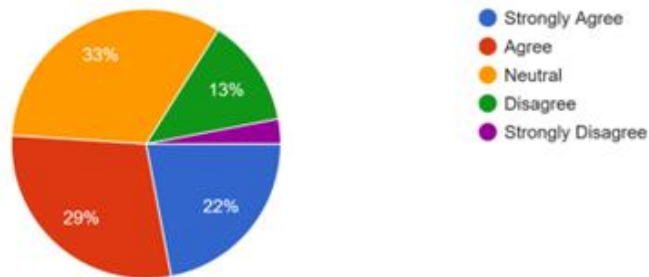


Figure 7.4.8: Effectiveness of Global Regulations

Question: I perceive global regulations, such as the GDPR, to be more effective than Indian data protection laws.

Responses: 22 “percent strongly agreed”, 29 “percent agreed”, 33 “percent were neutral”, 13 “percent disagreed”, and 3 “percent strongly disagreed”.

Interpretation:

A total of 51 percent view global frameworks like GDPR as more effective than domestic laws, whereas 33 percent neutrality implies limited familiarity with comparative legal standards. This demonstrates that global awareness among students exists but lacks depth in analytical comparison.

100 responses

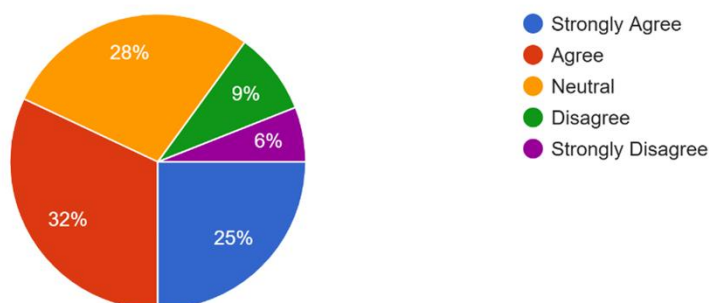


Figure 7.4.9: Awareness of Data Protection Law Implications

Question: I am aware of the implications of data protection laws on future legal practices.

Responses: 25 “percent strongly agreed”, 32 “percent agreed”, 28 “percent were neutral”, 9 “percent disagreed”, and 6 “percent strongly disagreed”.

Interpretation:

A combined 57 percent of law students acknowledge awareness of how data laws influence future practice. The 28 percent neutral group, however, signals that experiential and case-based exposure remains insufficient, pointing to a theoretical rather than practical understanding.

100 responses

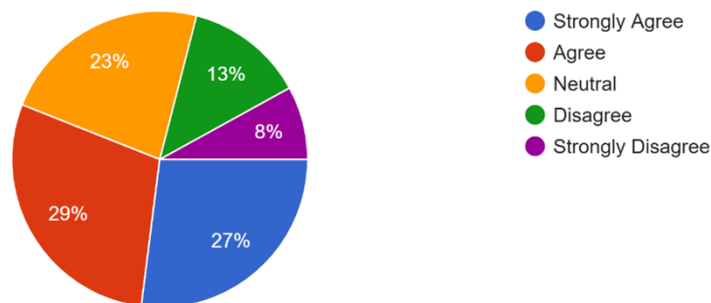


Figure 7.4.10: Preparedness for Data Privacy Cases

Question: I feel adequately prepared to address legal cases involving data privacy in my future legal career.

Responses: 27 “percent strongly agreed”, 29 “percent agreed”, 23 “percent were neutral”, 13 “percent disagreed”, and 8 “percent strongly disagreed”.

Interpretation:

While 56 percent feel prepared to handle data privacy cases, 23 percent neutrality and 21 percent disagreement indicate moderate preparedness levels. This suggests that professional readiness remains constrained by limited experiential exposure and practical legal training in data privacy litigation.

100 responses

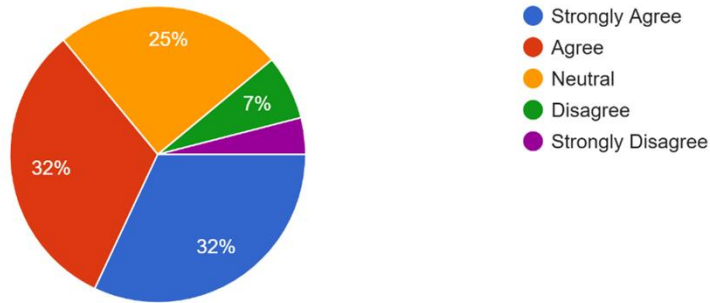


Figure 7.4.11: Legal Regulation of Non-Personal Data

Question: I believe Non-Personal Data should be subject to specific legal regulations.

Responses: 32 “percent strongly agreed”, 32 “percent agreed”, 25 “percent were neutral”, 7 “percent disagreed”, and 4 “percent strongly disagreed”.

Interpretation:

A significant 64 percent of law students believe *Non-Personal Data* requires its own legal regulation, reflecting a growing recognition that anonymized and aggregated data should not remain outside formal governance. The 25 percent neutral responses highlight the need for enhanced academic engagement with emerging policy debates on *Non-Personal Data* frameworks.

100 responses

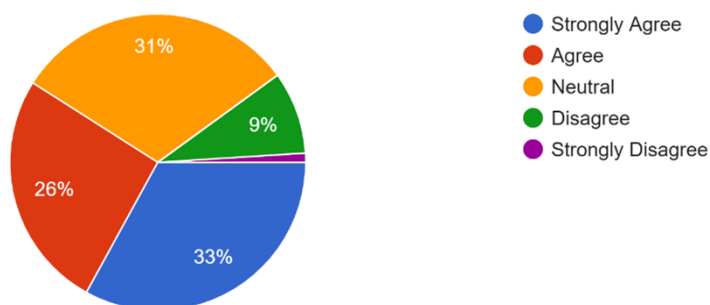


Figure 7.4.12: Inclusion of Specialized Courses on NPD Laws

Question: Specialized courses on Non-Personal Data laws should be incorporated into law school curricula.

Responses: 33 “percent strongly agreed”, 26 “percent agreed”, 31 “percent were neutral”, 9 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

A total of 59 percent of respondents favor incorporating specialized *NPD* law courses into legal curricula. However, 31 percent neutral responses suggest that while awareness exists, students lack clarity on how these topics can be practically structured or assessed within traditional legal education.

100 responses

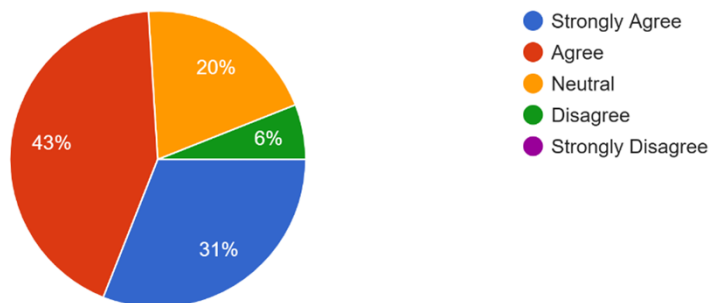


Figure 7.4.13: Awareness Needs Among Legal Practitioners

Question: I believe legal practitioners require enhanced awareness regarding Non-Personal Data governance.

Responses: 31 “percent strongly agreed”, 43 “percent agreed”, 20 “percent were neutral”, and 6 “percent disagreed”.

Interpretation:

An overwhelming 74 percent agree that existing practitioners lack adequate understanding of *NPD* governance. This consensus demonstrates that law students perceive a professional knowledge gap that academia must help bridge through targeted teaching and continuing legal education.

100 responses

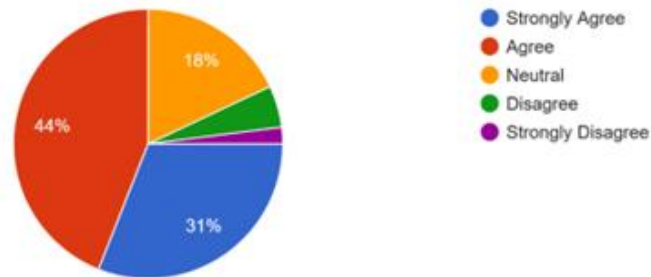


Figure 7.4.14: Separate Legal Framework for Non-Personal Data

Question: Non-Personal Data should be regulated under a distinct legal framework separate from personal data.

Responses: 31 “percent strongly agreed”, 44 “percent agreed”, 18 “percent were neutral”, 5 “percent disagreed”, and 2 “percent strongly disagreed”.

Interpretation:

A total of 75 percent of students supports a distinct legal regime for non-personal data. This indicates a maturing conceptual awareness that personal data and *Non-Personal Data* require differentiated treatment to address issues like data value extraction and anonymization integrity.

100 responses

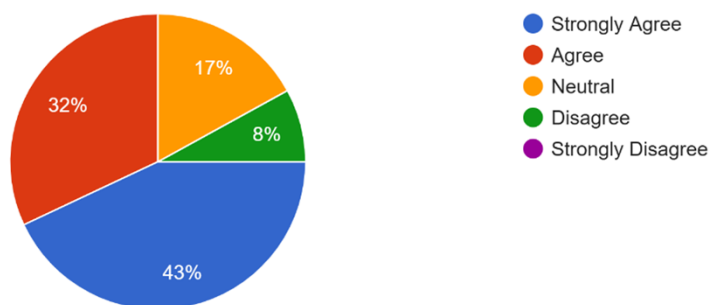


Figure 7.4.15: Awareness of Privacy as a Fundamental Right

Question: I understand that personal privacy is a fundamental right under Indian law.

Responses: 43 “percent strongly agreed”, 32 “percent agreed”, 17 “percent were neutral”, and 8 “percent disagreed”.

Interpretation:

A strong 75 percent of respondents correctly identify privacy as a constitutionally recognized right under *Justice K.S. Puttaswamy v. Union of India (2017)*. This suggests that core constitutional awareness is well integrated into legal education, though 17 percent neutrality implies incomplete comprehension of its broader implications for data protection.

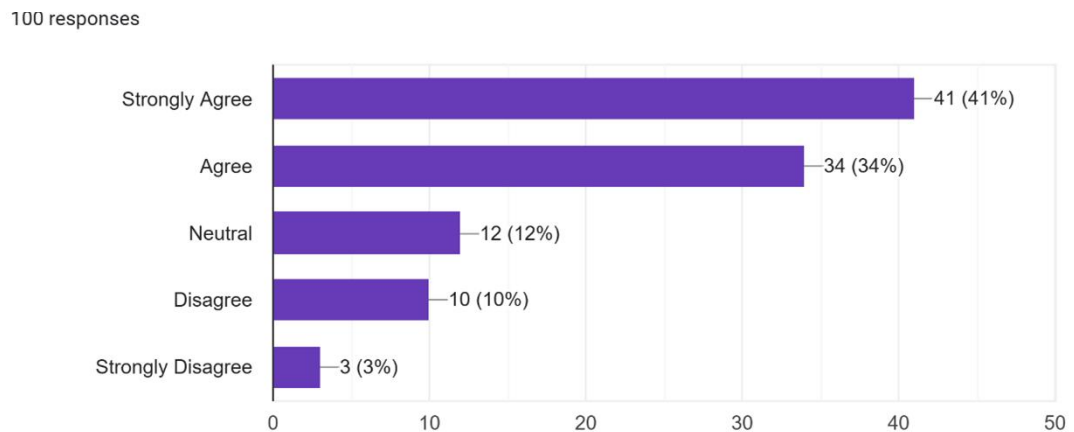


Figure 7.4.16: Data Privacy as a Future Legal Concern

Question: I believe data privacy will be one of the major legal issues in the future.

Responses: 41 “percent strongly agreed”, 34 “percent agreed”, 12 “percent were neutral”, 10 “percent disagreed”, and 3 “percent strongly disagreed”.

Interpretation:

An overwhelming 75 percent foresee data privacy as a dominant legal challenge of the future. The finding underscores an evolving perception among young scholars that digital transformation will significantly reshape the scope of civil liberties and regulatory jurisprudence.

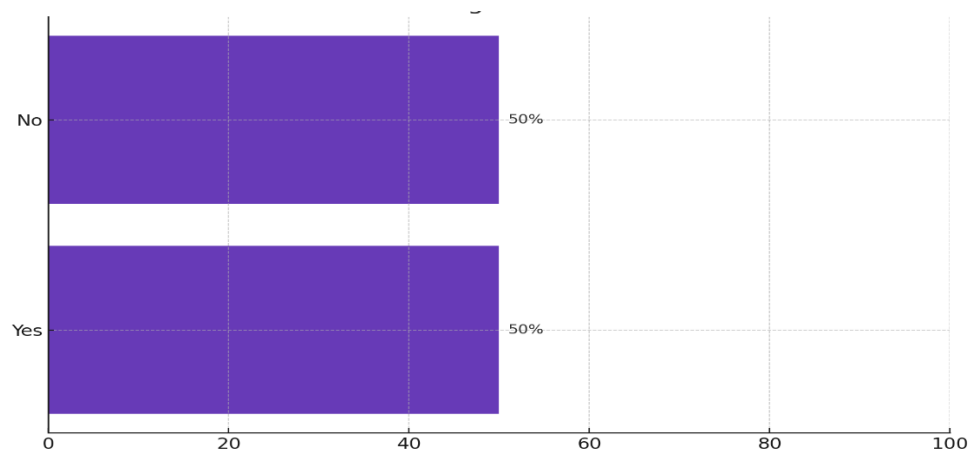


Figure 7.4.17: Exposure to Data Protection Laws in Curriculum

Question: Have you studied data protection and privacy laws as part of your curriculum?

Responses: 50 percent Yes, 50 percent No.

Interpretation:

The nearly even split (50:50) indicates inconsistency in how law schools across India incorporate data protection topics. This demonstrates a lack of curricular standardization, with some institutions offering electives on technology law while others continue with traditional doctrinal courses.

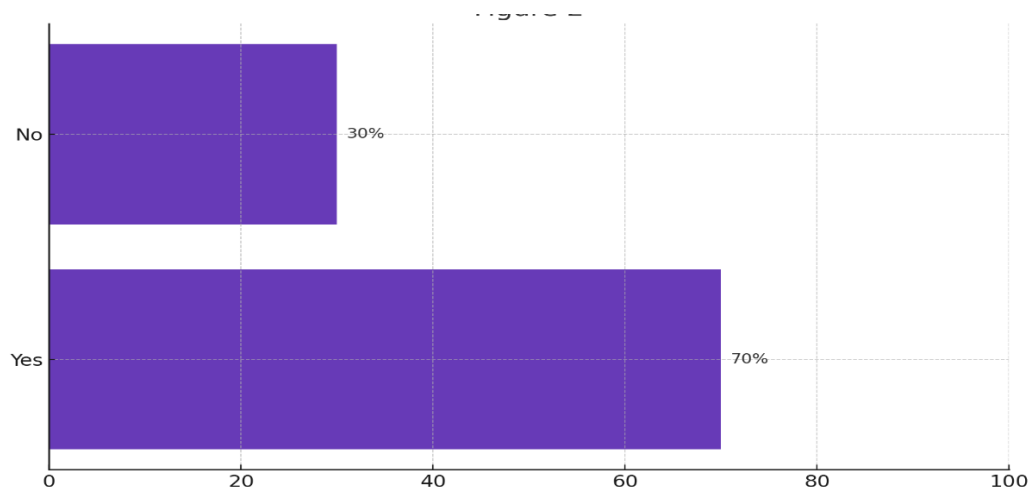


Figure 7.4.18: Familiarity with Legal Distinction Between Data Types

Question: Are you familiar with the legal distinction between personal and non-personal data?

Responses: 70 percent Yes, 30 percent No.

Interpretation:

A solid 70 percent confirm familiarity with the legal distinction, revealing positive exposure to emerging data law concepts. Yet the 30 percent unaware segment points to unequal access to specialized knowledge or institutional emphasis within academic programs.

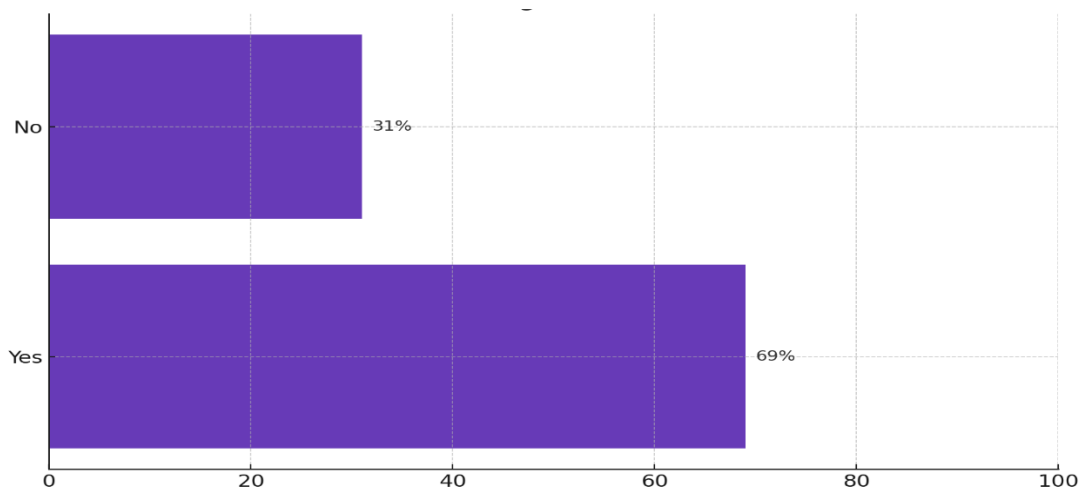


Figure 7.4.19: Awareness of Legal Remedies for Privacy Breaches

Question: Do you know the legal remedies available for breaches of personal privacy?

Responses: 69 percent Yes, 31 percent No.

Interpretation:

The 69 percent awareness level is encouraging, suggesting that law students are informed of available remedies under constitutional and statutory law. However, 31 percent lack awareness, reflecting that procedural remedies under new frameworks like the DPDP Act, 2023, are not yet fully integrated into legal pedagogy.

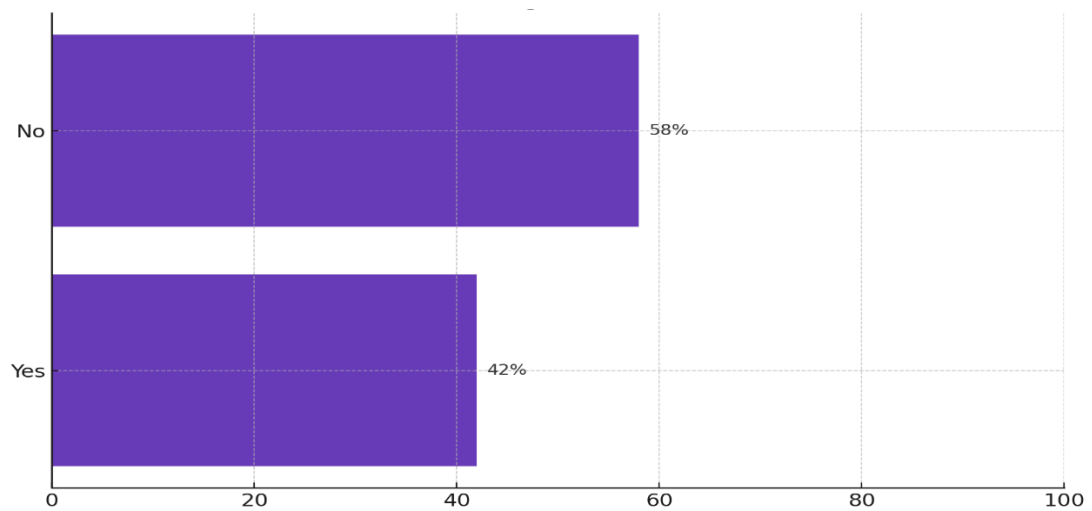


Figure 7.4.20: Confidence in Guiding Data Privacy Complaints

Question: Are you confident in guiding individuals on how to file complaints related to data misuse or privacy violations?

Responses: 42 percent Yes, 58 percent No.

Interpretation:

Despite theoretical understanding, only 42 percent express confidence in guiding others on complaint mechanisms. The majority (58 percent) admit lack of procedural familiarity, underscoring a gap between legal knowledge and applied competence, highlighting the need for clinical and practical exposure to cyber and data law mechanisms.

7.4.3 Summary of Key Findings

The analysis of responses from law students reveals a generation of future legal professionals who possess considerable conceptual awareness of data protection yet remain inadequately equipped with the applied knowledge required to navigate the evolving digital regulatory landscape. The findings indicate that while students conceptually recognize the need for legal frameworks governing personal and non-personal data, there exists a significant pedagogical gap between academic exposure and procedural readiness.

A substantial proportion of respondents, 64 percent, reported a comprehensive understanding of data concepts encompassing both personal and non-personal dimensions. However, nearly 36 percent either expressed uncertainty or disagreement, suggesting that while foundational awareness is prevalent, comprehension of complex data classifications such as anonymized, pseudonymized, or aggregated data remains limited. Similarly, 76 percent claimed the ability to distinguish between personal and non-personal data, yet the persistence of 16 percent disagreement and 11 percent neutrality underscores a need for more structured instruction on definitional and operational distinctions as codified under the Digital Personal Data Protection Act, 2023 (DPDP Act).

Awareness of the Indian data protection framework is moderate, with 60 percent of students reporting familiarity, while 40 percent either remain uncertain or uninformed. This uneven distribution signifies that the DPDP Act and its jurisprudential context have yet to achieve full curricular penetration within Indian legal education. The pattern further suggests a disparity between awareness of broad legislative intent and understanding of its procedural or institutional mechanisms.

In terms of normative perception, the demand for specialized legislation on *Non-Personal Data* governance was overwhelmingly supported, with 71 percent endorsing distinct provisions and another 75 percent favoring the creation of a separate legal framework for such data. These results reveal that law students conceptually recognize *Non-Personal Data* as a unique legal category requiring independent regulatory treatment. Correspondingly, 64 “percent agreed” that *Non-Personal Data* should be subject to specific statutory controls, reflecting alignment with international best practices advocating differential governance based on identifiability and economic use of data.

When evaluating global versus national perspectives, 57 percent considered global uniform data protection laws more effective than national legislation, and 51 percent perceived frameworks such as the *General Data Protection Regulation (GDPR)* to be superior to India’s evolving model. Nonetheless, a sizeable neutral group (29-33 percent) indicates an absence of deep comparative understanding, suggesting that

international legal dimensions of data governance remain under-represented in current law curricula.

The educational component of the survey exposes a critical developmental insight. Only 50 percent of respondents confirmed having studied data protection and privacy law as part of their formal curriculum, while 51 percent had not. Moreover, 59 percent advocated for specialized courses on *Non-Personal Data* law, and 66 percent believed that legal education should provide a more comprehensive treatment of such subjects. These findings collectively signal that Indian law schools have yet to systematically integrate data law as a mainstream subject. The emphasis of students on curricular reform evidences their recognition of the growing relevance of technology law in future legal practice.

Students demonstrated a strong awareness of constitutional privacy rights, with 75 percent acknowledging personal privacy as a fundamental right under Article 21, following *Justice K.S. Puttaswamy v. Union of India* (2017). Similarly, 75 percent believed data privacy would constitute one of the major legal issues of the future, indicating awareness of shifting normative priorities in digital governance. However, when self-assessing preparedness for practical application, only 56 percent expressed confidence in handling data privacy matters in their professional careers. This discrepancy between theoretical knowledge and practical confidence highlights the necessity of integrating experiential learning through moot courts, legal aid clinics, and technology law internships.

Awareness of legal remedies for privacy breaches was relatively high (69 percent), yet only 42 percent felt capable of guiding individuals on complaint procedures. This divergence underscores an implementation-level knowledge gap. Students possess conceptual understanding of rights but lack exposure to procedural frameworks for enforcement, grievance redress, or administrative compliance under the DPDP Act.

Further, 74 percent of respondents perceived that current legal practitioners require enhanced awareness of *Non-Personal Data* governance. This observation from the academic community itself underscores the urgency for interdisciplinary continuing education programs. Law students recognize that the emerging field of data law

transcends conventional legal boundaries, demanding familiarity with cyber-forensics, data valuation, and cross-border jurisdictional complexities.

Collectively, the responses reveal a dual trend, intellectual receptivity and institutional insufficiency. Law students demonstrate progressive attitudes toward global integration, specialized regulation, and curricular modernization. Nonetheless, limited procedural literacy, unequal exposure, and absence of standardized pedagogy impede their transition from conceptual understanding to practical competence.

In conclusion, the law students' perspective highlights four critical imperatives for India's legal education and policy ecosystem:

1. **Curricular Integration:** Mandatory inclusion of data protection, privacy, and *Non-Personal Data* law within undergraduate and postgraduate syllabi.
2. **Capacity Building:** Establishment of specialized training, certification, and research centers on technology and data law.
3. **Comparative Orientation:** Systematic introduction of global data protection instruments to foster international comprehension.
4. **Practical Preparedness:** Creation of clinical learning opportunities and simulated legal exercises involving data privacy disputes.

These imperatives, if implemented, would bridge the academic-practical divide and enable future legal professionals to engage confidently with the complex, multidisciplinary realities of data governance in the digital age.

Table 7.4.1. Summary of Key Responses from Law Students on Awareness and Perceptions of Non-Personal Data

Statement Number	Statement (Shortened)	Raw Response Data	Key Metric (% Agreement/Yes)	Main Insight
1	Understanding of data concepts	23% Strongly Agreed, 41% Agreed, 20% Neutral, 6% Disagreed, 10%	23% Strongly Agree + 41% Agree	Majority indicate conceptual understanding, though not uniformly strong.

		Strongly Disagreed		
2	Distinguish personal vs non-personal data	27% Strongly Agreed, 49% Agreed, 11% Neutral, 5% Disagreed, 8% Strongly Disagreed	27% Strongly Agree + 49% Agree	Strong ability to differentiate data types.
3	Awareness of Indian legal framework	27% Strongly Agreed, 33% Agreed, 25% Neutral, 9% Disagreed, 6% Strongly Disagreed	27% Strongly Agree + 33% Agree	Moderate awareness of DPDP Act, but more legal depth needed.
4	Need for NPD legal provisions	39% Strongly Agreed, 32% Agreed, 14% Neutral, 11% Disagreed, 4% Strongly Disagreed	39% Strongly Agree + 32% Agree	Strong support for specific NPD legislation.
5	Global uniform data laws preferred	24% Strongly Agreed, 33% Agreed, 29% Neutral, 11% Disagreed, 3% Strongly Disagreed	24% Strongly Agree + 33% Agree	Positive view on harmonized global standards.
6	Include NPD in legal education	26% Strongly Agreed, 40% Agreed, 22% Neutral, 10% Disagreed, 2% Strongly Disagreed	26% Strongly Agree + 40% Agree	Strong academic demand for curriculum expansion on NPD.
7	Confidence in Indian NPD regulation	17% Strongly Agreed, 26% Agreed, 28% Neutral, 16% Disagreed, 13%	17% Strongly Agree + 26% Agree	Students show limited confidence in regulatory sufficiency.

		Strongly Disagreed		
8	GDPR/global laws more effective	22% Strongly Agreed, 29% Agreed, 33% Neutral, 13% Disagreed, 3% Strongly Disagreed	22% Strongly Agree + 29% Agree	Some believe global laws are stronger, but many remain unsure.
9	Data laws impact future legal practice	25% Strongly Agreed, 32% Agreed, 28% Neutral, 9% Disagreed, 6% Strongly Disagreed	25% Strongly Agree + 32% Agree	Reasonable awareness but practical exposure still needs strengthening.
10	Preparedness for data privacy cases	27% Strongly Agreed, 29% Agreed, 23% Neutral, 13% Disagreed, 8% Strongly Disagreed	27% Strongly Agree + 29% Agree	Over half feel prepared, but practical readiness remains moderate.
11	NPD requires specific regulations	32% Strongly Agreed, 32% Agreed, 25% Neutral, 7% Disagreed, 4% Strongly Disagreed	32% Strongly Agree + 32% Agree	Strong belief in need for a dedicated NPD regulatory structure.
12	Specialized NPD courses needed	33% Strongly Agreed, 26% Agreed, 31% Neutral, 9% Disagreed, 1% Strongly Disagreed	33% Strongly Agree + 26% Agree	Interest in specialization exists, though clarity is still evolving.
13	Practitioners need NPD awareness	31% Strongly Agreed, 43% Agreed, 20% Neutral, 6% Disagreed	31% Strongly Agree + 43% Agree	Students perceive significant knowledge gaps among legal practitioners.

14	Separate legal framework for NPD	31% Strongly Agreed, 44% Agreed, 18% Neutral, 5% Disagreed, 2% Strongly Disagreed	31% Strongly Agree + 44% Agree	Strong endorsement for distinct NPD governance.
15	Privacy is a fundamental right	43% Strongly Agreed, 32% Agreed, 17% Neutral, 8% Disagreed	43% Strongly Agree + 32% Agree	Strong constitutional awareness among students.
16	Data privacy is a major future legal issue	41% Strongly Agreed, 34% Agreed, 12% Neutral, 10% Disagreed, 3% Strongly Disagreed	41% Strongly Agree + 34% Agree	High expectation of data privacy dominating future legal discourse.
17	Studied data protection in curriculum	50% Yes, 50% No	50% Yes	Curriculum inclusion is inconsistent across institutions.
18	Familiar with legal distinction	70% Yes, 30% No	70% Yes	Most students understand distinction; remaining need exposure.
19	Aware of legal remedies for privacy breaches	69% Yes, 31% No	69% Yes	Solid awareness, though newer legal mechanisms need greater classroom focus.
20	Confidence in guiding privacy complaints	42% Yes, 58% No	42% Yes	Students lack procedural confidence; clinical training required.

7.5. Information Technology Professionals

7.5.1 Descriptive Statistics and Interpretation

This section presents and interprets the responses of 100 Information Technology professionals on their understanding, perception, and practical engagement with data governance, specifically concerning personal and non-personal data. The findings reflect a high degree of conceptual and operational familiarity with data protection issues, informed by professional exposure to data processing environments, compliance requirements, and technology-driven workflows. The responses further indicate strong support for clear regulatory frameworks, including the need for distinct legal treatment of non-personal data and global harmonization of data governance standards, highlighting the sector's critical role in shaping and implementing effective data protection mechanisms in India's evolving digital ecosystem.

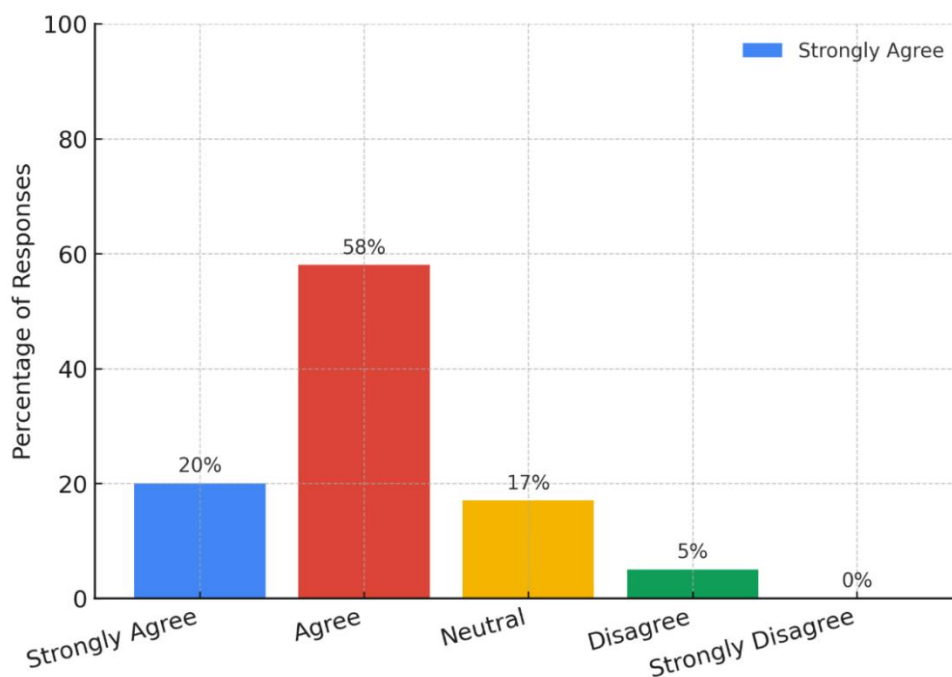


Figure 7.5.1: Understanding of the Concept of Data

Question: I possess a comprehensive understanding of the concept of data, including personal and non-personal data.

Responses: 20 “percent strongly agreed”, 58 “percent agreed”, 17 “percent were neutral”, and 5 “percent disagreed”.

Interpretation:

A majority of 78 percent of data professionals expressed confidence in their conceptual understanding of both personal and non-personal data. This indicates a strong foundational grasp among respondents working in technologically informed environments. The 17 percent neutral group likely represents individuals involved in managerial or non-technical data roles, suggesting a variation in domain familiarity across specializations.

100 responses

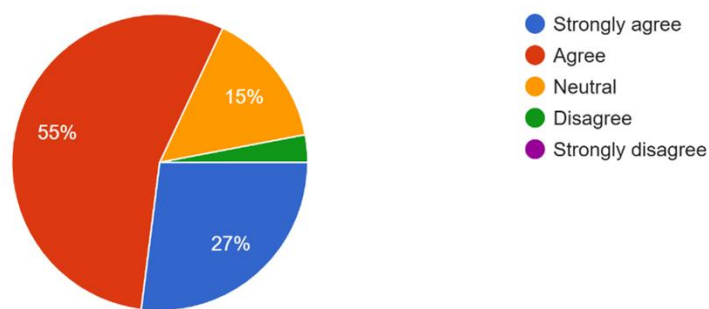


Figure 7.5.2: Ability to Distinguish Between Personal and Non-Personal Data

Question: I am capable of clearly distinguishing between personal data and non-personal data.

Responses: 27 “percent strongly agreed”, 55 “percent agreed”, 15 “percent were neutral”, and 3 “percent disagreed”.

Interpretation:

An overwhelming 82 percent demonstrated clarity in differentiating data types, indicating that professionals in the field are better positioned than other respondent groups to apply classification distinctions in operational or compliance contexts. However, the 15 percent neutrality still points to the necessity for standard institutional training on evolving definitions under India’s emerging data governance architecture.

100 responses

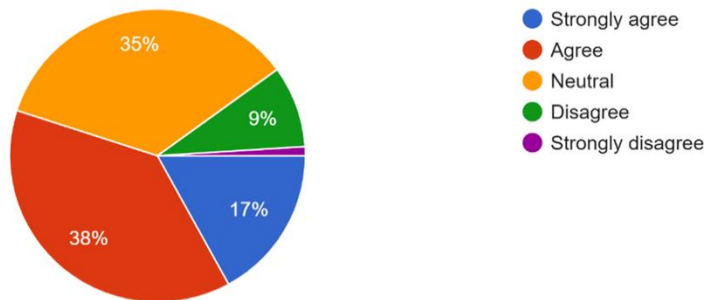


Figure 7.5.3: Awareness of Indian Data Protection Framework

Question: I am well-informed about the existing Indian legal framework governing data protection.

Responses: 17 “percent strongly agreed”, 38 “percent agreed”, 35 “percent were neutral”, 9 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

A cumulative 55 percent acknowledged awareness of India’s data protection laws, yet the 35 percent neutrality reflects a significant information gap. Despite working within the data ecosystem, many professionals lack legal literacy regarding compliance obligations under statutes such as the Digital Personal Data Protection Act, 2023 (DPDP Act). This underscores the need for structured intersectoral awareness initiatives.

100 responses

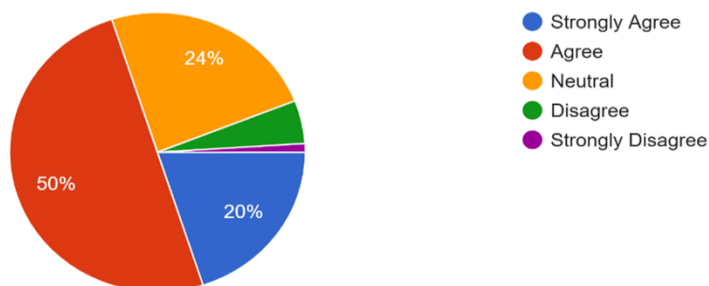


Figure 7.5.4: Necessity of Legal Provisions for Non-Personal Data

Question: In my view, the formulation of specific legal provisions for Non-Personal Data is necessary.

Responses: 20 “percent strongly agreed”, 50 “percent agreed”, 24 “percent were neutral”, 5 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

A combined 70 percent of respondents support the formulation of distinct legal provisions for non-personal data. This sentiment reflects practitioners’ recognition of the growing economic, ethical, and policy implications associated with data that is anonymized yet commercially valuable. The neutrality of 24 percent may arise from uncertainty regarding legislative feasibility or enforcement mechanisms.

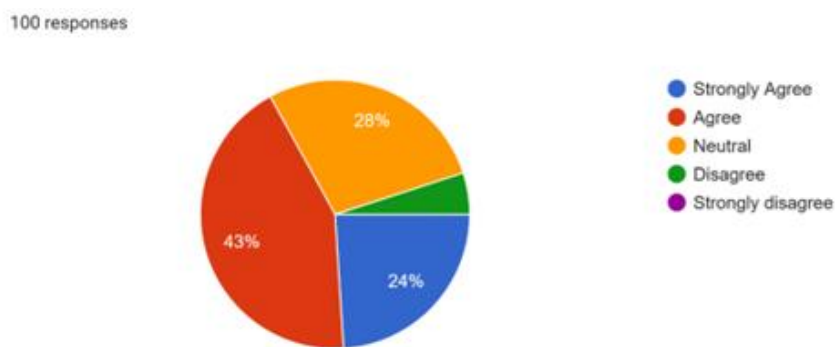


Figure 7.5.5: Preference for Global Uniform Data Protection Laws

Question: I consider global uniform data protection laws to be more effective than national laws in addressing data-related challenges.

Responses: 24 “percent strongly agreed”, 43 “percent agreed”, 28 “percent were neutral”, 4 “percent disagreed”, and 1 “percent strongly disagreed”.

Interpretation:

A substantial 67 percent endorsed the notion of harmonized global standards, demonstrating that professionals engaged with cross-border data handling recognize the inefficiencies of fragmented national frameworks. This mirrors international

advocacy for interoperability among data governance regimes, akin to the GDPR’s global influence.

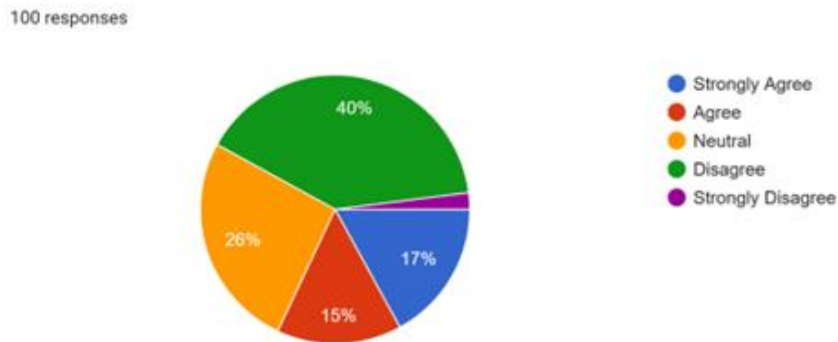


Figure 7.5.6: Adequacy of Indian Regulations for the Technology Sector

Question: I consider Indian regulations sufficient for governing Non-Personal Data usage within the technology sector:

Responses: 17 “percent strongly agreed”, 15 “percent agreed”, 26 “percent were neutral”, 40 “percent disagreed”, and 2 “percent strongly disagreed”.

Interpretation:

A majority 42 “percent disagreed”, reflecting skepticism among professionals regarding the adequacy of India’s existing legal structures to govern data beyond the personal sphere. The high neutral proportion (26 percent) suggests ongoing uncertainty as stakeholders await further clarity on implementation mechanisms for *Non-Personal Data* governance.

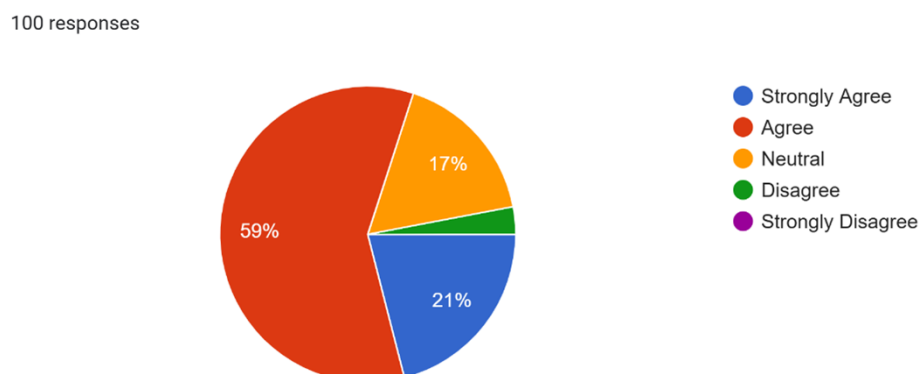


Figure 7.5.7: Distinct Legal Protections for Non-Personal Data

Question: Non-Personal Data requires distinct legal protections separate from personal data regulations.

Responses: 21 “percent strongly agreed”, 59 “percent agreed”, 17 “percent were neutral”, and 3 “percent disagreed”.

Interpretation:

A striking 80 percent support differentiation between legal frameworks for personal and non-personal data, indicating sectoral recognition of unique governance requirements such as anonymization, value extraction, and public interest access. The negligible disagreement reinforces consensus within the data industry about the insufficiency of a one-size-fits-all legal model.

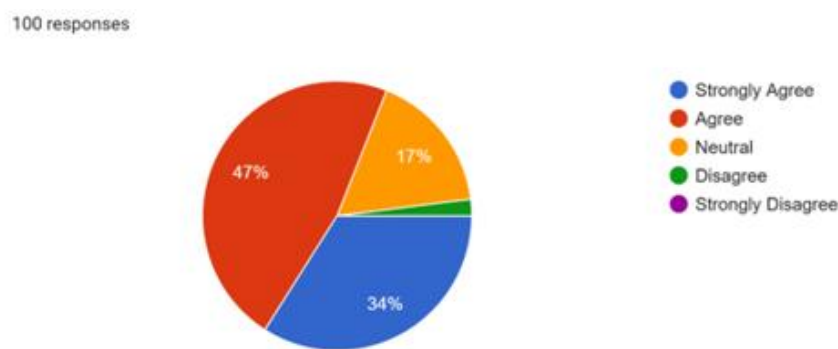


Figure 7.5.8: Need for Comprehensive Non-Personal Data Regulation in India

Question: There is a need for more comprehensive regulatory frameworks governing Non-Personal Data in India.

Responses: 34 “percent strongly agreed”, 47 “percent agreed”, 17 “percent were neutral”, and 2 “percent disagreed”.

Interpretation:

An overwhelming 81 percent agreement reflects that professionals actively perceive gaps in India’s current governance model. This reinforces the demand for a coherent, statutory framework to govern access, sharing, and monetization of non-personal datasets while ensuring privacy preservation and accountability.

100 responses

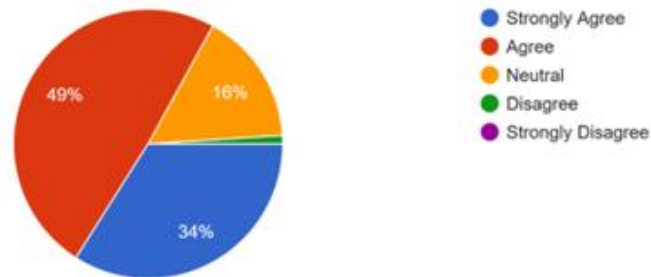


Figure 7.5.9: Importance of Global Standards for Non-Personal Data Governance

Question: Global standards for Non-Personal Data governance would enhance regulatory consistency and compliance.

Responses: 34 “percent strongly agreed”, 49 “percent agreed”, 16 “percent were neutral”, and 1 “percent disagreed”.

Interpretation:

A near-consensus (83 percent) view among data professionals emphasizes the need for globally harmonized governance models. This suggests that industry practitioners, especially those handling multinational data flows, see interoperability as a practical solution for achieving both compliance efficiency and trust assurance in data ecosystems.

100 responses

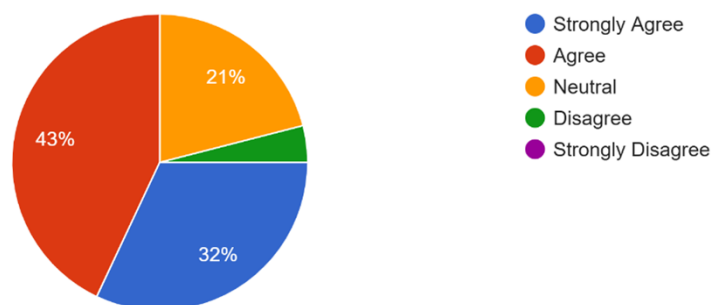


Figure 7.5.10: Legal Consideration for Economic Value of Non-Personal Data

Question: In my view, the economic value of Non-Personal Data warrants specific legal consideration.

Responses: 32 “percent strongly agreed”, 43 “percent agreed”, 21 “percent were neutral”, and 4 “percent disagreed”.

Interpretation:

With 75 percent agreement, data professionals widely recognize the economic dimension of *Non-Personal Data* as a driver of innovation and competition policy. Their perspective aligns with contemporary economic jurisprudence emphasizing that data, even when anonymized, constitutes a valuable non-rival asset deserving legal recognition in terms of ownership, access, and sharing frameworks.

100 responses

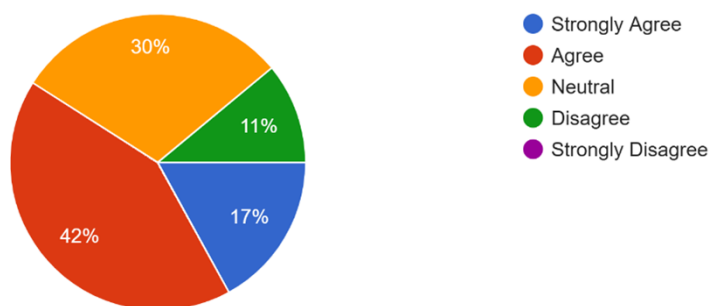


Figure 7.5.11: Impact of Indian Data Protection Laws on Professional Activities

Question: My professional activities are impacted by the clarity and limitations of Indian data protection laws.

Responses: 17 “percent strongly agreed”, 42 “percent agreed”, 30 “percent were neutral”, and 11 “percent disagreed”.

Interpretation:

A cumulative 59 percent of respondents acknowledged that the existing clarity and limitations within Indian data protection laws directly influence their professional responsibilities. This indicates that legal ambiguity around data regulation affects operational decisions and compliance strategies in the data industry. The 30 percent

neutrality suggests that certain professionals, particularly those in non-regulatory roles, may not experience these challenges as directly.

100 responses

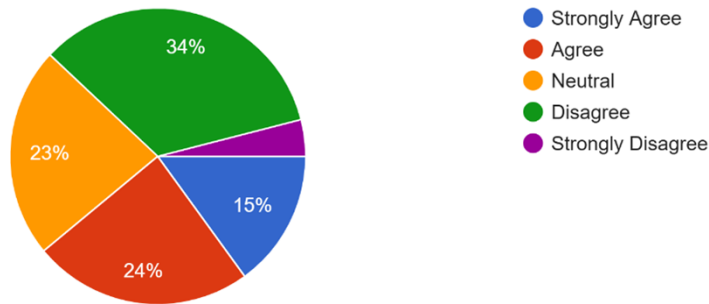


Figure 7.5.12: Effectiveness of Anonymization in Safeguarding Privacy

Question: Non-Personal Data can be anonymized effectively without infringing on individual privacy rights.

Responses: 15 “percent strongly agreed”, 24 “percent agreed”, 23 “percent were neutral”, 34 “percent disagreed”, and 4 “percent strongly disagreed”.

Interpretation:

A divided response emerged, with 39 percent expressing confidence in anonymization techniques, while 38 “percent disagreed” or strongly disagreed. This nearly equal split demonstrates ongoing uncertainty among professionals regarding the technical sufficiency of anonymization in guaranteeing privacy. The 23 percent neutral respondents indicate a cautious stance, reflecting awareness of potential re-identification risks inherent in large-scale data analytics.

100 responses

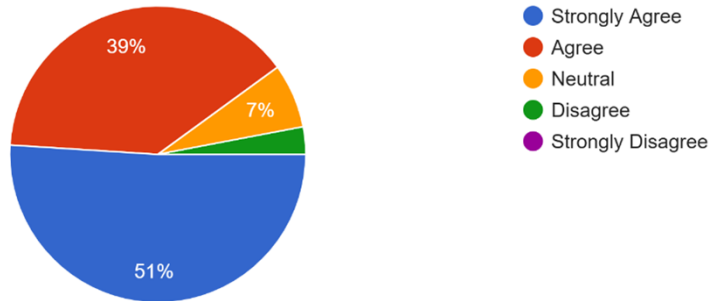


Figure 7.5.13: Advocacy for Transparent Government Data Policies

Question: I advocate for more transparent government policies on the usage of non-personal data.

Responses: 51 “percent strongly agreed”, 39 “percent agreed”, 7 “percent were neutral”, and 3 “percent disagreed”.

Interpretation:

An overwhelming 90 percent agreement underscores a collective call for policy transparency. Data professionals consistently emphasize the need for clarity in how the government collects, shares, and utilizes non-personal data. This sentiment aligns with global policy discourses stressing public accountability and open data principles as prerequisites for ethical data governance.

100 responses

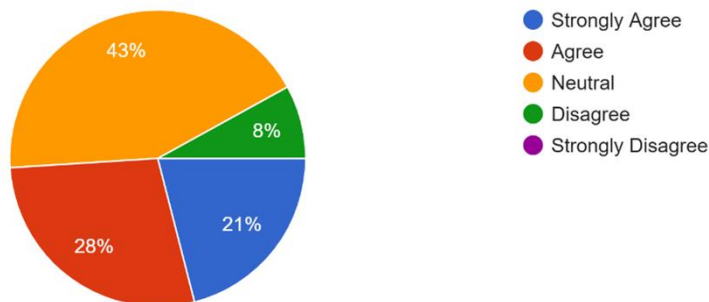


Figure 7.5.14: Adherence to International Data Protection Standards

Question: I follow international data protection laws, such as the GDPR, in my work.

Responses: 21 “percent strongly agreed”, 28 “percent agreed”, 43 “percent were neutral”, and 8 “percent disagreed”.

Interpretation:

A total of 49 percent of respondents indicated compliance with international frameworks such as the *General Data Protection Regulation (GDPR)*, suggesting that global standards inform corporate practices among Indian professionals. However, the 43 percent neutrality indicates that these frameworks are not uniformly integrated across sectors, particularly among domestic-oriented firms.

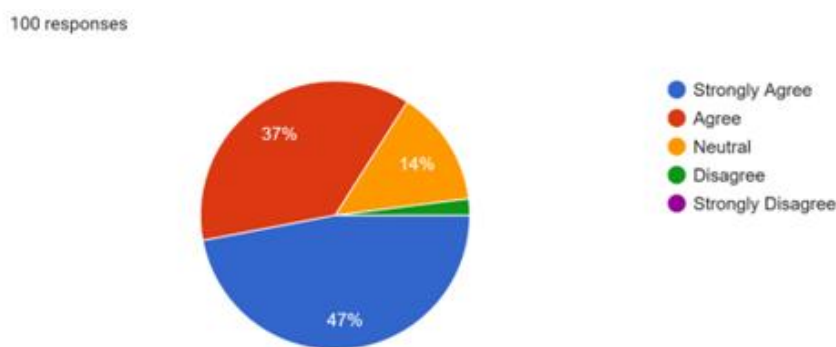


Figure 7.5.15: Influence of Fundamental Right to Privacy on Data Handling

Question: I believe personal privacy as a fundamental right should influence how companies handle personal and non-personal data.

Responses: 47 “percent strongly agreed”, 37 “percent agreed”, 14 “percent were neutral”, and 2 “percent disagreed”.

Interpretation:

A striking 84 percent agreement reflects that data professionals acknowledge constitutional privacy principles as a guiding standard for corporate data governance. This alignment with *Puttaswamy (2017)* reinforces the intersection between constitutional ethics and industry practice, indicating a maturing sense of legal responsibility within the data sector.

100 responses

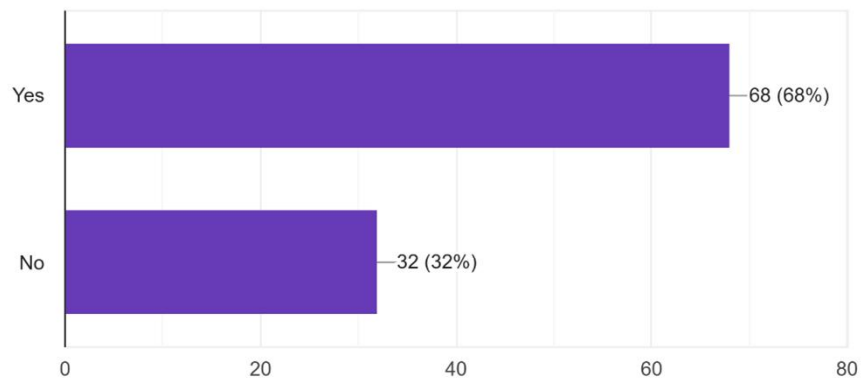


Figure 7.5.16: Engagement with Non-Personal Data at Work

Question: Do you work with Non-Personal Data as part of your professional role?

Responses: 68 percent responded “Yes” and 32 percent responded “No.”

Interpretation:

A majority of 68 percent of professionals actively handle *Non-Personal Data* in their workplace, confirming the centrality of such data in analytics, artificial intelligence, and product development. The 32 percent non-engagement may represent managerial or policy-level roles detached from direct data processing functions.

100 responses

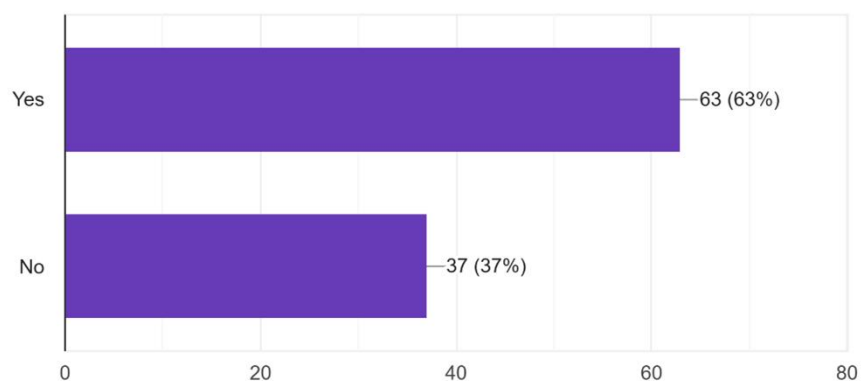


Figure 7.5.17: Familiarity with Indian Laws on Non-Personal Data

Question: Are you familiar with Indian laws governing the regulation of non-personal data?

Responses: 63 percent responded “Yes” and 37 percent responded “No.”

Interpretation:

A moderate 63 percent familiarity rate indicates a significant awareness gap within the professional community. Despite frequent interaction with non-personal datasets, more than one-third of respondents lack formal understanding of India’s legal position, reflecting the evolving and fragmented nature of current policy frameworks.

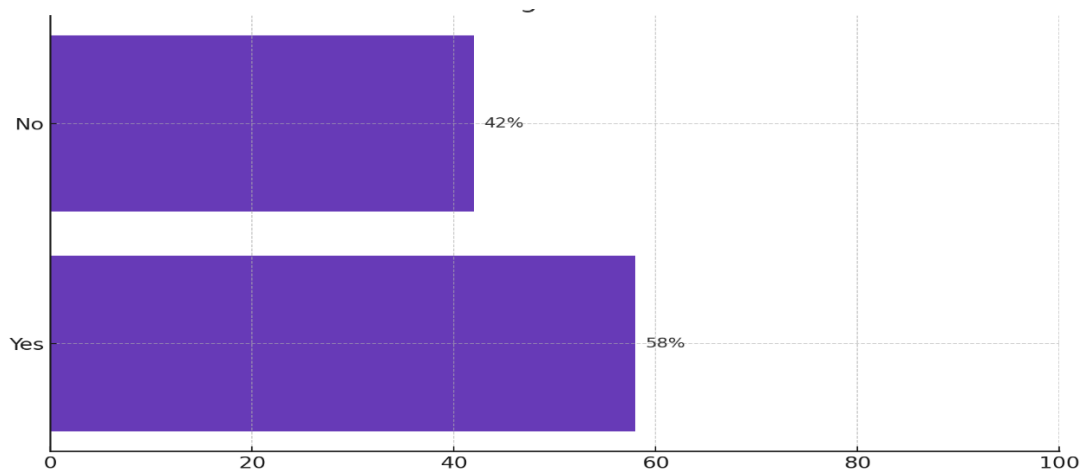


Figure 7.5.18: Challenges in Differentiating Data Types

Question: Have you encountered challenges in distinguishing between personal and non-personal data?

Responses: 58 percent responded “Yes” and 42 percent responded “No.”

Interpretation:

More than half (58 percent) of respondents reported difficulty in delineating personal from non-personal data. This finding reflects practical ambiguity in applying definitions to hybrid or inferred datasets, emphasizing the need for operational guidelines to supplement legislative definitions.

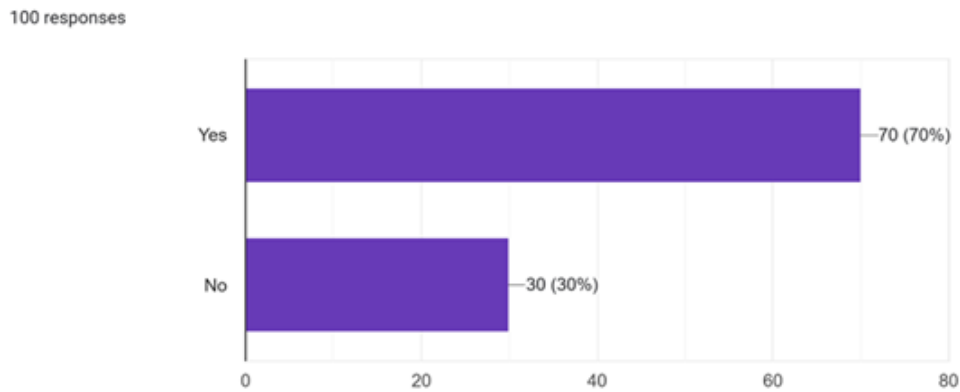


Figure 7.5.19: Experience of Privacy Breaches Due to Unclear Legal Regulations

Question: Have you experienced situations where personal data breaches occurred due to unclear legal regulations?

Responses: 70 percent responded “Yes” and 30 percent responded “No.”

Interpretation:

A concerning 70 percent of professionals have witnessed or encountered privacy breaches attributable to regulatory opacity. This highlights the pressing need for comprehensive enforcement mechanisms and institutional clarity in India’s data protection framework to prevent legal uncertainty from translating into operational vulnerability.

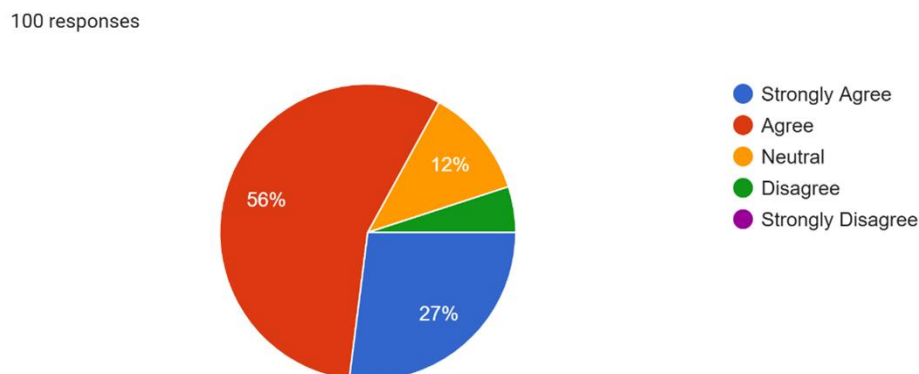


Figure 7.5.20: Support for Global Uniform Laws on Non-Personal Data

Question: I would support global uniform laws for the handling of non-personal data.

Responses: 27 “percent strongly agreed”, 56 “percent agreed”, 12 “percent were neutral”, and 5 “percent disagreed”.

Interpretation:

An overwhelming 83 percent support for international harmonization reflects professional consensus toward globally consistent standards for *Non-Personal Data* governance. This alignment with prior findings reinforces the view that cross-border coherence is vital for innovation, accountability, and trust in global digital economies.

7.5.2 Summary of Key Findings

The responses of data professionals present a nuanced understanding of *Non-Personal Data* governance grounded in practical experience, regulatory awareness, and operational challenges. The findings reveal four dominant themes: high conceptual literacy, strong advocacy for reform, recognition of regulatory insufficiencies, and preference for global harmonization.

A considerable majority (78 percent) indicated a sound conceptual understanding of data categories, and 82 percent demonstrated clarity in distinguishing personal from non-personal data. This confirms that professionals in the data ecosystem possess domain knowledge essential for operational compliance. Yet, 35 percent neutrality on awareness of India’s legal framework and 37 percent unfamiliarity with its provisions underline a critical gap between technical expertise and legal understanding.

Support for distinct governance of *Non-Personal Data* was consistent across questions, 70 percent endorsed separate legal provisions, 80 percent sought differentiated protection, and 81 percent favored comprehensive Indian regulation. Respondents also viewed the economic value of *Non-Personal Data* (75 percent) as warranting legal attention, signifying their awareness of its role in innovation and competitive advantage.

From a policy standpoint, 90 percent demanded greater transparency in governmental data practices, while 59 percent admitted that the clarity and limitations of current laws directly impact their work. This indicates that professionals view regulatory

uncertainty not merely as a legal issue but as a practical impediment to data-driven operations.

Internationally, 83 percent supported global uniform laws and 67 percent viewed international frameworks as superior, reflecting the globalized nature of their professional environments. This convergence suggests that data professionals advocate interoperability and cross-border consistency in regulatory standards.

Despite strong ethical alignment, evident from 84 percent upholding privacy as a constitutional principle influencing corporate conduct, operational realities remain challenging. 58 percent faced difficulties in classifying data, and 70 percent observed privacy breaches linked to unclear legal mandates. These findings underscore that definitional ambiguity and weak enforcement continue to hinder effective compliance.

Overall, the responses illustrate that while Indian data professionals exhibit robust conceptual and ethical awareness, they face persistent structural and legislative obstacles. They strongly advocate for legislative reform, international alignment, and clearer implementation protocols to transform India's data governance ecosystem into one that is both innovation-friendly and legally robust.

Table 7.5.1. Summary of Key Responses from IT Professionals on Awareness and Perceptions of Non-Personal Data

Statement Number	Statement (Shortened)	Raw Response Data	Key Metric (% Agreement/Yes)	Main Insight
1	Understanding of data concepts	20% Strongly Agreed, 58% Agreed, 17% Neutral, 5% Disagreed	20% Strongly Agree + 58% Agree	Strong conceptual grasp of personal and non-personal data among IT professionals.
2	Distinguish personal vs non-personal data	27% Strongly Agreed, 55% Agreed, 15% Neutral, 3% Disagreed	27% Strongly Agree + 55% Agree	Very strong clarity on data categorization for operational and compliance settings.

3	Awareness of Indian data protection framework	17% Strongly Agreed, 38% Agreed, 35% Neutral, 9% Disagreed, 1% Strongly Disagreed	17% Strongly Agree + 38% Agree	Awareness exists but remains limited; legal literacy needs improvement.
4	Need for NPD legal provisions	20% Strongly Agreed, 50% Agreed, 24% Neutral, 5% Disagreed, 1% Strongly Disagreed	20% Strongly Agree + 50% Agree	Strong call for specific legislation on non-personal data.
5	Preference for global uniform laws	24% Strongly Agreed, 43% Agreed, 28% Neutral, 4% Disagreed, 1% Strongly Disagreed	24% Strongly Agree + 43% Agree	High support for international harmonization of data protection rules.
6	Indian regulations sufficient for NPD	17% Strongly Agreed, 15% Agreed, 26% Neutral, 40% Disagreed, 2% Strongly Disagreed	17% Strongly Agree + 15% Agree	Majority believe Indian NPD governance remains inadequate.
7	NPD requires distinct legal protections	21% Strongly Agreed, 59% Agreed, 17% Neutral, 3% Disagreed	21% Strongly Agree + 59% Agree	Very strong professional consensus on differentiated NPD legal treatment.
8	Need comprehensive NPD regulation in India	34% Strongly Agreed, 47% Agreed, 17% Neutral, 2% Disagreed	34% Strongly Agree + 47% Agree	Strong demand for a robust, structured NPD regulatory framework.
9	Importance of global NPD standards	34% Strongly Agreed, 49% Agreed, 16% Neutral, 1% Disagreed	34% Strongly Agree + 49% Agree	Consensus for global interoperability of NPD governance.

10	NPD has economic value needing legal consideration	32% Strongly Agreed, 43% Agreed, 21% Neutral, 4% Disagreed	32% Strongly Agree + 43% Agree	Broad recognition of NPD as a commercial asset requiring legal safeguards.
11	Indian data protection laws impact professional activity	17% Strongly Agreed, 42% Agreed, 30% Neutral, 11% Disagreed	17% Strongly Agree + 42% Agree	Data laws influence professional duties; neutrality reflects role variations.
12	Anonymization safeguards privacy effectively	15% Strongly Agreed, 24% Agreed, 23% Neutral, 34% Disagreed, 4% Strongly Disagreed	15% Strongly Agree + 24% Agree	Views divided; significant doubt around anonymity and re-identification risks.
13	Need transparent government NPD policies	51% Strongly Agreed, 39% Agreed, 7% Neutral, 3% Disagreed	51% Strongly Agree + 39% Agree	Extremely strong support for public transparency in government use of NPD.
14	Follow international data protection standards	21% Strongly Agreed, 28% Agreed, 43% Neutral, 8% Disagreed	21% Strongly Agree + 28% Agree	Nearly half align with GDPR-like standards; high neutrality limits uniform compliance.
15	Privacy as a fundamental right should guide data handling	47% Strongly Agreed, 37% Agreed, 14% Neutral, 2% Disagreed	47% Strongly Agree + 37% Agree	Strong constitutional rights awareness influencing ethical data governance.
16	Work involves NPD	68% Yes, 32% No	68% Yes	Majority actively process NPD, confirming relevance in IT workflows.
17	Familiar with Indian NPD laws	63% Yes, 37% No	63% Yes	Moderate familiarity; more legal capacity building is required.

18	Challenges in distinguishing data types	58% Yes, 42% No	58% Yes	Practical confusion exists, especially with derived or inferred datasets.
19	Privacy breaches due to unclear laws	70% Yes, 30% No	70% Yes	High incidence of regulatory ambiguity leading to privacy risks.
20	Support global uniform NPD laws	27% Strongly Agreed, 56% Agreed, 12% Neutral, 5% Disagreed	27% Strongly Agree + 56% Agree	IT professionals strongly endorse global NPD harmonization.

7.6 Key Comparative Findings

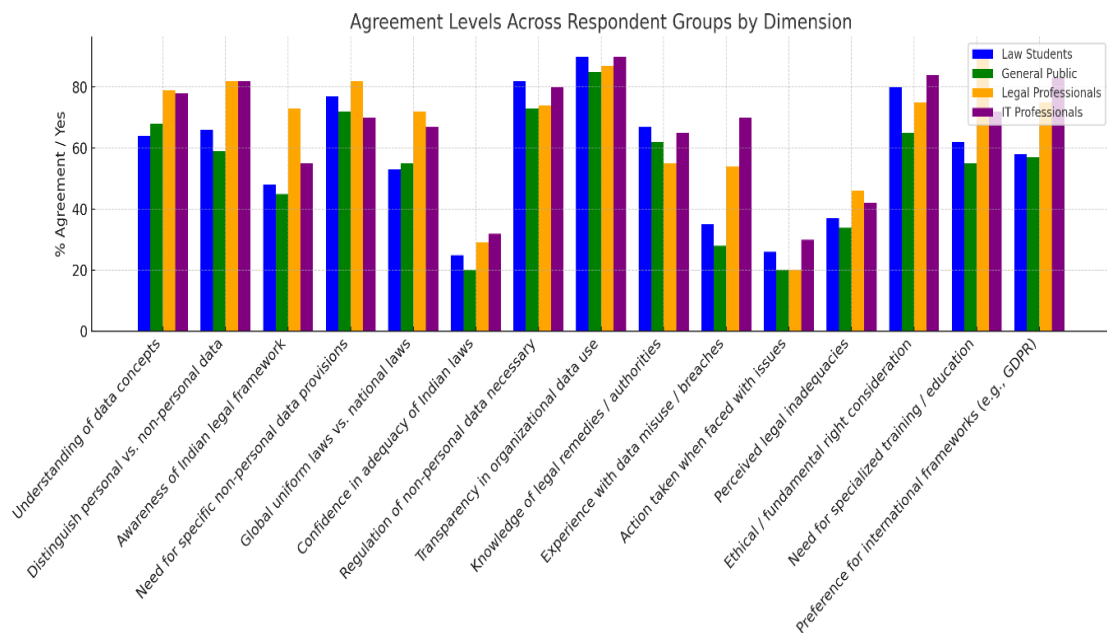


Figure 7.6.1. Comparative findings

Understanding and Awareness

Across the surveyed categories, legal and information technology professionals demonstrated the strongest grasp of data-related concepts and showed a clear ability to distinguish between personal and non-personal data. Their higher awareness may

be attributed to their direct professional engagement with laws, technologies, and compliance frameworks. Law students reflected a moderate level of confidence, suggesting that their knowledge remains primarily theoretical and classroom-based, with limited exposure to practical applications. In contrast, the general public displayed only partial understanding, with evident gaps in technical interpretation and awareness of legal distinctions. This indicates that while awareness of “data” as a general concept is spreading, the sophistication of that awareness remains uneven and profession-dependent.

Legal Adequacy and Regulation Needs

Respondents across all four categories expressed limited confidence in the adequacy of India’s existing legal framework governing personal and non-personal data. A majority emphasized that current regulations do not sufficiently address the evolving challenges posed by new forms of data use, aggregation, and monetization. This concern was most strongly voiced by legal professionals familiar with statutory limitations and enforcement bottlenecks. The consensus was that a distinct legal mechanism dedicated to *Non-Personal Data* is urgently required to bridge the governance gap. Additionally, participants highlighted the need for greater transparency within organizational data-handling practices, indicating that public accountability should be a central element of future regulatory reform.

Global Harmonization

Professionals, particularly those engaged in the technology sector, strongly supported the idea of international coordination in data governance. They noted that global harmonization would facilitate consistency, ensure smoother cross-border data exchanges, and prevent regulatory conflicts that could hinder innovation or compliance. Law students and members of the general public were relatively more neutral, expressing conditional support provided that such international alignment respects national interests, cultural priorities, and domestic constitutional principles. This difference in perception reflects an underlying tension between the practical benefits of international uniformity and the normative desire to retain local autonomy over digital governance.

Practical Exposure and Experience

Exposure to data misuse and security breaches varied across respondent groups. Information technology professionals reported the highest incidence of such encounters, given their proximity to operational systems and cybersecurity environments. Legal professionals followed, often through their advisory or litigation-related work. However, despite this exposure, the number of respondents who took remedial action after a breach remained consistently low. This inaction suggests that procedural complexities, limited awareness of enforcement options, and perceived inefficiency of grievance mechanisms discourage individuals from pursuing formal remedies. The pattern indicates that awareness of data issues alone does not ensure an active culture of redressal.

Training and Ethical Awareness

Both legal and information technology professionals emphasized the need for continuous, specialized training in data management, privacy standards, and regulatory compliance. Their responses reveal a shared understanding that data handling is not solely a technical process but also an ethical and legal responsibility. Ethical sensitivity and respect for privacy principles were particularly strong among respondents engaged in professional practice, likely due to their first-hand experience with the consequences of data misuse. Law students, while recognizing the importance of ethics, tended to perceive it within an academic rather than a practical framework. Overall, the findings highlight a growing awareness of the moral dimension of data governance, especially among professional groups.

Table 7.6.1 Consolidated Comparison Table (Common Questions Only)

This table compares only those questions that were identically asked across all four respondent groups. Here ‘SA’ means Strongly Agreed and ‘A’ means Agreed.

No .	Statement (Shortened)	General Public (Key Metric)	Law Students (Key Metric)	Legal Professionals (Key Metric)	IT Professionals (Key Metric)	Comparative Insight
1	Understanding of data concepts	15% SA + 53% A	23% SA + 41% A	24% SA + 55% A	20% SA + 58% A	Legal & IT respondents demonstrate the strongest conceptual clarity.
2	Distinguish personal vs NPD	16% SA + 50% A	27% SA + 49% A	24% SA + 58% A	27% SA + 55% A	Legal & IT groups show high capability in differentiating data types.
3	Awareness of Indian data protection framework	9% SA + 39% A	27% SA + 33% A	19% SA + 54% A	17% SA + 38% A	Legal professionals exhibit the highest awareness.
4	Need for specific NPD provisions	17% SA + 60% A	39% SA + 32% A	43% SA + 39% A	20% SA + 50% A	All groups strongly support dedicated NPD legislation.
5	Preference for global uniform laws	15% SA + 38% A	24% SA + 33% A	26% SA + 46% A	24% SA + 43% A	Legal & IT show the strongest support for global alignment.
6	Indian laws adequate for personal data	5% SA + 22% A	14% SA + 29% A	8% SA + 11% A	7% SA + 25% A	Confidence is extremely low across all groups.
7	India’s NPD regulation sufficient	5% SA + 17% A	17% SA + 26% A	4% SA + 9% A	17% SA + 15% A	Legal professionals are most

						critical of existing NPD regulation.
9	Need transparency from companies	32% SA + 56% A	59% SA + 37% A	65% SA + 27% A	51% SA + 39% A	Very strong agreement, led by legal professionals.
10	NPD should be legally protected	38% SA + 46% A	32% SA + 56% A	27% SA + 58% A	32% SA + 43% A	Strongest support from legal professionals.
11	Concern about organizational data use	36% SA + 45% A	31% SA + 43% A	41% SA + 34% A	47% SA + 39% A	High concern across all groups, especially IT.
12	Need uniform global laws	36% SA + 45% A	23% SA + 36% A	28% SA + 46% A	34% SA + 49% A	IT & legal professions show strong preference.
13	Support stricter national laws	32% SA + 51% A	33% SA + 42% A	27% SA + 58% A	51% SA + 39% A	Legal & IT show the highest support.
18	Know legal remedies for breaches	39% Yes	69% Yes	61% Yes	69% Yes	Highest levels among law students & IT professionals.
19	Know authorities for complaints	50% Yes	69% Yes	50% Yes	58% Yes	Law students are most informed.
20	Understand complaint process	40% Yes	42% Yes	20% Yes	70% Yes	IT strongest; legal professionals weakest in procedural knowledge.

Table 7.6.2: Group-Specific Questions (Non-Common Questions)

This table presents questions that were unique to one respondent group or were not uniformly asked across all four groups. These cannot be compared directly across categories. Here ‘SA’ means Strongly Agreed and ‘A’ means Agreed.

Group	Statement No.	Statement (Shortened)	Key Metric (SA + A / Yes)	Insight
General Public	14	Experienced data misuse	65% Yes	High exposure to privacy breaches.
	15	Took action after misuse	26% Yes	Very low follow-through after breaches.
	16	Inaction due to unclear laws	63% Yes	Legal ambiguity discourages action.
	17	Privacy is a fundamental right	73% Yes	High constitutional awareness.
Law Students	14	Separate legal framework for NPD	31% SA + 44% A	Strong preference for a distinct NPD regulatory regime.
	15	Privacy is a fundamental right	43% SA + 32% A	Strong constitutional understanding among students.
	16	Data privacy is a major future legal issue	41% SA + 34% A	Students recognize privacy as an emerging legal challenge.
	17	Studied data protection laws in curriculum	50% Yes	Curriculum exposure uneven across institutions.
Legal Professionals	14	Legal community adequately informed about NPD	6% SA + 9% A	Extremely low NPD awareness among practitioners.
	15	National frameworks sufficient for NPD	3% SA + 18% A	Broad dissatisfaction with existing frameworks.
	16	Need collaboration between law enforcement and cyber experts	57% SA + 30% A	Very strong support for coordinated governance.
	17	International frameworks improve effectiveness	41% SA + 34% A	Strong belief in the value of global alignment.

	18	Encountered data misuse cases	54% Yes	Many have seen real-world breach instances.
	19	Pursued legal action	20% Yes	Very few take action—indicates systemic barriers.
	20	Inaction due to legal inadequacies	54% Yes	Over half cite unclear or weak laws as the cause.
IT Professionals	14	Effectiveness of anonymization	15% SA + 24% A	Divided opinions; high concern about re-identification risks.
	15	Transparent government NPD policies needed	51% SA + 39% A	Strong call for policy transparency.
	16	Follow international standards (e.g., GDPR)	21% SA + 28% A	Half follow global standards; neutrality indicates inconsistency.
	17	Privacy as a fundamental right should shape data handling	47% SA + 37% A	IT professionals strongly recognize privacy as a guiding principle.
	18	Work involves NPD	68% Yes	Majority interact with NPD regularly.
	19	Familiar with Indian NPD laws	63% Yes	Reasonable familiarity, but gaps remain.
	20	Difficulty distinguishing PD / NPD	58% Yes	Many faces practical challenges with grey-zone datasets.

7.7. Key Findings of the Overall Analysis

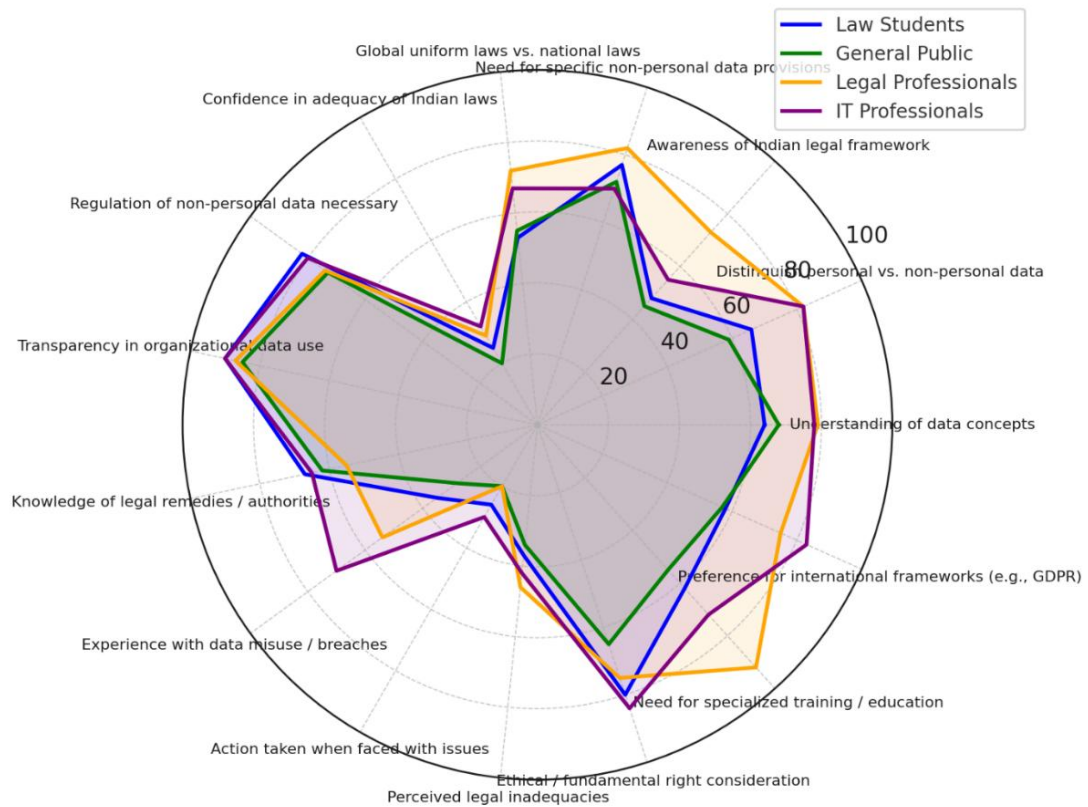


Figure 7.7.1. Key Findings of the Overall Analysis

Awareness and Understanding of Data Concepts

The overall findings show that awareness of data concepts is widespread across the population but differs in depth and precision. Legal and IT professionals displayed the highest confidence, with approximately seventy-eight percent confirming their ability to conceptualize and differentiate between personal and non-personal data. Their confidence can be attributed to their continuous engagement with applied settings such

as casework, compliance, and data analytics. Law students and the general public, though familiar with the idea of data, were more neutral in their responses, suggesting that their understanding remains general rather than analytical. This pattern illustrates a knowledge hierarchy where technical and legal experts possess substantive comprehension, while non-specialist groups retain a surface-level understanding shaped largely by exposure rather than expertise.

Awareness of the Indian Legal Framework

Awareness of the Indian legal system governing data protection varied sharply among the four groups. Legal professionals reported the highest familiarity, primarily due to their experience with the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. Their awareness extended to interpretative and procedural dimensions of these laws. IT professionals, while well-versed in the operational side of data, demonstrated only moderate awareness of legal provisions, revealing a disjunction between practice and legal knowledge. Law students and the general public displayed weaker awareness, ranging between forty-five and sixty percent, which indicates persistent gaps in both legal education and public outreach. The result reveals a systemic knowledge deficit where those most affected by data practices are often least informed about the laws meant to protect them.

Perceptions of Adequacy of Indian Laws

Confidence in the sufficiency of India's data protection regime remains uniformly low. Fewer than one-third of respondents across any group believed that existing laws provide adequate safeguards for either personal or non-personal data. Nearly half the respondents identified specific gaps in *Non-Personal Data* regulation. The Digital Personal Data Protection Act, 2023, while widely acknowledged as a progressive reform, is perceived as overly limited to personal data and insufficiently equipped to regulate anonymized or aggregated datasets. This consistent skepticism across diverse respondent groups reflects diminishing trust in the state's capacity to ensure comprehensive data governance.

Recognition of the Need for *Non-Personal Data* Regulation

A clear consensus emerged on the necessity for specialized regulation of non-personal data, with seventy to eighty-two percent supporting the establishment of a dedicated legal framework. Respondents noted that the absence of such legislation leaves *Non-Personal Data* vulnerable to re-identification, commercial exploitation, and cross-border misuse. Legal and IT professionals particularly emphasized the operational risks of anonymization and inadequate enforcement mechanisms, while law students and the general public highlighted ethical and social concerns. The responses collectively indicate a widely perceived regulatory vacuum that requires urgent legislative intervention.

Global Harmonization versus National Frameworks

Respondents were divided on whether India should prioritize global harmonization or strengthen national frameworks. Legal and IT professionals, whose work often involves cross-border transactions, favored global harmonization to align with international standards such as the General Data Protection Regulation of the European Union. Law students and the general public, however, displayed greater preference for context-specific national rules that preserve domestic autonomy. This divergence underscores the ongoing debate between universal standardization and contextual adaptability in data governance policymaking.

Transparency and Ethical Concerns

The demand for transparency emerged as nearly universal. More than eighty-five percent of respondents advocated stronger obligations for both government agencies and private organizations to disclose how they collect, use, and share data. Between seventy-five and eighty-four percent also favored embedding the constitutional right to privacy into broader data governance systems. This suggests a deep public and professional expectation that data management should be grounded in ethical accountability and respect for individual autonomy. The responses confirm that citizens and professionals alike view transparency as the foundation of trust in digital governance.

Practical Experience and Limited Remedial Action

Practical experience with data misuse was highest among information technology professionals at approximately seventy percent, followed by legal professionals at fifty-four percent. Law students and members of the general public reported fewer but still notable encounters. Despite these experiences, only about one-fifth to one-third pursued formal complaints or legal remedies. Commonly cited barriers included lack of awareness of available procedures, inefficiency of institutional redressal systems, and procedural delays. This discrepancy between rights awareness and enforcement behavior illustrates that mere recognition of privacy rights is insufficient without accessible and responsive mechanisms for redress.

Capacity-Building and Training Gaps

The need for capacity enhancement was a recurring theme. Legal professionals, at over ninety percent, stressed specialized training for judges, enforcement officers, and investigators. Law students nearly unanimously supported the inclusion of *Non-Personal Data* governance in legal curricula, recognizing that current academic programs focus excessively on personal data and privacy. IT professionals requested clearer regulatory guidance to synchronize technical practice with legal compliance, while the general public called for widespread legal literacy campaigns. The collective insight demonstrates that without education, training, and awareness, even the most comprehensive laws risk ineffective implementation.

7.8 Conclusion

The empirical investigation reveals a central paradox within India's data governance landscape: a broad base of awareness exists, yet confidence in protection mechanisms remains limited. Participants across all groups recognized the relevance of data protection, but they also expressed widespread dissatisfaction with the sufficiency of the current legal framework. The Digital Personal Data Protection Act, 2023, though a pivotal milestone, is perceived as incomplete because it fails to address the specific challenges of non-personal data. Respondents overwhelmingly supported the establishment of distinct legislation to govern such data, especially in areas related to re-identification, economic misuse, and international data transfers.

Moreover, the findings reflect a consistent demand for enhanced transparency, stronger institutional accountability, and improved ethical standards within data management practices. Despite growing awareness, most respondents do not pursue legal remedies due to procedural and structural barriers, indicating an enforcement gap between rights and remedies. The study thus confirms that India's current approach remains fragmented, reactive, and in need of comprehensive reform that combines legal innovation, administrative efficiency, and public education.

CHAPTER 8

CONCLUSION AND RECOMMENDATIONS

8.1 Conclusion

The research undertaken in this thesis has traced the evolution, challenges, and prospects of *Non-Personal Data (NPD)* governance, situating it within India's rapidly transforming digital ecosystem and the broader global context. Across its doctrinal, comparative, and empirical dimensions, the study establishes that *NPD* has become an indispensable legal and economic category in the twenty-first century. It is no longer a residual by-product of digital activity but a pivotal resource that drives innovation, shapes governance, and influences both national policy and international relations. The findings collectively affirm that India's current framework remains incomplete without a coherent, enforceable, and principled legal regime for the regulation of non-personal data.

Each chapter of this thesis was designed to address a specific objective and corresponding hypothesis, thereby ensuring methodological coherence throughout. The first chapter introduced the research problem and framework; the subsequent chapters from 2 through 6 each examined doctrinal, comparative, and theoretical aspects aligned with the stated objectives and hypotheses, while Chapter 7 consolidated the empirical evidence across all dimensions. Together, these components collectively reinforce the study's central argument and validate its hypotheses.

The introductory chapter set the conceptual and methodological foundation by distinguishing between personal and *Non-Personal Data* and by identifying the research problem, objectives, and hypotheses. It underscored that while India has achieved a significant milestone through the Digital Personal Data Protection Act 2023, this legislation deliberately confines itself to personal data and omits anonymized, aggregated, and machine-generated datasets. This legislative silence has resulted in a governance vacuum, leaving vast repositories of *NPD* unregulated despite their immense social and economic potential. The introduction also emphasized that any viable framework must reconcile the imperatives of innovation and data-driven

growth with the ethical demands of privacy, accountability, and equitable benefit sharing.

Chapter 2 expanded upon this conceptual base by examining data as a legal and economic asset and by exploring its categorization under existing statutes. It demonstrated that the Information Technology Act 2000 and its allied rules provide only limited coverage and are primarily oriented toward cybersecurity and personal data breaches. The discussion revealed that the stratification of data rights according to provenance, sensitivity, and jurisdiction is essential to effective regulation. The analysis of the GDPR and the DPDP Act highlighted that while personal and sensitive data receive stringent protection, machine-generated and anonymized data remain peripheral in most legal systems. This lacuna necessitates an evolved governance structure capable of addressing ownership, access, and accountability in the context of non-personal data.

Chapter 3 built upon this analysis by defining the nature, scope, and technical contours of *NPD*. Drawing on comparative jurisprudence and authoritative international sources, it proposed a refined legal definition that includes anonymized, aggregated, and machine-generated datasets which cannot be linked to an identifiable individual. The chapter further elaborated on the challenges of anonymization and the persistent risk of re-identification, stressing that technical measures alone are inadequate without accompanying legal safeguards. The exploration of stakeholder roles, governments, corporations, academia, and civil society, demonstrated that the governance of *NPD* is inherently multidisciplinary, requiring the intersection of law, technology, and ethics.

Chapter 4 undertook an extensive comparative study across major jurisdictions, including the European Union, the United Kingdom, Australia, South Korea, Kenya, the United States, China, Singapore, Japan, Brazil, and Canada. The analysis revealed diverse regulatory philosophies but a converging global recognition of *NPD* as an economic and societal resource. European models emphasize harmonization, ethical data altruism, and federated data infrastructures; Asian frameworks, particularly those of South Korea and Japan, prioritize innovation and trust; while emerging economies such as Kenya align data governance with developmental objectives. The comparison

demonstrated that legal clarity, institutional oversight, and cross-border cooperation are common determinants of successful governance. It also showed that fragmented or purely sectoral approaches, as seen in the United States, limit interoperability and consistency. The lessons drawn from these jurisdictions provide both normative guidance and practical reference points for India's evolving regulatory architecture.

Chapter 5 advanced the argument that regulating *NPD* is not merely a matter of administrative necessity but a constitutional and socio-economic imperative. The chapter developed a set of normative principles, clarity of definitions, legally regulated data-sharing ecosystems, ethical governance, balanced innovation, and international cooperation, that together constitute a holistic model for *NPD* governance. It demonstrated that jurisdictions which integrate these principles achieve higher levels of transparency, innovation, and public trust. The analysis also reaffirmed that legal certainty encourages responsible data use, mitigates monopolistic control, and fosters equitable participation in the digital economy.

Chapter 6 traced India's legislative and judicial trajectory toward *NPD* governance, assessing both achievements and shortcomings. It examined the proposals of the Kris Gopalakrishnan Expert Committee, including the classification of *NPD* into public, community, and private categories and the creation of institutional roles such as data custodians and trustees. Although these proposals have not yet been translated into law, they establish a conceptual blueprint for future reform. The chapter also analyzed Indian jurisprudence, particularly the judgments in *K.S. Puttaswamy v. Union of India*, *Karmanya Singh Sareen v. Union of India*, *Eastern Book Company v. D.B. Modak*, and *PhonePe v. Resilient Innovation*, to demonstrate how constitutional principles of privacy, transparency, and fairness implicitly support the regulation of anonymized and community-based data. The conclusion drawn from this doctrinal and judicial synthesis is that India possesses a strong normative foundation but lacks the legislative and institutional mechanisms necessary for implementation.

Chapter 7 presented the empirical findings, offering valuable insights into stakeholder awareness, perceptions, and experiences. The survey, which encompassed legal professionals, information-technology experts, law students, and the general public,

revealed widespread understanding of data concepts but low confidence in existing legal protections. A significant majority across all groups supported the creation of a dedicated *NPD* law, highlighting the urgent need for transparency, ethical accountability, and enforcement. The responses confirmed that knowledge of data issues does not automatically translate into legal recourse, as procedural barriers and limited institutional responsiveness persist. The findings also underscored the importance of capacity building, continuous professional training, and inclusion of *NPD* governance within legal education to bridge the gap between awareness and action.

Taken together, the conclusions of the doctrinal and empirical chapters establish a coherent narrative. *Non-Personal Data* governance in India stands at a critical threshold. The country has the conceptual understanding, judicial endorsement, and policy intent to regulate *NPD*, yet the absence of a binding statutory framework and specialized institutional oversight constrains progress. The evidence affirms that governance of *NPD* is a socio-legal necessity rather than a policy option. A comprehensive framework must provide clear definitions, delineate institutional roles, establish access and benefit-sharing mechanisms, and mandate technical and ethical safeguards. Without such a framework, the advantages of digital transformation risk being concentrated among a few dominant entities, eroding public trust and widening social inequities.

The research therefore concludes that India must either expand the existing DPDP Act through a dedicated chapter on *NPD* or, preferably, enact a separate *Non-Personal Data* Governance Act harmonized with personal-data protection law yet distinct in scope and function. Such legislation should institutionalize a *Non-Personal Data* Authority, define trustee and custodian responsibilities, and embed fairness, transparency, and innovation as guiding principles. Supported by robust anonymization standards and periodic risk audits, this approach would balance technological advancement with constitutional values and social welfare.

In essence, this thesis demonstrates that the governance of *NPD* constitutes the next frontier of digital regulation. Its effective realization will determine whether data

functions as a tool of collective progress or as a vector of inequality. India's opportunity lies in designing a forward-looking, ethically grounded, and globally interoperable framework that transforms *Non-Personal Data* from an unregulated asset into a foundation for equitable development, accountable governance, and sustainable digital growth.

8.2 Hypothesis Testing

The hypotheses formulated at the outset of this research were designed to assess whether India's current and emerging legal frameworks adequately conceptualize and govern *Non-Personal Data (NPD)* in alignment with global standards and domestic digital imperatives. The empirical and doctrinal analyses undertaken across the preceding chapters provide a strong evidentiary basis for testing these hypotheses.

Hypothesis 1:

“A uniform legal definition of the term Non-Personal Data is essential for safeguarding the digital economy.”

The doctrinal and empirical findings across all respondent groups confirm this hypothesis. The absence of a statutory definition of *NPD* has created profound conceptual ambiguity, affecting legal clarity, regulatory coherence, and stakeholder awareness.

The doctrinal component, which examined Indian and comparative frameworks such as the Digital Personal Data Protection Act (2023), the EU's Regulation (EU) 2018/1807 on the Free Flow of Non-Personal Data, and the United Kingdom's National Data Strategy (2020), reveals that while advanced jurisdictions provide definitional clarity and institutional guidance, India remains without a precise legal formulation for *NPD*. The DPDP Act deliberately confines itself to “personal data,” thereby excluding anonymized, aggregated, and machine-generated datasets that constitute the foundation of artificial intelligence, analytics, and digital governance. This definitional vacuum inhibits both enforcement and innovation by leaving ownership, access rights, and accountability undetermined.

Table 8.2.1 Summary of Percentage Responses on Understanding and Distinction Between Personal and Non-Personal Data

Respondent Group	Comprehensive Understanding of Data Concepts (Q1)	Neutral Response (Q1)	Disagree + Strongly Disagree (Q1)	Ability to Distinguish Personal vs NPD (Q2)	Disagreed That Distinction is Legally Clear (Q2)
General Public	15% Strongly Agree + 53% Agree	22% Neutral	10% Disagree + 2% Strongly Disagree	16% Strongly Agree + 50% Agree	34% Disagreed
IT Professionals	20% Strongly Agree + 58% Agree	17% Neutral	5% Disagree + 0% Strongly Disagree	27% Strongly Agree + 55% Agree	42% Disagreed
Legal Professionals	24% Strongly Agree + 55% Agree	16% Neutral	5% Disagree + 0% Strongly Disagree	24% Strongly Agree + 58% Agree	49% Disagreed
Law Students	23% Strongly Agree + 41% Agree	20% Neutral	6% Disagree + 10% Strongly Disagree	27% Strongly Agree + 49% Agree	16% Disagreed + 5% Strongly Disagreed (21% total)

The empirical analysis reinforces these doctrinal observations. Across all four respondent categories - legal professionals, IT professionals, law students, and the general public, a consistent pattern of conceptual uncertainty and definitional inconsistency emerges. Among the general public, only 68 percent (15 percent Strongly Agree + 53 percent Agree) reported comprehensive understanding of data concepts, while 22 percent remained neutral and 12 percent disagreed, indicating that a significant portion of the population lacks foundational clarity on the distinction between personal and non-personal data. A similar pattern is visible among law students, where 64 percent (23 percent Strongly Agree + 41 percent Agree) claimed to possess comprehensive understanding, yet 20 percent were neutral and 16 percent expressed disagreement, suggesting that familiarity with data concepts is uneven. Although 76 percent of law students agreed that they could distinguish between personal and non-personal data, this understanding appears largely theoretical and is not supported by systematic curricular training, thereby limiting its practical application.

Among IT professionals, the pattern persists. While 78 percent (20 percent Strongly Agree + 58 percent Agree) demonstrated an understanding of data concepts and 82 percent (27 percent Strongly Agree + 55 percent Agree) claimed the ability to distinguish between personal and non-personal data, 42 percent disagreed that the legal distinction is sufficiently clear for professional use. This illustrates that even technically trained respondents encounter ambiguity when applying legal definitions to operational datasets. Legal professionals also displayed similar challenges: although 79 percent (24 percent Strongly Agree + 55 percent Agree) reported conceptual understanding and 82 percent (24 percent Strongly Agree + 58 percent Agree) indicated the ability to differentiate between personal and non-personal data, 49 percent disagreed that the distinction is clear within the legal framework. This represents the highest level of disagreement across all groups and highlights persistent challenges in statutory interpretation, practical application, and regulatory implementation.

Taken together, these findings reveal that the absence of a uniform legal definition of Non-Personal Data generates pervasive uncertainty across both academic and

professional domains. The lack of definitional clarity produces conceptual ambiguity, affecting even those working within legal and technological sectors. This ambiguity translates into operational confusion, influencing organizational compliance, data-handling practices, anonymization standards, and the broader functioning of data governance systems. The resulting regulatory fragmentation further compounds the problem, as authorities, practitioners, and institutions rely on inconsistent or improvised interpretations in the absence of statutory guidance. The empirical evidence also indicates notable academic and professional gaps: law students and significant portions of the general public demonstrated uneven levels of understanding, underscoring deficiencies in both formal legal education and public awareness.

Collectively, these findings validate Hypothesis 1. A consistent and uniform legal definition of *NPD* is indispensable for protecting economic and governance interests in the digital era. Without definitional precision, anonymization standards remain inconsistent, community data lacks protection, and re-identification risks persist. The study therefore concludes that establishing a statutory definition, supported by subordinate rules clarifying categories, boundaries, and enforcement, constitutes the foundational step toward an integrated data-governance regime.

Hypothesis 2:

“The lack of streamlined legal frameworks for Non-Personal Data governance across jurisdictions enables its misuse by corporations for monetary gain.”

The cumulative doctrinal and empirical evidence also strongly supports this hypothesis. The comparative analysis across jurisdictions demonstrates that fragmented or underdeveloped legal systems foster environments in which corporate entities exploit regulatory gaps for economic advantage. The empirical component further substantiates this through consistent stakeholder testimony of opacity, misuse, and insufficient redress mechanisms.

Table 8.2.2 Summary of Percentage Responses on Adequacy of Laws, Transparency, and Global Harmonization

Respondent Group	Indian Laws Sufficient to Safeguard NPD (Q3)	Demand for Corporate Transparency (Q4)	Support for Legal Protection of NPD (Q5)	Concern Over Organizational Data Use (Q6)	Exposure to Data Breaches / Misuse (Q7)	Support for Global Harmonized Laws (Q8)	Support for Amendment / Inclusion (Q9)
General Public	5% Strongly Agree + 22% Agree (27% total support; 47% disagree)	32% Strongly Agree + 56% Agree	38% Strongly Agree + 46% Agree	36% Strongly Agree + 45% Agree	28% Yes	36% Strongly Agree + 45% Agree	32% Strongly Agree + 51% Agree
IT Professionals	17% Strongly Agree + 15% Agree	51% Strongly Agree + 39% Agree	32% Strongly Agree + 43% Agree	47% Strongly Agree + 39% Agree	70% Yes	34% Strongly Agree + 49% Agree	51% Strongly Agree + 39% Agree
Legal Professionals	4% Strongly Agree + 9% Agree	65% Strongly Agree + 27% Agree	27% Strongly Agree + 58% Agree	41% Strongly Agree + 34% Agree	54% Yes	41% Strongly Agree + 34% Agree	27% Strongly Agree + 58% Agree
Law Students	17% Strongly Agree + 26% Agree	59% Strongly Agree + 37% Agree	32% Strongly Agree + 56% Agree	31% Strongly Agree + 43% Agree	35% Yes	24% Strongly Agree + 33% Agree	33% Strongly Agree + 42% Agree

Across respondent groups, the empirical findings establish a consistent pattern of perceived insufficiency in existing NPD governance frameworks. Among the general public, only 27 percent (5 percent Strongly Agree + 22 percent Agree) believed that Indian laws sufficiently safeguard NPD, while 47 percent disagreed. At the same time, 88 percent (32 percent Strongly Agree + 56 percent Agree) demanded greater transparency from corporations, and 84 percent (38 percent Strongly Agree + 46 percent Agree) supported explicit legal protection for NPD. The concern that organizational data use lacks adequate oversight was reflected in 81 percent agreement, and 28 percent reported direct exposure to data misuse or breaches. These findings indicate that regulatory shortcomings are directly perceived as facilitating opaque corporate practices.

IT professionals offered similarly strong evidence confirming the hypothesis. Only 32 percent expressed confidence in the sufficiency of Indian NPD regulation, while 90 percent (51 percent Strongly Agree + 39 percent Agree) demanded greater transparency in corporate data practices. A substantial 75 percent (32 percent Strongly Agree + 43 percent Agree) supported specific legal protection for NPD, and 86 percent expressed concern about organizational data use. Notably, 70 percent reported personal exposure to data breaches or misuse, directly linking regulatory ambiguity to operational vulnerabilities. Strong support for global harmonized laws, 83 percent (34 percent Strongly Agree + 49 percent Agree), reflects the recognition that fragmented international standards complicate compliance and facilitate cross-border exploitation of anonymized datasets.

The responses from legal professionals further reinforce these concerns. Only 13 percent (4 percent Strongly Agree + 9 percent Agree) believed that Indian laws adequately regulate NPD, while 75 percent (41 percent Strongly Agree + 34 percent Agree) supported global harmonization. A significant 85 percent (27 percent Strongly Agree + 58 percent Agree) viewed amendments to existing laws as necessary. Their insights indicate that statutory gaps and interpretational uncertainties enable corporations to monetize NPD without proportional transparency or accountability, allowing private actors to convert community or public datasets into proprietary economic assets.

Law students, representing future legal practitioners, also displayed awareness of these deficiencies. Only 43 percent (17 percent Strongly Agree + 26 percent Agree) considered Indian NPD governance adequate, while 96 percent (59 percent Strongly Agree + 37 percent Agree) demanded corporate transparency. 88 percent supported legal protection of NPD, and 74 percent expressed concern about how organizations manage anonymized or aggregated data. Although only 35 percent reported direct exposure to breaches, the overwhelming support for reform indicates that the next generation of legal professionals anticipates that unresolved regulatory gaps will continue to enable misuse in the absence of coherent legal structures.

These converging lines of evidence demonstrate that fragmented regulation facilitates the monetization of *NPD* without corresponding obligations for transparency, ethical compliance, or equitable benefit-sharing. The findings highlight that without statutory frameworks ensuring disclosure, auditability, and proportional sanctions, *NPD* governance will remain vulnerable to manipulation by dominant corporate actors.

Hence, Hypothesis 2 is confirmed: the lack of coherent, streamlined frameworks both within and across jurisdictions directly enables misuse and economic exploitation of *NPD*. Effective governance must therefore involve synchronized national and international legal instruments, explicit duties of disclosure and accountability for data-holding entities, and institutional mechanisms that ensure fair distribution of data-derived benefits.

Synthesis of Hypothesis Validation

The empirical findings across 400 respondents, supported by doctrinal analysis, collectively affirm both hypotheses. The results demonstrate that definitional clarity and regulatory coherence are indispensable preconditions for ethical and equitable use of Non-Personal Data. A uniform statutory definition is necessary to provide legal certainty, while a harmonized global governance structure is required to prevent corporate misuse and ensure transparency.

Together, the hypotheses establish that *Non-Personal Data* governance is not merely a technical or administrative concern but a constitutional and socio-economic imperative. The absence of comprehensive regulation threatens to erode both public

trust and market fairness, while robust legal frameworks can transform *NPD* into a catalyst for innovation, research, and inclusive development.

8.3 Recommendations

The study establishes that *Non-Personal Data (NPD)* has emerged as a vital driver of the global digital economy, influencing policy design, governance frameworks, and socio-economic development. However, the findings across doctrinal and empirical dimensions reveal that while India has achieved significant progress in personal data protection through the Digital Personal Data Protection Act (2023), the governance of *NPD* remains fragmented, policy-driven, and under-institutionalized. The following recommendations are proposed to bridge the gap between conceptual ambition and regulatory implementation. These suggestions are categorized into four interrelated domains: policy and legal reform, academic and professional capacity-building, societal and ethical awareness, and institutional innovation.

I. Policy and Legal Recommendations

i. Enactment of a Comprehensive Data Protection Legislation

India should adopt a unified legislative framework that encompasses personal data, non-personal data, and anonymized datasets within a single comprehensive statute. Rather than maintaining fragmented or sectoral legislations, a consolidated law would provide definitional precision, avoid jurisdictional overlaps, and create a coherent governance structure. Each category, personal, non-personal, and anonymized data, should form distinct chapters within the statute, establishing harmonized rights, obligations, and enforcement mechanisms. This integrated framework would not only align with global standards such as the European Union's GDPR and the EU Regulation 2018/1807 on the Free Flow of *Non-Personal Data* but also reflect India's developmental priorities.

The Digital Personal Data Protection Act (2023) may serve as a foundational model for expansion, incorporating provisions on *NPD* access rights, anonymization standards, and benefit-sharing mechanisms.

ii. Establishment of an Independent Regulator for Data Governance

A dedicated Data Protection and Governance Authority (DPGA) should be constituted as an independent statutory body empowered to oversee both personal and non-personal data. Its mandate should include supervisory, regulatory, and adjudicatory powers to ensure compliance, accountability, and consistency across sectors. The DPGA should function as a central coordinating authority, similar to the Reserve Bank of India's role in the financial ecosystem, monitoring multiple regulators, enforcing penalties, and issuing advisory guidelines on anonymization, data sharing, and cross-border transfers. A strong institutional framework is essential to transform India's data governance from reactive oversight to proactive regulation.

iii. Mandatory Transparency and Accountability Mechanisms

Transparency must become the cornerstone of *NPD* governance. Corporations, start-ups, and public bodies should be legally mandated to publish annual transparency reports disclosing the nature of datasets collected, anonymization techniques applied, sharing arrangements, and third-party access permissions. These reports would serve both regulatory and public accountability purposes, helping monitor misuse while reinforcing trust.

The Securities and Exchange Board of India (SEBI) model for disclosure norms and global transparency reports by major technology companies provide useful templates adaptable to the *NPD* context. Additionally, these reports could serve as a vital database for empirical monitoring by policymakers and researchers.

iv. International Harmonization of Legal Standards

Given the cross-border character of data flows, India's legal framework should actively engage in international cooperation to harmonize standards of *NPD* governance. Bilateral and multilateral agreements should address anonymization norms, ethical AI data sharing, and dispute resolution mechanisms for transnational data exchanges.

Lessons from the European Union, South Korea, and Kenya demonstrate that balanced integration of domestic priorities with international consistency enhances both investor

confidence and citizen protection. India should play a proactive role in shaping global dialogues on *NPD* governance through platforms such as the G20 and the OECD.

II. Academic and Professional Recommendations

i. Curriculum Integration and Legal Education Reform

Data governance, encompassing both personal and non-personal data, should be made a mandatory part of academic curricula in law, information technology, and management disciplines. It must not remain an elective subject but be integrated as a core component of cyber law and IT law, ensuring that students develop a sound understanding of the legal, ethical, and technological dimensions of data regulation. The precedent for such integration already exists. Over time, the Right to Information Act (RTI), 2005, the Information Technology Act, 2000, and Intellectual Property Rights (IPR) laws have become standard components of Indian legal education. These subjects, once introduced as specialized electives, are now routinely taught in most universities. As a result, students graduate with a clear grasp of transparency obligations under RTI, digital transaction and cybersecurity issues under the IT Act, and innovation protection under IPR regimes. In a similar manner, *Non-Personal Data* (*NPD*) governance can be incorporated within the existing Cyber Law and IPR modules, addressing issues such as data classification, anonymization, ownership, and benefit-sharing. Embedding *NPD* concepts in this framework would ensure that future professionals not only understand the technical process of data generation but also the legal and ethical responsibilities attached to it. This reform would create a generation of legally and technologically literate professionals equipped to interpret, implement, and innovate within India's evolving data governance landscape.

ii. Specialized Professional Training

Capacity building must extend beyond academia to include structured training for judges, lawyers, law enforcement agencies, regulators, and IT professionals. Judicial academies should integrate modules on digital evidence, data governance, and anonymization risks into continuing education programs. Similarly, professional institutions such as the National Institute of Electronics and Information Technology (NIELIT) could offer certification courses on *NPD* compliance, anonymization

technologies, and ethical AI frameworks. Regular workshops, seminars, and e-learning modules should facilitate cross-disciplinary understanding between legal and technical professionals, thereby bridging the existing skill and literacy gaps.

iii. Research Incentivization and Institutional Support

There is an urgent need to foster a robust research ecosystem on data governance. Targeted grants, fellowships, and institutional partnerships should be provided to universities, think tanks, and policy research centers to study anonymization methods, re-identification risks, and the socio-economic implications of data-driven systems.

Government-sponsored programs, akin to research funding in renewable energy and biotechnology, should be extended to data governance innovation. Such initiatives would help generate an indigenous knowledge base and technical standards tailored to India's socio-economic realities.

III. Societal Recommendations

i. National Awareness and Legal Literacy Campaigns

Awareness among citizens about their rights, risks, and remedies relating to *NPD* remains alarmingly low. To bridge this gap, the government should launch a nationwide awareness campaign, through television, radio, and social media, educating the public on data rights, grievance mechanisms, and safe digital practices. Drawing inspiration from the national UPI fraud awareness campaign, a dedicated helpline could be introduced for reporting instances of data misuse or breach. Public outreach is vital for strengthening trust and participatory governance in the digital ecosystem.

ii. Promotion of Community Participation through Data Trusts

The concept of data trusts should be piloted to institutionalize community participation in *NPD* governance. These trusts would enable local communities to collectively decide how their data, such as agricultural, health, or mobility data, is shared and utilized, ensuring that benefits flow back to them. This model parallels the successful framework of self-help groups that manage collective resources at the grassroots level.

By embedding community representation in data governance, India can align technological innovation with distributive justice and democratic accountability.

iii. Embedding the Right to Privacy within *NPD* Governance

The constitutional right to privacy under Article 21, recognized in *K.S. Puttaswamy v. Union of India*, must be extended to encompass non-personal and community data. Although *NPD* does not identify individuals directly, its re-identification potential and societal implications warrant constitutional protection. This extension would ensure that privacy is treated not merely as an individual right but as a collective and contextual safeguard, reinforcing ethical accountability in data governance. The principle of “privacy by design” should be legally mandated across both personal and *Non-Personal Data* ecosystems.

IV. Ethical and Governance-Oriented Reflections

The study reaffirms that technology alone cannot guarantee justice or equality. The rapid expansion of artificial intelligence and algorithmic governance has rendered data both an instrument of progress and a source of vulnerability. Policymakers must therefore pursue a balance between technological innovation and ethical restraint. Legal frameworks should integrate human-centric values such as transparency, accountability, inclusivity, and fairness. Governance models that emphasize participatory oversight, through multi-stakeholder councils comprising government, industry, academia, and civil society, can ensure that technological advancements remain consistent with democratic ethics.

The overarching recommendation is thus twofold: India must transition from policy to legislation and from awareness to enforceable adequacy. This transition requires not only legal reform but also institutional strengthening, societal education, and global alignment. A standalone *Non-Personal Data* Governance Act, harmonized with the DPDP Act, 2023, is imperative to secure the dual goals of economic innovation and rights protection. The integration of these legal, educational, and ethical recommendations will transform data governance into an inclusive, accountable, and forward-looking framework that positions India as a global leader in equitable digital transformation.

8.4 Final Reflection

“The goal is to turn data into information, and information into insight.” — Carly Fiorina

The research undertaken for this thesis began with this vision: to understand how *Non-Personal Data (NPD)* could become a catalyst for innovation, governance, and social good. Yet, as the study evolved, it also revealed the profound risks embedded in the unrestrained expansion of the digital sphere. As technology continues to expand the boundaries of possibility, wisdom must define its limits. The rise of artificial intelligence and algorithmic governance, fueled by vast and often unregulated data, stands as both a triumph of human intellect and a warning of its excesses. The virtual world, boundless, intangible, and complex- is a grey domain, far larger and more unpredictable than the oceans of the Earth.

Although data drives progress, its misuse can equally precipitate harm. For a sustainable and humane digital future, societies must learn to balance innovation with restraint, efficiency with ethics, and progress with prudence.

“Data is the new oil, but the fire it fuels may one day burn beyond our control.”

Only by embedding human values, accountability, and wisdom into technological systems can humanity ensure that data remains a tool of empowerment rather than domination.

The journey of this research thus concludes not merely with policy prescriptions, but with a broader reminder: that governance, in the truest sense, is not about control of data, but about control of ourselves.

This study may serve as an anchor point for future research, offering a foundational framework for continued academic inquiry into the governance of Non-Personal Data.

**

BIBLIOGRAPHY

Table of Authorities

Part 1: Statutes & Regulations

Part 2: International Treaties & Instruments

Part 3: Cases

Part 4: Books

Part 5: Reports & Institutional Publications

Part 6: Journal Articles

Part 7: Online Sources

PART 1: STATUTES & REGULATIONS

A. Indian Statutes, Bills & Regulations

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016 (India).

Aadhaar and Other Laws (Amendment) Act, No. 14 of 2019 (India).

CERT-In Directions on Information Security Practices, Procedures, Prevention, Response, and Reporting of Cyber Incidents, Apr. 28, 2022 (India).

Constitution of India (1950).

Digital Personal Data Protection Act, No. 19 of 2023 (India).

Indian Contract Act, No. 9 of 1872 (India).

Indian Evidence Act, No. 1 of 1872, §§ 65A-65B (India).

Indian Penal Code, No. 45 of 1860 (India).

Information Technology Act, No. 21 of 2000 (India).

Information Technology (e-Governance Standards) Rules, 2015 (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022, G.S.R. 1253(E) (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, G.S.R. 311(E) (India).

Master Circular on Credit Information Companies, Reserve Bank of India (2021) (India).

Master Direction, Digital Payment Security Controls, Reserve Bank of India (2021) (India).

Master Direction, Information Technology Governance, Risk, Controls and Assurance Practices, Reserve Bank of India (2023) (India).

SEBI Cybersecurity and Cyber Resilience Framework (2019) (India).

Telecom Regulatory Authority of India, Recommendations on Data Protection Framework for the Telecom Sector (2017) (India).

UIDAI (Authentication) Regulations, 2021 (India).

B. Indian Policies & Frameworks

Bureau of Indian Standards, IS 17428:2020, Data Privacy Assurance Requirements (India).

Data Empowerment and Protection Architecture (DEPA), NITI Aayog (2020) (India).

Digital India Act, Proposed Framework, Ministry of Electronics & Information Technology (2023-2024) (India).

Digital Information Security in Healthcare Act (Draft), Ministry of Health & Family Welfare (2018) (India).

Draft National Cyber Security Strategy, National Security Council Secretariat (2021) (India).

Draft National Data Governance Framework Policy, Ministry of Electronics & Information Technology (2022) (India).

Electronic Health Record (EHR) Standards, Ministry of Health & Family Welfare (2016) (India).

India Enterprise Architecture (IndEA) Framework, Ministry of Electronics & Information Technology (2018) (India).

MeghRaj Cloud Policy (National Cloud Initiative), Ministry of Electronics & Information Technology (2012) (India).

National AI Strategy (“AI for All”), NITI Aayog (2018) (India).

National Cyber Security Policy, Ministry of Communications & Information Technology (2013) (India).

National Data Sharing and Accessibility Policy, Department of Science & Technology (2012) (India).

National Digital Communications Policy, Ministry of Communications (2018) (India).

National Health Authority, Health Data Management Policy (2022) (India).

Proposed Digital Personal Data Protection Rules (Draft for Consultation) (2025) (India).

C. European Union Instruments

Regulation (EU) 2016/679, of the European Parliament and of the Council of 27

April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Regulation (EU) 2018/1807, on the Free Flow of Non-Personal Data, 2018 O.J. (L 303) 59.

Regulation (EU) 2019/1024, on Open Data and the Re-Use of Public Sector Information, 2019 O.J. (L 172) 56.

Regulation (EU) 2022/868, on European Data Governance (Data Governance Act), 2022 O.J. (L 152) 1.

Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM (2022) 68 final (Feb. 23, 2022).

D. Foreign Statutes (Non-EU)

Australia, Data Availability and Transparency Act, 2022 (Cth).

Australia, Privacy Act, 1988 (Cth).

Brazil, *Lei Geral de Proteção de Dados Pessoais* (LGPD), Law No. 13,709 (2018).

Canada, Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

China, Data Security Law, Order No. 84 (2021).

China, Personal Information Protection Law, Order No. 91 (2021).

France, *Loi pour une République numérique*, Law No. 2016-1321 (7 Oct. 2016).

Germany, Data Strategy (Federal Ministry for Economic Affairs & Climate Action 2021).

Japan, Basic Act on the Advancement of Utilizing Public and Private Sector Data, Act No. 103 of 2016.

Kenya, Data Protection Act, No. 24 of 2019.

Singapore, Personal Data Protection Act, Act No. 26 of 2012 (rev. ed. 2021).

Singapore Government, Smart Nation and Digital Government Blueprint (2018).

South Korea, Data Industry Promotion Act, Act No. 16439 (2019).

South Korea, Personal Information Protection Act, Act No. 10465 (2011) (as amended 2020).

United Kingdom, Data Protection Act 2018.

United Kingdom, National Data Strategy, Department for Digital, Culture, Media & Sport (2021).

United States, California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199 (2018).

PART 2: INTERNATIONAL TREATIES & INSTRUMENTS

A. Multilateral Treaties & Conventions

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Apr. 15, 1994, 33 I.L.M. 81 (1994).

Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, 828 U.N.T.S. 221.

Budapest Convention on Cybercrime, Nov. 23, 2001, 41 I.L.M. 282 (2002).

Budapest Treaty on the International Recognition of the Deposit of Microorganisms for the Purposes of Patent Procedure, Apr. 28, 1977, 32 U.S.T. 1241.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+), Council of Europe, Oct. 18, 2018.

International Covenant on Civil and Political Rights (ICCPR), Dec. 16, 1966, 999 U.N.T.S. 171.

International Covenant on Economic, Social and Cultural Rights (ICESCR), Dec. 16, 1966, 993 U.N.T.S. 3.

Madrid Agreement Concerning the International Registration of Marks, June 14, 1891, 828 U.N.T.S. 389.

Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled, June 27, 2013.

Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, 21 U.S.T. 1583, 828 U.N.T.S. 305.

Patent Cooperation Treaty, June 19, 1970, 28 U.S.T. 7645.

Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, Oct. 26, 1961, 496 U.N.T.S. 43.

United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.

WIPO Copyright Treaty, Dec. 20, 1996, 2186 U.N.T.S. 121.

WIPO Performances and Phonograms Treaty, Dec. 20, 1996, 2186 U.N.T.S. 203.

B. International & Intergovernmental Soft Law Instruments

G20 Osaka Leaders' Declaration, Data Free Flow with Trust (DFFT) Commitment (G20 2019).

Internet Governance Forum (IGF), Annual Reports (United Nations).

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).

OECD, Recommendation of the Council on Digital Security Risk Management for Trust and Resilience (2019).

OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463 (2021).

United Nations, Guiding Principles on Business and Human Rights, U.N. Doc. A/HRC/17/31 (2011).

UN General Assembly, Resolution on the Right to Privacy in the Digital Age, G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Dec. 18, 2013).

UNESCO, Recommendation on the Ethics of Artificial Intelligence, Nov. 23, 2021.

PART 3: CASE LAW

A. Indian Cases

Eastern Book Co. v. D.B. Modak, (2008) 3 S.C.C. 385 (India).

Emergent Genetics India Pvt. Ltd. v. Shailendra Shivam, 2011 S.C.C. OnLine Del. 3244 (India).

John Richard Brady v. Chemical Process Equipments, A.I.R. 1987 Del. 213 (India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

Karmanya Singh Sareen v. Union of India, W.P. (C) 799/2017 (India).

Kharak Singh v. State of U.P., (1964) 1 S.C.R. 331 (India).

Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

State of Karnataka v. Ranganath Reddy, (1978) 4 S.C.C. 608 (India).

B. European Union Cases

Breyer v. Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779.

Data Protection Commissioner v. Facebook Ireland Ltd., Case C-673/17, EU:C:2019:1140.

Peter Nowak v. Data Protection Commissioner, Case C-434/16, EU:C:2017:994.

Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs (SABAM), Case C-70/10, EU:C:2011:771.

Y.S. v. Minister voor Immigratie, Integratie en Asiel, Joined Cases C-141/12 & C-372/12, EU:C:2014:240.

C. United States Cases

Diamond v. Chakrabarty, 447 U.S. 303 (1980).

Fed. Trade Comm’n v. Facebook, Inc., No. 3:19-cv-2134 (N.D. Cal. 2019).

PART 4: BOOKS

A. International Books

Bell, Daniel, *The Coming of Post-Industrial Society* (Basic Books 1973).

Castells, Manuel, *The Information Age: Economy, Society, and Culture* (3 vols., Wiley-Blackwell 1996–1998).

Cohen, Julie E., *Between Truth and Power: The Legal Construction of Informational Capitalism* (Oxford Univ. Press 2019).

Floridi, Luciano, *The Philosophy of Information* (Oxford Univ. Press 2011).

Floridi, Luciano, *The Ethics of Data: Perspectives from Philosophy and Law*, in *The Cambridge Handbook of Information and Data Ethics* (2021).

Hartzog, Woodrow, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard Univ. Press 2018).

Hoecke, Mark van, ed., *Data Law in the EU: Regulation, Governance, and Compliance* (Cambridge Univ. Press 2021).

Kuner, Christopher, *Transborder Data Flows and Data Privacy Law* (Oxford Univ. Press 2013).

Lobel, Orly, *You Don't Own Me: How Mattel v. MGA Set Off a Revolution in IP* (Norton 2017).

Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton Univ. Press 2009).

Mayer-Schönberger, Viktor & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013).

Murray, Andrew, *Information Technology Law: The Law and Society* (Oxford Univ. Press 2019).

Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard Univ. Press 2015).

Reed, Chris & Jonathan Cave, *Big Data and the Law* (Edward Elgar 2018).

Schwartz, Paul M. & Daniel J. Solove, *Information Privacy Law* (Wolters Kluwer 2020).

Yeung, Karen & Martin Lodge, eds., *Algorithmic Regulation* (Oxford Univ. Press 2019).

B. Indian Books

Duggal, Pavan, *Handbook on Cyberlaw* (Universal 2020).

Fatima, Talat, *Cyber Crimes* (Universal 2018).

Gopalakrishnan, N.S. & T.G. Agitha, *Principles of Intellectual Property* (Eastern Book Co.).

Gupta, Apar, *Internet Freedom in India* (Hachette 2020).

Iyer, Ramaswamy, *Information Technology Law and Practice* (LexisNexis 2021).

Padmanabhan, Ananth, *Intellectual Property and Innovation Law in India* (Oxford Univ. Press 2019).

Ramaswamy, S., *Legal Aspects of Computing and Information Technology* (PHI 2016).

Seervai, H.M., *Constitutional Law of India* (4th ed., Universal 2019).

Shome, Shayak, *Digital Competition Law in India* (2023).

Shukla, V.N., *Constitution of India* (13th ed., Eastern Book Co. 2017).

Sivakumar, S., *Indian Media and Cyberspace Law* (LexisNexis).

Verma, S.K., *Cyberspace and Data Privacy Law in India* (publisher varies).

C. Institutional & Open-Access Academic Books (treated as books under Bluebook Rule 15)

Amsterdam University Press, *Responsible Data Science* (AUP Open, OA edition).

Cambridge University Press, *Data-Driven Personalisation in Markets, Politics, and Regulation* (OA ed.).

Cambridge University Press, *The Politics of Big Data* (OA ed.).

Internet Society/Oxford Internet Institute, *The Global Information Society* (OA ed.).

Internet Society/OII, *Rethinking the Digital Economy* (OA ed.).

ITU, *AI for Good: Global Governance and Ethics* (OA ed.).

MIT Press, *Algorithmic Accountability* (OA ed.).

MIT Press, *Open Data and the Knowledge Society* (OA ed.).

Royal Society, *Data Management and Use: Governance in the 21st Century* (2017).

Springer, *Data Protection and Privacy: The Age of Intelligent Machines* (2021, OA ed.).

D. Institutional Comprehensive Works (Book-Length World Reports)

OECD, *Digital Economy Outlook* (2017; 2020; 2023).

UNCTAD, *Digital Economy Report* (2019; 2021; 2023).

World Bank, *World Development Report 2016: Digital Dividends*.

World Bank, *World Development Report 2021: Data for Better Lives*.

PART 5: REPORTS & INSTITUTIONAL PUBLICATIONS

A. Indian Reports & Institutional Publications

Department of Science & Technology, *National Data Sharing and Accessibility Policy* (2012).

European Union Agency for Cybersecurity (ENISA), *Guidelines on Security Measures for Cloud Computing* (2022).

Internet Governance Forum (IGF), *Annual Progress Report on Internet Governance* (United Nations 2022).

Law Commission of India, *262nd Report: Review of Data Protection Framework* (2017).

Ministry of Economy, Trade & Industry (Japan), *Data Free Flow with Trust (DFFT)* (2019).

Ministry of Electronics & Information Technology (MeitY), *Draft National Data Governance Framework Policy* (2022).

National Institute of Public Finance and Policy (NIPFP), *Working Papers on Data Governance* (various years).

National Law School of India University (NLSIU), *Indian Journal of Law & Technology* (various issues).

NITI Aayog, *Data Empowerment and Protection Architecture (DEPA)* (2020).

NITI Aayog, *National Strategy for Artificial Intelligence—AI for All* (2018).

Reserve Bank of India, *Report of the Working Group on Digital Lending—Including Lending Through Online Platforms and Mobile Apps* (2021).

Supreme Court of India, *Right to Privacy as Fundamental Right—Summary of Puttaswamy Judgment* (2017).

Vidhi Centre for Legal Policy, *A Roadmap for India's Data Governance Framework* (2019).

B. International, Multilateral, and Foreign Institutional Reports

Ashoka University, Centre for Digital Economy Policy Research (C-DEP), *Reports on Data Markets and Digital Regulation* (various 2020–2023).

Brookings Institution, *Governing Data for Development* (2020).

Carnegie India, *India's Approach to Data Governance* (2020).

Centre for Internet & Society (India), *Data Governance and Non-Personal Data Working Papers* (various years).

Centre for Internet & Society (International), *Algorithmic Accountability and Data Governance Papers* (various).

European Commission, *A European Strategy for Data*, COM(2020) 66 final (Feb. 19, 2020).

European Data Protection Board, *Guidelines on Data Anonymization and Pseudonymization* (2020).

European Data Protection Board, *Guidelines on Data Portability*, EDPB-000-2021 (2021).

Infocomm Media Development Authority (Singapore), *Data Sharing Framework* (2022).

Internet Freedom Foundation, *Research Papers on Privacy, Data Protection, and Digital Rights* (various).

Observer Research Foundation (ORF), *Digital Rights & Data Governance Series* (various).

OECD, *OECD Privacy Framework* (2013).

OECD, *Recommendation of the Council on Digital Security Risk Management for Trust and Resilience* (2019).

OECD, *OECD Principles on Artificial Intelligence* (2019).

Royal Society (UK), *Data Management and Use: Governance in the 21st Century* (2017).

Singapore Government, *Smart Nation and Digital Government Blueprint* (2018).

Takshashila Institution, *Data Empowerment, Consent & India's Digital State* (various).

UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age—Report of the High Commissioner*, U.N. Doc. A/HRC/27/37 (2014).

UNCTAD, *Digital Economy Report 2021: Cross-Border Data Flows and Development* (2021).

United Nations Conference on Trade and Development, *Digital Economy Report 2021: Cross-Border Data Flows and Development—For Whom Does the Data Flow?* (2021).

United Nations Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (2014).

UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

World Bank, *World Development Report 2021: Data for Better Lives* (2021).

World Economic Forum, *Data for Common Purpose Initiative (DCPI)* (2021).

World Trade Organization, *Joint Statement on E-Commerce and Digital Trade* (2021).

PART 6: JOURNAL ARTICLES

A. Journal Articles (International)

Balkin, Jack M., *Information Fiduciaries and the First Amendment*, 49 UC Davis L. Rev. 1183 (2016).

Bygrave, Lee A., *The Role of Purpose Limitation in EU Data Protection Law*, 2 Int'l Data Privacy L. 1 (2012).

Calo, Ryan, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995 (2014).

Cohen, Julie E., *What Privacy Is For*, 126 Harv. L. Rev. 1904 (2013).

Edwards, Lilian & Michael Veale, *Slave to the Algorithm?*, Manchester L. Sch. Working Paper (2017).

Ezrachi, Ariel & Maurice E. Stucke, *Digitalisation & Competition Policy: The Need for Coherence*, 14 J. Eur. Comp. L. & Prac. 65 (2020).

Finck, Michèle & Frank Pallas, *They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data Under the GDPR*, 15 J. Intell. Prop. L. & Tech. 1 (2022).

Fuster, Gloria González, *The Emergence of Personal Data Protection as a Fundamental Right*, 28 Eur. L.J. 130 (2014).

Graef, Inge, *Data as an Essential Facility*, 23 Colum. Sci. & Tech. L. Rev. 66 (2021).

Greenleaf, Graham, *Global Data Privacy Laws: 145 National Laws & Many Bills*, Privacy L. & Policy Rep. (2021).

Hildebrandt, Mireille, *Law for Computer Scientists and Other Folk*, Tech. & Reg. 1 (2019).

Kaminski, Margot, *Binary Governance: Privacy and Civil Rights in the Age of Big Data*, 92 Wash. L. Rev. 1763 (2017).

Kerber, Wolfgang, *Data Access, Interoperability and Portability in EU Data Governance*, 28 Eur. L. Rev. 883 (2021).

Khan, Lina, *Amazon's Antitrust Paradox*, 126 Yale L.J. 710 (2017).

Kuner, Christopher, *The Internet and the Global Reach of EU Law*, 62 Int'l & Comp. L.Q. 117 (2013).

Lynskey, Orla, *Deconstructing Data Subject Rights*, 28 Eur. L. Rev. 369 (2017).

Lynskey, Orla & Bert-Jaap Koops, *The GDPR and the Regulation of Non-Personal Data*, Comput. L. & Sec. Rev. (2020).

- Mittelstadt, Brent et al., *The Ethics of Algorithms: Mapping the Debate*, 3 Big Data & Soc'y 1 (2016).
- Pasquale, Frank, *Vertical Regulation of the Online Economy*, 4 Eur. J. Risk & Reg. 1 (2013).
- Richards, Neil & Woodrow Hartzog, *Privacy's Trust Framework*, 116 Mich. L. Rev. 445 (2017).
- Samuelson, Pamela, *Privacy as Intellectual Property?*, 52 Stan. L. Rev. 1125 (2000).
- Selinger, Evan & Woodrow Hartzog, *Obscurity and Privacy*, 88 Notre Dame L. Rev. 191 (2012).
- Solove, Daniel J., *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006).
- Solove, Daniel J. & Paul Schwartz, *Reconciling U.S. and EU Approaches to Privacy*, 102 Calif. L. Rev. 877 (2014).
- van Alsenoy, Brendan, *Liability for Algorithms in the EU*, 7 J. Eur. L. Stud. 105 (2020).
- Zarsky, Tal, *Incompatible: The GDPR and Machine Learning*, 27 N. Ill. U. L. Rev. 42 (2018).

B. Journal Articles (India-Specific)

- Babu, Rajesh, *Cross-Border Data Flows and India's Trade Commitments*, 55 J. World Trade 105 (2021).
- Kalyani, S., *Cybersecurity and the Indian Regulatory Landscape*, 34 Comput. L. & Sec. Rev. 123 (2018).
- Kamath, Nandan, *Competition, Data and Digital Markets in India*, 18 Indian Competition L. Rev. 201 (2021).

Matthan, Rahul, *Non-Personal Data Governance in India: A New Frontier*, 12 Nat'l L. Sch. India Rev. 55 (2021).

Mehta, P.P., *Algorithmic Governance and Indian Law*, 7 Indian J.L. & Tech. 1 (2022).

Prasanna, S., *Data Localization in India: Sovereignty, Security and Trade*, 15 Indian J.L. & Tech. 75 (2022).

Ramanathan, Usha, *Aadhaar: From Identity to Surveillance*, 9 Indian J. Const. L. 32 (2019).

Sarkar, K. & S. Roy, *Legal Challenges of Data Re-Identification in India*, 28 Indian J.L. & Tech. 45 (2020).

Sengupta, Arghya, *Privacy and the Indian State*, 3 Indian L. Rev. 25 (2019).

Shah, R.M., *India's Data Governance Framework: Challenges and Opportunities*, 30 Int'l J.L. & Info. Tech. 211 (2022).

PART 7: ONLINE SOURCES

A. Indian Online Sources

Ashoka University, Centre for Digital Economy Policy Research (C-DEP), Reports & Working Papers, <https://cdep.ashoka.edu.in>.

Centre for Internet & Society (CIS) India, Data Governance & NPD Working Papers, <https://cis-india.org>.

Internet Freedom Foundation (IFF), Research Papers on Privacy & Data Protection, <https://internetfreedom.in>.

Jindal Global Law School, JGLS Working Paper Series on Privacy & Technology Law, <https://jgu.edu.in>.

National Institute of Public Finance and Policy (NIPFP), Working Papers on Data Governance, <https://nipfp.org.in>.

National Law School of India University (NLSIU), Indian Journal of Law & Technology (Open Access), <https://ijlt.in>.

Observer Research Foundation (ORF), Digital Rights & Technology Policy Papers, <https://orfindia.org>.

Takshashila Institution, Public Policy Research on Data Protection & Digital State, <https://takshashila.org.in>.

Vidhi Centre for Legal Policy, Reports on Data Governance Framework, <https://vidhilegalpolicy.in>.

B. International Online Sources

Brookings Institution, Data Governance & AI Research Papers, <https://brookings.edu>.

European Commission, Digital Strategy & Data Act Documentation, <https://ec.europa.eu>.

European Data Protection Board (EDPB), Guidelines & Opinions, <https://edpb.europa.eu>.

Internet Society (ISOC), Digital Governance Publications, <https://internetsociety.org>.

MIT Press Open, Open Access Books on AI & Data, <https://mitpress.mit.edu/open>.

OECD, Digital Policy Papers & Privacy Guidelines, <https://oecd.org>.

Royal Society (UK), Technology Governance Publications, <https://royalsociety.org>.

United Nations Conference on Trade and Development (UNCTAD), Digital Economy Reports, <https://unctad.org>.

World Economic Forum (WEF), Data for Common Purpose Initiative (DCPI),
<https://www.weforum.org>.

World Bank, Open Knowledge Repository (OKR), Digital Governance Titles,
<https://openknowledge.worldbank.org>.

International Telecommunication Union (ITU), AI & Digital Governance
Publications, <https://itu.int>.

**

ANNEXURE I

QUESTIONNAIRE

Common Questions for All Sets (5 Questions)

1. I possess a comprehensive understanding of the concept of data, including personal and non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
2. I am capable of clearly distinguishing between personal data and non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
3. I am well-informed about the existing Indian legal framework governing data protection.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
4. In my view, the formulation of specific legal provisions for non-personal data is necessary.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
5. I consider global uniform data protection laws to be more effective than national laws in addressing data-related challenges.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree

Set 1: Law Implementers (Judges, Police, Legal Experts)

1. I believe the current Indian legal framework adequately addresses challenges related to personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
2. I consider the existing Indian legal provisions sufficient to regulate non-personal data usage and protection.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
3. I am confident in effectively applying Indian data protection laws within legal proceedings.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree

4. There is a substantial need for specialized legal training for law enforcement agencies in handling data-related cases.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
5. I am knowledgeable about international data protection laws, including regulations such as the GDPR.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
6. I believe existing Indian data protection laws require amendments to address emerging challenges posed by non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
7. The legal distinction between personal and non-personal data is sufficiently clear for application in legal contexts.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
8. In my opinion, non-personal data necessitates a distinct and comprehensive set of legal regulations.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
9. I believe that the legal community in India is adequately informed about non-personal data regulations.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
10. National legal frameworks are sufficient to address issues arising from non-personal data in the Indian context.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
11. Enhanced collaboration between law enforcement agencies and cyber experts is essential for effective data-related legal proceedings.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
12. I believe adopting international frameworks on non-personal data governance would enhance the effectiveness of Indian legal systems.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
13. Have you encountered cases involving data misuse or breaches in your professional capacity?
Options: Yes / No
14. In instances of data-related issues, did you pursue any legal action?
Options: Yes / No
15. If no legal action was taken, was it due to perceived inadequacies or ambiguities in existing laws?
Options: Yes / No

Set 2: Public in General

1. I am confident that Indian law provides adequate protection for my personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
2. I believe that existing Indian regulations are sufficient to safeguard non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
3. I am well-informed about how organizations collect and utilize non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
4. In my view, greater transparency is required from companies regarding the use of non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
5. I believe that non-personal data should be explicitly protected under legal frameworks.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
6. I am concerned about the ways in which my personal and non-personal data are utilized by organizations.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
7. Uniform global laws for data protection are necessary to ensure comprehensive data security.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
8. I support the implementation of more stringent national laws governing personal and non-personal data usage.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
9. Have you personally experienced issues related to data privacy or misuse, such as identity theft or data breaches?
Options: Yes / No
10. Did you take any action (e.g., filed a complaint) when faced with data-related issues?
Options: Yes / No
11. If no action was taken, was it due to unclear or insufficient legal provisions?
Options: Yes / No

12. Are you aware that personal privacy is recognized as a fundamental right under Indian law?
Options: Yes / No
13. Do you know the legal remedies available to you if your personal privacy is breached?
Options: Yes / No
14. Are you aware of the relevant authorities (e.g., police, consumer courts, cyber cells) to approach if your data privacy is violated?
Options: Yes / No
15. Do you understand the process of filing a complaint regarding the misuse of personal data?
Options: Yes / No

Set 3: Law Students

1. I believe legal education should include a more comprehensive study of non-personal data laws.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
2. I am confident that Indian legislation adequately regulates non-personal data usage.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
3. I perceive global regulations, such as the GDPR, to be more effective than Indian data protection laws.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
4. I am aware of the implications of data protection laws on future legal practices.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
5. I feel adequately prepared to address legal cases involving data privacy in my future legal career.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
6. I believe non-personal data should be subject to specific legal regulations.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
7. Specialized courses on non-personal data laws should be incorporated into law school curricula.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree

8. I believe legal practitioners require enhanced awareness regarding non-personal data governance.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
9. Non-personal data should be regulated under a distinct legal framework separate from personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
10. I understand that personal privacy is a fundamental right under Indian law.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
11. I believe data privacy will be one of the major legal issues in the future.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
12. Have you studied data protection and privacy laws as part of your curriculum?
Options: Yes / No
13. Are you familiar with the legal distinction between personal and non-personal data?
Options: Yes / No
14. Do you know the legal remedies available for breaches of personal privacy?
Options: Yes / No
15. Are you confident in guiding individuals on how to file complaints related to data misuse or privacy violations?
Options: Yes / No

Set 4: Data Professionals (Data Experts, Cyber Experts)

1. I consider Indian regulations sufficient for governing non-personal data usage within the technology sector.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
2. Non-personal data requires distinct legal protections separate from personal data regulations.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
3. There is a need for more comprehensive regulatory frameworks governing non-personal data in India.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree

4. Global standards for non-personal data governance would enhance regulatory consistency and compliance.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
5. In my view, the economic value of non-personal data warrants specific legal consideration.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
6. My professional activities are impacted by the clarity and limitations of Indian data protection laws.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
7. Non-personal data can be anonymized effectively without infringing on individual privacy rights.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
8. I advocate for more transparent government policies on the usage of non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
9. I follow international data protection laws, such as the GDPR, in my work.
Options: Fully Aware / Partially Aware / Not Aware
10. I believe personal privacy as a fundamental right should influence how companies handle personal and non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree
11. Do you work with non-personal data as part of your professional role?
Options: Yes / No
12. Are you familiar with Indian laws governing the regulation of non-personal data?
Options: Yes / No
13. Have you encountered challenges in distinguishing between personal and non-personal data?
Options: Yes / No
14. Have you experienced situations where personal data breaches occurred due to unclear legal regulations?
Options: Yes / No
15. I would support global uniform laws for the handling of non-personal data.
Options: Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree

प्रश्नावली (QUESTIONNAIRE)

सभी समूहों के लिए सामान्य प्रश्न (5 प्रश्न)

1. मुझे डेटा की अवधारणा, जिसमें व्यक्तिगत और गैर-व्यक्तिगत डेटा शामिल है, का व्यापक ज्ञान है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
2. मैं व्यक्तिगत डेटा और गैर-व्यक्तिगत डेटा के बीच स्पष्ट रूप से अंतर कर सकता/सकती हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
3. मैं भारत में डेटा संरक्षण के मौजूदा कानूनी ढांचे के बारे में भली-भांति जानता/जानती हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
4. मेरे विचार में, गैर-व्यक्तिगत डेटा के लिए विशेष कानूनी प्रावधानों का निर्माण आवश्यक है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
5. मेरा मानना है कि डेटा-संबंधी चुनौतियों से निपटने के लिए वैश्विक समान डेटा संरक्षण कानून राष्ट्रीय कानूनों की तुलना में अधिक प्रभावी हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत

समूह 1: विधिक पेशेवर (Legal Professionals)

1. मेरा मानना है कि वर्तमान भारतीय कानूनी ढांचा व्यक्तिगत डेटा से संबंधित चुनौतियों का पर्याप्त रूप से समाधान करता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
2. मेरा मानना है कि मौजूदा भारतीय कानूनी प्रावधान गैर-व्यक्तिगत डेटा के उपयोग और संरक्षण को विनियमित करने के लिए पर्याप्त हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
3. मुझे भारतीय डेटा संरक्षण कानूनों को विधिक कार्यवाहियों में प्रभावी रूप से लागू करने का आत्मविश्वास है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत

4. डेटा-संबंधी मामलों को संभालने में कानून प्रवर्तन एजेंसियों के लिए विशेष विधिक प्रशिक्षण की अत्यधिक आवश्यकता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
5. मैं अंतरराष्ट्रीय डेटा संरक्षण कानूनों, जैसे जीडीपीआर (GDPR), से परिचित हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
6. मेरा मानना है कि मौजूदा भारतीय डेटा संरक्षण कानूनों में गैर-व्यक्तिगत डेटा से संबंधित नई चुनौतियों को ध्यान में रखते हुए संशोधन की आवश्यकता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
7. व्यक्तिगत और गैर-व्यक्तिगत डेटा के बीच का विधिक अंतर कानूनी संदर्भों में पर्याप्त रूप से स्पष्ट है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
8. मेरे विचार में, गैर-व्यक्तिगत डेटा के लिए एक अलग और व्यापक कानूनी ढांचा आवश्यक है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
9. मेरा मानना है कि भारत में विधिक समुदाय गैर-व्यक्तिगत डेटा विनियमों के बारे में पर्याप्त रूप से अवगत है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
10. राष्ट्रीय कानूनी ढांचे भारत में गैर-व्यक्तिगत डेटा से उत्पन्न समस्याओं के समाधान के लिए पर्याप्त हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
11. डेटा-संबंधी विधिक कार्यवाहियों के प्रभावी संचालन के लिए कानून प्रवर्तन एजेंसियों और साइबर विशेषज्ञों के बीच बेहतर सहयोग आवश्यक है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
12. मेरा मानना है कि गैर-व्यक्तिगत डेटा प्रशासन पर अंतरराष्ट्रीय ढांचे को अपनाने से भारतीय कानूनी प्रणाली की प्रभावशीलता बढ़ेगी।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
13. क्या आपने अपने पेशेवर कार्य में डेटा दुरुपयोग या डेटा उल्लंघन से संबंधित मामलों का सामना किया है?
विकल्प: हाँ / नहीं
14. क्या आपने डेटा-संबंधी मुद्दों के मामलों में कोई कानूनी कार्रवाई की थी?
विकल्प: हाँ / नहीं

15. यदि कोई कानूनी कार्रवाई नहीं की गई, तो क्या यह मौजूदा कानूनों की अपर्याप्तता या अस्पष्टता के कारण था?
विकल्प: हाँ / नहीं

समूह 2: आम जनता (General Public)

1. मुझे विश्वास है कि भारतीय कानून मेरे व्यक्तिगत डेटा की पर्याप्त सुरक्षा प्रदान करता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
2. मेरा मानना है कि मौजूदा भारतीय विनियम गैर-व्यक्तिगत डेटा की सुरक्षा के लिए पर्याप्त हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
3. मुझे यह भली-भाँति ज्ञात है कि संगठन गैर-व्यक्तिगत डेटा कैसे एकत्रित और उपयोग करते हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
4. मेरे विचार में, कंपनियों को गैर-व्यक्तिगत डेटा के उपयोग के बारे में अधिक पारदर्शिता बरतनी चाहिए।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
5. मेरा मानना है कि गैर-व्यक्तिगत डेटा को कानूनी ढाँचे के अंतर्गत स्पष्ट रूप से संरक्षित किया जाना चाहिए।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
6. मुझे इस बात की चिंता है कि संगठन मेरे व्यक्तिगत और गैर-व्यक्तिगत डेटा का उपयोग किस प्रकार करते हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
7. डेटा सुरक्षा सुनिश्चित करने के लिए वैश्विक समान कानून आवश्यक हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
8. मैं व्यक्तिगत और गैर-व्यक्तिगत डेटा के उपयोग को नियंत्रित करने के लिए अधिक कठोर राष्ट्रीय कानूनों के कार्यान्वयन का समर्थन करता/करती हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत

9. क्या आपने व्यक्तिगत रूप से डेटा गोपनीयता या दुरुपयोग (जैसे पहचान की चोरी या डेटा उल्लंघन) से संबंधित कोई समस्या अनुभव की है?
विकल्प: हाँ / नहीं
10. क्या आपने डेटा-संबंधी समस्या का सामना करने पर कोई कार्रवाई (जैसे शिकायत दर्ज करना) की थी?
विकल्प: हाँ / नहीं
11. यदि कोई कार्रवाई नहीं की गई, तो क्या यह अस्पष्ट या अपर्याप्त कानूनी प्रावधानों के कारण था?
विकल्प: हाँ / नहीं
12. क्या आप जानते हैं कि भारतीय कानून के तहत व्यक्तिगत गोपनीयता को एक मौलिक अधिकार के रूप में मान्यता प्राप्त है?
विकल्प: हाँ / नहीं
13. क्या आप जानते हैं कि यदि आपकी व्यक्तिगत गोपनीयता का उल्लंघन होता है तो आपके लिए कौन से कानूनी उपाय उपलब्ध हैं?
विकल्प: हाँ / नहीं
14. क्या आप जानते हैं कि डेटा गोपनीयता के उल्लंघन की स्थिति में किन प्राधिकरणों (जैसे पुलिस, उपभोक्ता अदालतें, साइबर सेल) से संपर्क करना चाहिए?
विकल्प: हाँ / नहीं
15. क्या आप यह समझते हैं कि व्यक्तिगत डेटा के दुरुपयोग से संबंधित शिकायत दर्ज करने की प्रक्रिया क्या है?
विकल्प: हाँ / नहीं

समूह 3: विधि विद्यार्थी (Law Students)

1. मेरा मानना है कि विधि शिक्षा में गैर-व्यक्तिगत डेटा कानूनों का अधिक व्यापक अध्ययन शामिल किया जाना चाहिए।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
2. मुझे विश्वास है कि भारतीय कानून गैर-व्यक्तिगत डेटा के उपयोग को पर्याप्त रूप से नियंत्रित करता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत

3. मैं यह मानता/मानती हूँ कि जीडीपीआर जैसे वैश्विक विनियम भारतीय डेटा संरक्षण कानूनों की तुलना में अधिक प्रभावी हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
4. मैं डेटा संरक्षण कानूनों के भावी विधिक अभ्यास पर प्रभावों से अवगत हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
5. मैं भविष्य में डेटा गोपनीयता से संबंधित मामलों को संभालने के लिए पर्याप्त रूप से तैयार महसूस करता/करती हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
6. मेरा मानना है कि गैर-व्यक्तिगत डेटा को विशेष कानूनी प्रावधानों के तहत विनियमित किया जाना चाहिए।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
7. गैर-व्यक्तिगत डेटा कानूनों पर विशेष पाठ्यक्रमों को विधि विद्यालय के पाठ्यक्रम में शामिल किया जाना चाहिए।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
8. मैं यह मानता/मानती हूँ कि विधिक पेशेवरों को गैर-व्यक्तिगत डेटा प्रशासन के संबंध में अधिक जागरूकता की आवश्यकता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
9. गैर-व्यक्तिगत डेटा को व्यक्तिगत डेटा से अलग कानूनी ढांचे के अंतर्गत विनियमित किया जाना चाहिए।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
10. मैं समझता/समझती हूँ कि व्यक्तिगत गोपनीयता भारतीय कानून के तहत एक मौलिक अधिकार है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
11. मेरा मानना है कि डेटा गोपनीयता भविष्य के प्रमुख विधिक मुद्दों में से एक होगा।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
12. क्या आपने अपने पाठ्यक्रम में डेटा संरक्षण और गोपनीयता कानूनों का अध्ययन किया है?
विकल्प: हाँ / नहीं
13. क्या आप व्यक्तिगत और गैर-व्यक्तिगत डेटा के बीच विधिक भेद से परिचित हैं?
विकल्प: हाँ / नहीं

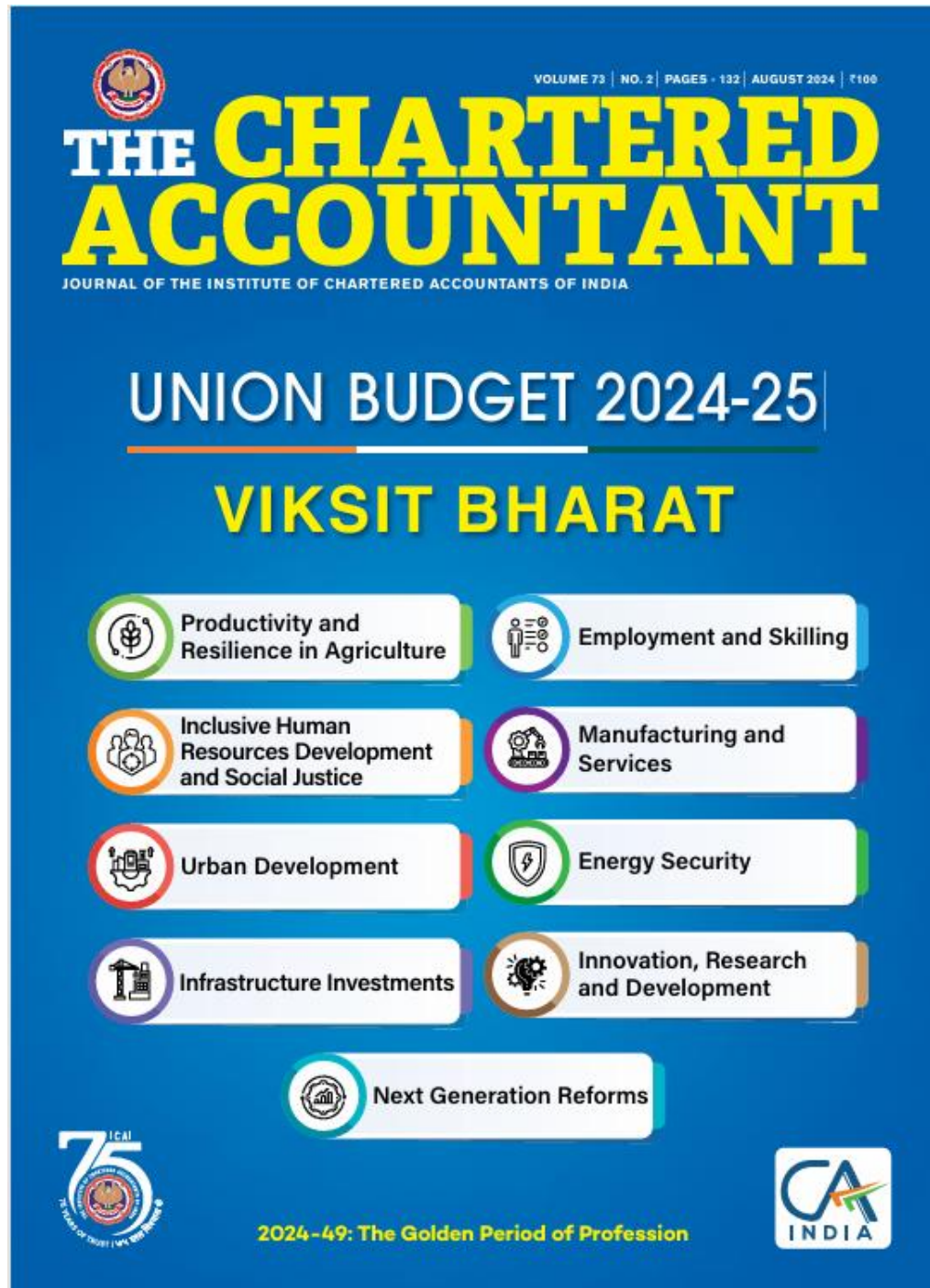
14. क्या आप व्यक्तिगत गोपनीयता के उल्लंघन के लिए उपलब्ध कानूनी उपायों के बारे में जानते हैं?
विकल्प: हाँ / नहीं
15. क्या आप डेटा दुरुपयोग या गोपनीयता उल्लंघन से संबंधित शिकायत दर्ज करने के बारे में व्यक्तियों का मार्गदर्शन करने में सक्षम हैं?
विकल्प: हाँ / नहीं

समूह 4: सूचना प्रौद्योगिकी पेशेवर (IT Professionals)

1. मेरा मानना है कि भारतीय विनियम तकनीकी क्षेत्र में गैर-व्यक्तिगत डेटा के उपयोग को नियंत्रित करने के लिए पर्याप्त हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
2. गैर-व्यक्तिगत डेटा को व्यक्तिगत डेटा विनियमों से अलग कानूनी संरक्षण की आवश्यकता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
3. भारत में गैर-व्यक्तिगत डेटा के लिए अधिक व्यापक नियामक ढांचे की आवश्यकता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
4. गैर-व्यक्तिगत डेटा प्रशासन के लिए वैश्विक मानक नियामक स्थिरता और अनुपालन को बढ़ावा देंगे।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
5. मेरे विचार में, गैर-व्यक्तिगत डेटा का आर्थिक मूल्य विशेष कानूनी विचार की मांग करता है।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
6. मेरी व्यावसायिक गतिविधियाँ भारतीय डेटा संरक्षण कानूनों की स्पष्टता और सीमाओं से प्रभावित होती हैं।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
7. गैर-व्यक्तिगत डेटा को इस प्रकार अनाम किया जा सकता है कि वह व्यक्तिगत गोपनीयता अधिकारों का उल्लंघन न करे।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत

8. मैं गैर-व्यक्तिगत डेटा के उपयोग पर अधिक पारदर्शी सरकारी नीतियों की वकालत करता/करती हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
9. मैं अपने कार्य में जीडीपीआर जैसे अंतरराष्ट्रीय डेटा संरक्षण कानूनों का पालन करता/करती हूँ।
विकल्प: पूर्णतः जागरूक / आंशिक रूप से जागरूक / अनजान
10. मेरा मानना है कि व्यक्तिगत गोपनीयता को मौलिक अधिकार के रूप में मान्यता मिलने से कंपनियों को व्यक्तिगत और गैर-व्यक्तिगत डेटा के साथ अधिक जिम्मेदारी से व्यवहार करना चाहिए।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत
11. क्या आप अपने पेशेवर कार्य में गैर-व्यक्तिगत डेटा के साथ काम करते हैं?
विकल्प: हाँ / नहीं
12. क्या आप गैर-व्यक्तिगत डेटा के विनियमन से संबंधित भारतीय कानूनों से परिचित हैं?
विकल्प: हाँ / नहीं
13. क्या आपको व्यक्तिगत और गैर-व्यक्तिगत डेटा के बीच अंतर करने में किसी चुनौती का सामना करना पड़ा है?
विकल्प: हाँ / नहीं
14. क्या आपने ऐसे मामले देखे हैं जहाँ अस्पष्ट कानूनी विनियमों के कारण व्यक्तिगत डेटा उल्लंघन हुए हों?
विकल्प: हाँ / नहीं
15. मैं गैर-व्यक्तिगत डेटा के प्रबंधन के लिए वैश्विक समान कानूनों का समर्थन करता/करती हूँ।
विकल्प: पूर्णतः सहमत / सहमत / तटस्थ / असहमत / पूर्णतः असहमत

PUBLICATIONS



THE CHARTERED ACCOUNTANT

JOURNAL OF THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

SPECIAL WRITE-UP

- 265** The Accounting Profession's Role in Economic Growth: Potential, Challenges, and Opportunities
-Prof. Dale Pinto
- 268** Building Tomorrow's Profession
-Malcolm Baschus
- 270** The importance of developing Sustainability Reporting Standards for the Public Sector
-Ian Carruthers
- 272** Technology to drive innovation in firms of the future
-Vincent Mathole
- 275** The Evolution and Future of the Accounting Profession
-Soo Hoo Khoo Yuen
- 277** Gen AI - Complementing Skillsets of Finance Professionals
-CA Samir Sekharia
- 280** Sustainable Business, Sustainable Growth
-CA Supratim Dutta
- 283** Startups for Viksit Bharat - Building a Developed India by 2047
-CA Nivad Karpe
- 286** Capital Markets: Catalysts for India's Economic Transformation
-CA Sunil Singhania
- 290** Youth Entrepreneurship: Driving India's Development
-CA Siddharth Pai
- 293** The Path to a \$30 Trillion Economy: Chartered Accountants as Architects of India's Future
-CA Aman Gupta



CA CONNECT

- 294** Listing of members and Firms - Ethical issues and CA Connect Portal
-CA (Dr.) Anuj Goyal



CORPORATE GOVERNANCE

- 297** Enhancing Corporate Governance through Non-Personal Data
-Dr. Kuldeep Singh Panwar
-Jaishree Gaur

ICAI NEWS

- 321** Certificate Course on Concurrent Audit of Banks
- 321** CA Foundation Examination Result
- 322** CA Final Examination Result
- 322** CA Intermediate Examination Result
- 323** Invitation for empanelment as Examiners for Chartered Accountants Examinations
- 325** Campus for Newly Qualified Chartered Accountants (NQCA)

SUBSCRIPTION RATES

Inland subscribers	₹ 1,000 per annum
Overseas	\$170 per annum (subscribers by air mail)
For Overseas Members/Subscribers	
• Air Mail Surcharge	₹ 5,400 per annum
CA Students	₹ 1,400 for 3.5 years
	₹ 400 per annum
Other students & faculties	₹ 600 per annum

CLASSIFIEDS

Minimum ₹ 2,000/- for the first twenty five words or part thereof and ₹ 500/- for five words or part thereof over and above first twenty five words.

Please contact: The Journal Section at ICAI Bhawan, Indraprastha Marg, New Delhi 110 002 or call at +91-11-32110472 or e-mail at ejournal@icai.in

EDITORIAL SUPPORT & DESIGN

Druck Media Private Limited
Plot No. 8 Udyog Vihar, Greater Noida, Uttar Pradesh, India- 201306
ICAI RESERVES THE RIGHT TO REJECT ADVERTISEMENTS.

Printed and published by Jai Kumar Batra on behalf of The Institute of Chartered Accountants of India (ICAI)

Editor - CA. Ranjeet Kumar Agarwal

Published at The Institute of Chartered Accountants of India, I.P. Marg, New Delhi - 110002 and printed at Druck Media Private Limited, Plot No.8, Udyog Vihar, Greater Noida, Uttar Pradesh, India- 201306

The views and opinions expressed or implied in THE CHARTERED ACCOUNTANT are those of the authors and do not necessarily reflect those of ICAI. Unsolicited articles and transparencies are sent in at the owner's risk and the publisher accepts no liability for loss or damage. Material in this publication may not be reproduced, whether in part or in whole, without the consent of ICAI.

DISCLAIMER: The ICAI is not in any way responsible for the result of any action taken on the basis of the advertisements published in the Journal. The members, however, may bear in mind the provisions of the Code of Ethics while responding to the advertisements.

Total Circulation: 74,366

Total No. of Pages: 132 including Covers

E-Journal circulation (Soft copy): 4,11,493

Enhancing Corporate Governance through Non-Personal Data



Dr. Kuldeep Singh Panwar
Academician

The article aims to explore the role of Non-Personal Data in shaping Corporate Governance in India, emphasizing its transformative impact on decision-making, risk management, and strategic planning. It highlights the importance of emerging technologies and robust governance frameworks for utilizing Non-Personal Data effectively. Real-world examples illustrate its diverse applications and address associated challenges. The article concludes by asserting that Non-Personal Data will be a valuable asset for enhancing corporate governance practices.

In today's interconnected and rapidly evolving business landscape, the role of data in shaping Corporate Governance practices cannot be underestimated. With the proliferation of digital technologies and the exponential growth of data sources, corporations are increasingly reliant on data-driven insights to navigate complex challenges, mitigate risks, and seize opportunities for growth. At the heart of this data-driven revolution lies Non-Personal Data, a vast reservoir of information encompassing financial metrics, market trends, operational performance indicators, and more.

Non-Personal Data serves as a cornerstone of Corporate Governance, providing decision-makers with invaluable insights into the internal workings of their organizations and the external forces shaping their industries. Unlike personal data, which is subject to stringent privacy regulations and ethical considerations, Non-Personal Data offers a wealth of information that can be analyzed, interpreted, and utilized to drive informed decision-making processes.

The significance of Non-Personal Data in Corporate Governance is multifaceted. From facilitating



Jaishree Gaur
Research Scholar





VOLUME 73 | NO. 6 | PAGES - 132 | DECEMBER 2024 | ₹100

THE CHARTERED ACCOUNTANT

JOURNAL OF THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

ICAI

WOFA

WORLD FORUM
OF ACCOUNTANTS | 31ST JAN - 2ND FEB 2025
NEW DELHI, INDIA

Accountability Meets Innovation (AI): For A Sustainable Planet



2024-49: The Golden Period of Profession



THE CHARTERED ACCOUNTANT

JOURNAL OF THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

VOLUME 73 (NO. 4) 2023 132 PAGES 2023 ₹ 100



BANKING

- 797** Unveiling Asset Quality Metrics of Banks: Exploring the Myth of Net NPA Ratio and Dispelling Provisioning Misconceptions
- *Dr. J. Madegonda & Dr. Indira P.M. Gowda*
- 803** Asset Liability Management (Liquidity Risk and Interest Rate Risk in Banking Book (IRBB)) in the bank - Why does it matter more today than ever
- *CA. Anicy Harware*



FINANCE

- 808** Strategic Finance: Unveiling the Multifaceted Role of Today's CFO
- *CA. Tejas Savde*

INSURANCE

- 814** Navigating Uncharted Waters: A Deep Dive into Overlooked Territories of Insurance Management
- *CA. Nagesh Mayakumtha*

MSME

- 818** Demystifying Section 43B(h): A Deep Dive into Micro and Small Enterprises Payment Compliance
- *CA. Heman Ujjainwala*

MANAGEMENT

- 824** The Wheel of Happiness- Finding our purpose at work as CAs: A perspective on Positive Organizational Behaviour
- *CA. Tilottama Tarafdar*

TECHNOLOGY

- 829** Understanding Application of Predictive Analytics to Finance Functions using Non-Personal Data
- *Dr. Kuldeep Singh Panwar & Jaishree Gaur*

ARTIFICIAL INTELLIGENCE

- 834** AI-driven innovations in auditing: A comprehensive exploration
- *CA. Deepak Rathore*
- 840** Navigating the Nexus of AI and Behavioural Decision-Making
- *CA. Dipak Kumar Singh*



LEADERSPEAK

- 846** Excerpts of the Address by Hon'ble Shri Justice Dipak Misra, Former Chief Justice of India on "Improving engagement across stakeholders" on the occasion of 8th Foundation Day of Indian Institute of Insolvency Professionals of ICAI (IIPI)
- *Shri Dipak Mishra*

For Overseas Members/Subscribers

- Air Mail Surcharge : ₹ 5,400 per annum
- CA Students : ₹ 1,400 for 3.5 years
- Other students & faculties : ₹ 400 per annum

CLASSIFIEDS:

Minimum ₹ 2,000/- for the first twenty five words or part thereof and ₹ 500/- for five words or part thereof over and above first twenty five words. Please contact: The Journal Section at ICAI Bhawan, Indraprastha Marg, New Delhi 110 002 or call at +91-11-30110472 or e-mail at sboard@icai.in

EDITORIAL SUPPORT & DESIGN

Druck Media Private Limited
Plot No. 8 Udyog Vihar, Greater Noida, Uttar Pradesh, India- 201306
ICAI RESERVES THE RIGHT TO REJECT ADVERTISEMENTS.
Printed and published by Jai Kumar Bhatia on behalf of
The Institute of Chartered Accountants of India (ICAI)
Editor - CA. Paragat Kumar Agarwal

Published at The Institute of Chartered Accountants of India, 1, P. Marg, New Delhi - 110002 and printed at Druck Media Private Limited, Plot No.8, Udyog Vihar, Greater Noida, Uttar Pradesh, India- 201306

The views and opinions expressed or implied in THE CHARTERED ACCOUNTANT are those of the authors and do not necessarily reflect those of ICAI. Unsolicited articles and transparencies are sent in at the owner's risk and the publisher accepts no liability for loss or damage. Material in this publication may not be reproduced, whether in part or in whole, without the consent of ICAI.

DISCLAIMER: The ICAI is not in any way responsible for the result of any action taken on the basis of the advertisements published in the Journal. The members, however, may bear in mind the provisions of the Code of Ethics while responding to the advertisements.

Total Circulation: 71,262
Total No. of Pages: 132 including Covers
E-Journal circulation (Soft copy): 4,29,990

Understanding Application of Predictive Analytics to Finance Functions using Non-Personal Data



Dr. Kuldeep Singh Panwar
Academician

This article explores the application of predictive analytics in finance functions including Chartered Accountancy, focusing on the utilization of non-personal data. It examines how non-personal data can enhance financial forecasting, risk management, and strategic planning. By integrating non-personal data into predictive models, Chartered Accountants can achieve more accurate financial insights and improve decision-making. Case studies illustrate the practical applications of non-personal data in financial services, demonstrating improved accuracy in forecasting and risk assessment. The findings underscore the transformative potential of predictive analytics in accounting, emphasizing the importance of adopting data-driven approaches to navigate the complexities of the financial landscape.



Jaishree Gaur
Research Scholar

Introduction

Predictive analytics is a branch of advanced analytics that utilizes historical data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on past data. Unlike traditional descriptive analytics, which focuses on what has already happened, predictive analytics aims to forecast future events, behaviors, or trends. It plays a pivotal role in enabling organizations to make informed decisions by providing actionable insights that anticipate potential scenarios.

In the modern business landscape, where competition is fierce, risks and future events are uncertain, and the volume of data generated is immense, predictive analytics has become a key differentiator. Businesses today operate in an

environment where uncertainty is constant, and the ability to predict outcomes is crucial for strategic planning. Predictive analytics helps organizations to harness the power of their data, allowing them to foresee risks, optimize operations, enhance customer experiences, and increase profitability.

For instance, in customer relationship management, predictive analytics is used to identify potential churn, allowing companies to take proactive measures to retain customers. In finance & banking, it aids in credit scoring, fraud detection, and risk management by analyzing patterns and trends that may indicate future financial threats. In supply chain management, it helps optimize inventory levels by predicting

BOOK CHAPTER



ANNEXURE III

PRESENTATIONS



Indian Council of
Social Science Research



ICSSR- NEW DELHI sponsored Two Days National Seminar
On
**ANTHROPOLOGY IN THE 21ST CENTURY: EMERGING AREAS OF RESEARCH IN
NORTHEAST INDIA AND ITS ROLE IN NATIONAL DEVELOPMENT**

19th and 20th March, 2024

Organized by

Department of Anthropology, Nagaland University (A Central University)

HQRS: ULUMAM, DIST: ZUNHEBOTO, NAGALAND. PIN-798627

Certificate of Academic Participation and Vigna Recognition



This is to appreciate the participation of Mr./Ms. Dr. MAISAREE CHUR

of Law, Nagaland University

in the seminar and acknowledge his/her contribution in presenting the paper. The above his/her presentation was Beyond the

Pandemic in the Post-Covid era.

Maithuwie

Maithuwie
Prof. M. S. Rawat
Dean, School of Sciences
Nagaland University

Prof. Sonamrath Bhattacharjee
Vice-Chancellor and Head
Department of Anthropology
Nagaland University



Ref. SATLC25/FPP/016



South Asian Technology Law Conclave, 2025

Certificate of Presentation

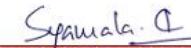
THIS IS TO CERTIFY THAT

Jaishree Gaur

from *Nagaland University, Lumami*, has successfully presented a paper titled *"Invisible Boundaries: Regulating Non-Personal Data in AI-Enabled Health Technologies in India"* in the *South Asian Technology Law Conclave, 2025 (SATLC 2025)*, Organised by the *Centre for Development of Intellectual Property and Research, Naovina Development of Intellectual Property and Research Foundation* as on May 30, 2025.


Mr. Dipendu Das
Director, CDIPR




Prof. (Dr.) Syamala Kandadai
Dean of Faculty, NUSRL Ranchi



Berkeley Stanford