The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Understanding 'Legal Obligation' as a Ground for Data Processing under DPDPA 2023

Isha Pimpalikar

INTRODUCTION:

The rise of technological infrastructure has developed the cyberworld, where information acts as the heartbeat of this world. In every fraction of a second, data is uploaded, stored, analyzed, and processed. The emergence of cyberspace has an indispensable impact our real world. We have lost track of how much cyberspace knows about us and how much of our data is widely shared and analyzed. Once data is entered into cyberspace, it travels at lightning speed, leaving us with little control over it. It often feels as though our personal information ceases to be ours, becoming accessible and readable by anyone. This results in a loss of control, privacy, and security over our data.

Figure 1: AI-generated illustration depicting a futuristic cyber world filled with personal data streams and

With such plethora of identifiable information available, questions arise about whether this excessive sharing and analysis of data poses a threat. India has introduced the Data Protection and Digital Privacy (DPDP) Act of 2023[1] to answer the question of data threats. This legislation aims to address these risks by filling gaps in data protection and securing the processing of personal information. Additionally, it assists in erasing digital footprints, thereby enhancing control over one's data.

WHAT IS PERSONAL DATA AND NEED FOR PROCESSING?

Any data or information that identifies with a living person, a specific living person is a personal data. This could be bits and pieces of information that is brought together, analysed for such identification.

[1] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).

Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the General Data Protection Regulation[2] (GDPR), the EU's main data protection law.

EXAMPLES OF PERSONAL DATA INCLUDE:

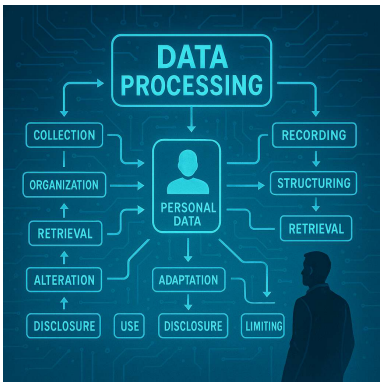


Figure 2: AI-generated illustration visualizing the stages and roles involved in personal data processing.

Data processing is anything that touches upon personal data. So, for instance, it covers the collection, recording, organization, structuring, storage, alteration or adaptation, retrieval, consultation, use-disclosure via transmission, distribution, or otherwise aligning or combining this with limiting, deleting or destroying personal data. Processing personal data may be done by individuals or private or public entities such as businesses or government agencies. Then, their obligations and liability for specific data processing depend on the role they play in the concerned processing. Data processing involves collecting and amending bits of digital data so that they will be able to form meaningful information. Data processing is one of the types of information transformation, generally described as any way by which information is changed so that anybody watching can note that something changes.

WHAT IS THE GROUND FOR PROCESSING DATA[3]?

As per Section 4 the DPDP Act, 2023:

[2] 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, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1

[3] Privacy International, Grounds for Processing of Personal Data (Part 5), in A Guide for Policy Engagement on Data Protection (2018).

(1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,— (a) for which the Data Principal has given her consent; or (b) for certain legitimate uses.

(2) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.

Consent: Consent is an act of affirmation given to do a particular act. In a data sense, assent given by the Data Principal to analyse and process data is consent.

Figure 3: AI-generated illustration portraying the formal process of a Data Principal voluntarily sharing financial data for a loan application in a bank setting.

Legitimate Purposes/ Lawful purposes: Data can sometimes be processed without consent. Therefore, it should be obligatory that all the Data Processors comply with the rules and acts. The purpose for processing should not be expressly forbidden by any law. It also includes retention of data after the purpose is satiated in certain cases due to legal obligation of some other acts.

For Eg: When applying for a loan, the Data Principal voluntarily provides bank account information, tax returns, and other financial documents for analysis to determine their creditworthiness. This act of sharing personal data is done willingly by the Data Principal.

Illustration: The definition of intermediaries according to IT Act, 2000, 'intermediaries' are those who hold or make information in electronic form or use a computer resource to transmit that information. This would include such platforms like messaging platforms or internet service providers that keep users' logs and information made available to them for a fixed period as prescribed by the government. For instance, when a user is reported for cyberbullying, a platform must save certain metadata for example, IP Addresses, login times, message timestamps and so on. Sharing this information with law enforcement is possible even without user consent upon an official request. This section of law, besides being a legal obligation, will also support the processing of data without consent for compliance with laws under the provisions of DPDPA 2023.

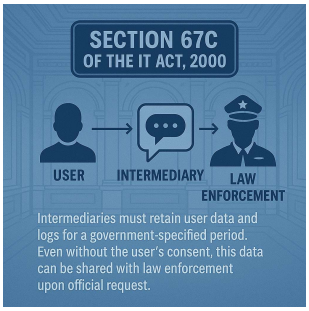
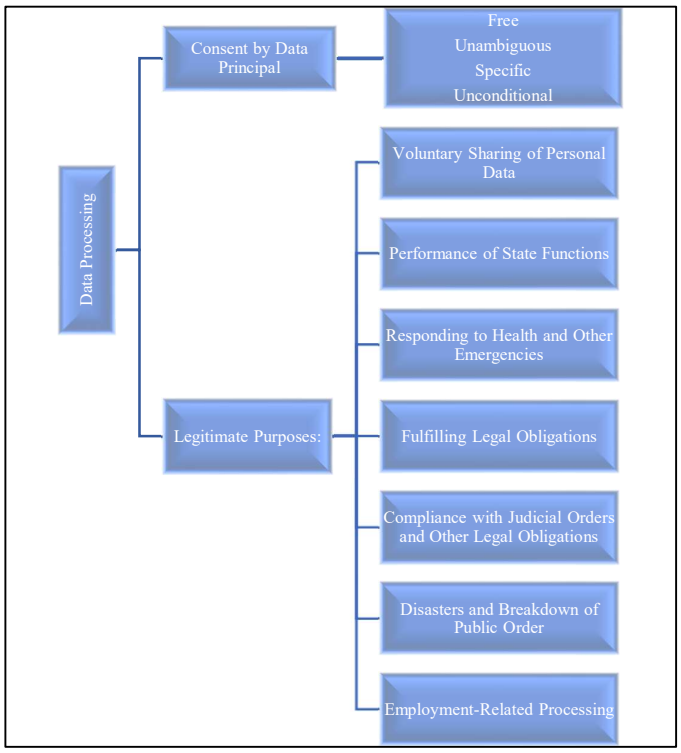


Figure 4: AI-generated illustration depicting legal obligations

UNDERSTANDING LEGAL OBLIGATION

The English word "obligation" derives from the Latin word ***obligare***, from the root lig-, meaning "to bind" or "tie." Savigny, the great classical thinker in law, described an obligation

as a certain form of control over an individual's specific act, not regarding the entire person: *"an act subtracted from their free will and subjected to another's will.*[4]*"*



The globalization of commerce and the digital ecosystem have transformed the significance of legal obligation as a concept, with repercussions for areas such as cross-border data supply and technological compliance. These transformations have consequently produced added challenges for enforcement and interpretation of norms, notably concerning data protection, consumer rights, and environmental accountability.

In that sense, legal obligation is one of the lawful grounds for processing personal data without consent under India's Digital Personal Data Protection Act (DPDPA) 2023. According to Section 7(1)(b) and 7(1)(c) of the Act, the processing of personal data is valid if:

- It is necessary to an obligation under any current law of India requiring a disclosure of such information to the State or its instrumentalities.
- It is needed for compliance with decrees, judgments, or orders under Indian laws or those of foreign courts in civil or contractual matters.

This legal regime shall ensure that such data fiduciaries are not prevented from discharging their duties under statute or court orders by the consent prescriptions. Such processing, however, must still be proportionate, necessary, and otherwise compliant with data protection provisions avoiding misuse or overreach.

WHAT ARE LEGAL OBLIGATIONS THAT REQUIRE RETENTION OF DATA?

[4] Liad Mudrik & Adina Roskies, Free Will Without Consciousness?, 26 Trends in Cognitive Sciences 525 (2022)

Having data retention policies is important for all organizations, whether small or large. These policies include how long data will be kept, how it will be managed, and when it will be securely discarded. An explicit and working data retention policy is an absolute must in our increasingly data-driven world. The retention of data is insisted upon by the law, which includes requirements for its retention for any amount of time for investigations, verification for law enforcement purposes, or simply because the company requires that data to do its work. In this case, if the restrictions of DPDPA and Draft DPDP Rules state that data must be kept for a specified period, this is pretty much where such requirements come in. Such practice helps law enforcement gain access to vital data in investigations, while at the same time, ensuring data usability for the benefit of business and data-driven insights.

Income Tax Act, 1961	6 years	Tax returns, financial records, books of accounts	Any person filing tax return
Goods and Services Act, 2017	6 years	GST invoices, returns, and records	Any person filing tax return
Companies Act, 2013	4 years	Books of accounts and vouchers	Company
	8 years	Annual returns (Section 92), certificates and documents	Company
	15 years	Register and index of debenture holders	Company
	Permanent	Register of members of company	Company Secretary or authorized person
Prevention of Money Laundering Act, 2002	5 years	Financial transactions, customer ID records, suspicious reports	Banks, financial institutions, reporting entities
Foreign Exchange Management Act, 1999	5 years	Records of foreign exchange transactions	Entities in foreign exchange

Banking Regulation Act, 1949	1 year	Credit card transactions	Banks, financial institutions
	5 years	Books of accounts	Banks
	7 years	Loan documents	Banks
	8 years	Books of accounts	Banks
Information Technology Act, 2000	60 days	User registration information	Intermediary
	180 days	Content transmitted on platforms	Intermediary
Aadhaar Act, 2016	6 months	Authentication records	Registered entities, service providers
	5 years	Meta data	Registered entities
Telecommunications Act, 2023	2 years	Call Data Records (CDR), Event Data Records (EDR), IP Data Records (IPDR)	Telecom service providers
CERT-In Guidelines, 2022	180 days	Logs of ICT systems	Service providers, intermediaries, data centres, corporates
SEBI Act, 2002	5 years	Transaction records	SEBI-regulated entities
	8 years	Board-approved documents	SEBI-regulated entities
RBI Master Circular on AML, 2013 / KYC Directions, 2016	10 years	Transaction records	NBFCs, MNBCs, RNBCs

IFSC (Payment Services) Regulations, 2024	10 years	Log of transactions	Payment service providers in IFSC
Public Records Act, 1993	3, 5, 10 years	Public records per category	Government/public authorities
Right to Information Act, 2005	20 years	Public records	Govt. bodies
Ministry of Civil Aviation Guidelines, 2014	3, 5, 10, 25 years	Public records	Civil Aviation departments
Minimum Wages Act, 1948	Permanently	Employee details: hours, wages, receipts	Employers under the Act
Medical Council of India Act, 1956	Lifetime of patient	Medical records per rules	Doctors
	3 years	Outpatient department (OPD) records	Doctors
Electronic Health Records Standards, 2016	Lifetime of patient	Electronic medical records	Doctors, healthcare institutions

CONCLUSION

Legal obligation serves as a legal framework that brings order within chaotic contexts where consent-centric models thrive and forms the basis of a legal boundary in a fluid situation. The framework suggests the '2023 Digital Personal Data Protection Act' is correct in stating that not all data processing can rely on consent, especially in matters concerning the State's functions, legal compliance, or the public interest. In section 7, the law operationalizes this by creating specific lawful bases for consent-less data processing, more so under statutory, judicial, or regulatory mandates.

This recognition has not been made lightheartedly nor constitutes a concession. It is a constitutional balancing act within an individual's legal order to exercise autonomy along with

the collective legal order. As a case in point, a bank abiding by the aid of anti-money laundering laws, a hospital maintaining e-health services for regulatory audits, or an intermediary maintaining logs for cybercrime support investigations all showcase the sole legal obligation ground that ensures data processors are not trapped amid a web of legislative dependencies.

Nonetheless, legal boundaries do not imply a free pass. Even with such borders, all other boundaries on reasonability in legal obligation of processing must be satisfied, which are proportionality, necessity and limitation of purpose.

EXTRA REFERENCES

1. *Data Protection Explained*, Eur. Comm'n, https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.

2. The Digital Personal Data Protection Act, 2023, No. 22 of 2023.

3. LAW Notes, *Jurisprudence is Define a Obligation*, https://lawnotes.co/tag/jurisprudence-is-define-a-obligation/

4. 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, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 5, 2016 O.J. (L 119) 1, https://gdpr-info.eu/art-5-gdpr/