INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

India

Introduction about the Firm

Ahlawat & Associates ("A&A") is one of the leading full-service law firms in India, catering both to domestic and international clients.

Incorporated in 1978 as primarily a litigation practice, A&A has steadily broadened its scope of expertise and services through addition of new partners (in varied practice areas), emerging as one of the leading law firms in India. Our firm provides comprehensive counsel on various legal services such as mergers and acquisitions, private equity, real estate, education, intellectual property, media and entertainment, technology, online gaming, sports, data protection and privacy, virtual digital assets, employment, labor, licensing and registration, taxation (direct and indirect), and business setup (globally). With numerous attorneys in the firm possessing knowledge and experience across various fields of law, A&A is equipped to handle diverse legal requirements of our clients worldwide.

Our services extend through diverse sectors of industry to facilitate foreign direct investments and business setup in India. A&A has assisted and continues to assist clients from over 20 jurisdictions to enter and flourish in India by providing various legal options to best suit their needs. A&A takes pride in being amongst the most sought-after legal service provider globally.

A&A has been one of the leading law firms in the data protection and data privacy sector in India. It has assisted numerous domestic as well as international clients with various legal requirements in this specific legal domain which includes assisting them with compliances under the relevant statutes, drafting of consent notices, preparation of internal data access control mechanisms, drafting of privacy policies, etc. A&A has also been extremely active in submitting inputs and comments to the Government on proposed legislations in this sector.

Contact Us

+91-11-41023400

www.ahlawatassociates.com

gaurav.bhalla@ahlawatassociates.in

Plot No. 66, LGF
#TheHub, Okhla Phase III, Okhla Industrial Estate
New Delhi, 110020 India

Introduction

The legal regime in India relating to data protection and privacy has undergone a significant re-haul and revamp. The Digital Data Protection Act, 2023 ("DPDPA") received the President's assent and was published in the official Gazette in India on August 11, 2023. Even though the DPDPA has been published in the Gazette, the date on which the statute will come into force is yet to be notified by the Government. The PDPA provides for the protection of the individual's rights in relation to their personal data which is in digital form or has been digitized subsequently. It further extends beyond the borders in case processing of personal data occurs outside of India as regards goods or services being provided to persons located in India.

There was an imminent requirement to curb the escalating concerns surrounding data breaches, unauthorized data exchange and absence of robust regulations surrounding processing of personal data of individuals. The enactment of the DPDPA seems to be a positive step taken by the government to address such concerns. While the rules under the DPDPA are yet to be released in the public domain (which will elaborate more on the manner of compliances), the DPDPA (in its current form) seems like an attempt by the government to strike a balance to safeguard the rights of individuals on one hand and at the same time ensuring that corporate entities are not overburdened with compliances.

Governing Data Protection Legislation

2.1. Overview of principal legislation

Since 2011 until 2023, India only had a very basic dedicated legislation covering the arena of data protection and data privacy. This piece of legislation was called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") which was framed under the Information Technology Act, 2000 ("IT Act"). It is only in 2023 that the Central Government enacted the DPDPA, thereby re-hauling and introducing a more comprehensive data protection legislation.

2.2. Additional or ancillary regulation, directives or norms

The regulatory landscape for data protection in India is additionally supplemented by a number of other laws (which are sector-specific). These legislations include Information Technology (the Indian Computer Emergency Response Team and the Manner of Performing Functions and Duties) Rules, 2013 and the Consumer Protection (E-Commerce) Rules, 2020. Further, Reserve Bank of India (RBI) has also prescribed a set of comprehensive guidelines for handling of personal data by banking and financial service institutions.

2.3. Upcoming or proposed legislation (if applicable)

The DPDPA, pursuant to its enactment, will become the principal legislation governing the laws relating to data protection in India. The DPDPA was passed with the objective of providing an effective and robust mechanism for protection of personal data. While the statute has been enacted and published in the official Gazette, it is yet to be notified (subsequent to which it will come into force). Further, the rules under the statute are also yet to be released in the public domain which will provide for the detailed manner in which compliances will be required to be observed.

Scope of Application

3.1. Legislative Scope

3.1.1.Definition of personal data

As per the DPDPA, Data means, 'a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means'. The Act further lays down that any data with which a person is directly or indirectly identifiable is referred to as 'personal data'.

3.1.2.Definition of different categories of personal data

It is pertinent to note that the DPDPA is applicable to the processing of digital personal data wherein the data has been collected in a digital form, or in a non-digital form but has been digitized subsequent to collection. Thus, the DPDPA excludes the data collected in a non-digitized form (which is not digitized subsequently) from its ambit.

3.1.3.Treatment of data and its different categories

- Regulation of personal and non-personal data

The DPDPA does not apply to personal data that is processed for the purpose of any personal or domestic use by an individual. It has been further laid down that it also does not apply to any data that has been made available to the public by either the Data Principal or any other person obligated to do so under any law.

- Regulation of electronic and non-electronic data

The DPDPA provides for the regulation of data that is collected in electronic form and non-electronic form that is subsequently digitized. However, it does not regulate data that is collected in non-electronic form, and isn't digitized subsequently.

3.1.4.Other key definitions pertaining to data and its processing

Other key definitions pertaining to Personal Data and its processing include:

a)Personal Data Breach - Any data that is subjected to unauthorized processing which also includes, accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data would be regarded as a breach of personal data.

b)Processing - Processing of personal data is considered as an operation or set of operations which is performed on digital personal data such as collection, recording, storage, organizing of data, etc.

3.2. Statutory exemptions

The DPDPA provides for certain exemptions wherein the Data Fiduciaries are exempt from specific obligations. These exemptions include instances where processing is essential for legal enforcement or by judicial bodies, for investigation, or processing data of Data Principals outside India based on contractual agreements. Moreover, the law permits the Central Government to exempt state instrumentalities from compliance in the interest of national sovereignty, security, public order, or international relations. It also exempts data processing for research, archival, or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is conducted according to prescribed standards. Additionally, the government has the authority to exempt certain categories of entities from specific obligations outlined in the provisions related to notice, data processing for decision-making, erasure, additional obligations and access to personal data.

3.3. Territorial and extra-territorial application

The DPDPA applies to the processing of personal data within the territory of India as well as the processing of personal data outside India (irrespective of where the Data Fiduciary is located) if such processing is in connection with any activity related to offering of goods or services to Data Principals located within India.

Legislative Framework

4.1. Key stakeholders

Following are the key stakeholders as per the DPDPA:

1. Data Fiduciary – Any individual or entity who is responsible for determining the purpose of processing of personal data.

2. Significant Data Fiduciary - The central government may notify a Data Fiduciary as a significant data fiduciary on the basis of certain factors which may include volume and sensitivity of personal data processed, risk to the right of Data Principal, security of the state, etc.

3. Data Principal - A person whose personal data is being collected for the purpose of processing. The DPDPA also provides for a condition where in case the individual is a child, the definition of Data Principal would further extend to its parents or legal guardians. Further, in case of a disabled person, the definition may extend to its lawful guardian.

4. Data Processor - A person who processes the personal data of the Data Principal on behalf of the Data Fiduciary.

5. Consent Manager - A person who serves as single point of contact for facilitating the process through which a Data Principal can provide, handle, assess, and retract their consent as regards their personal data.

4.2. Role and responsibilities of key stakeholders

A Data Fiduciary is responsible for processing personal data after complying with some primary prerequisites which include obtaining valid consent and giving a notice regarding the same to the Data Principal. As regards the Data Principal, it is their duty to comply with legal requirements while providing verifiable authentic information. Further, they should ensure that they never file a false or misleading grievance/complaint.

Further, it is pertinent to note that a Significant Data Fiduciary is required to additionally undertake certain obligations (in addition to the responsibilities undertaken by a Data Fiduciary) which includes appointing a 'Data Protection Officer'.

As regards the Consent Manager, they play an important role in standardizing consent management process for a Data Fiduciary. Consent Managers shall be accountable to the Data Principals and shall act on their behalf subject to obligations which will be prescribed by the Government.

Requirements for Data Processing

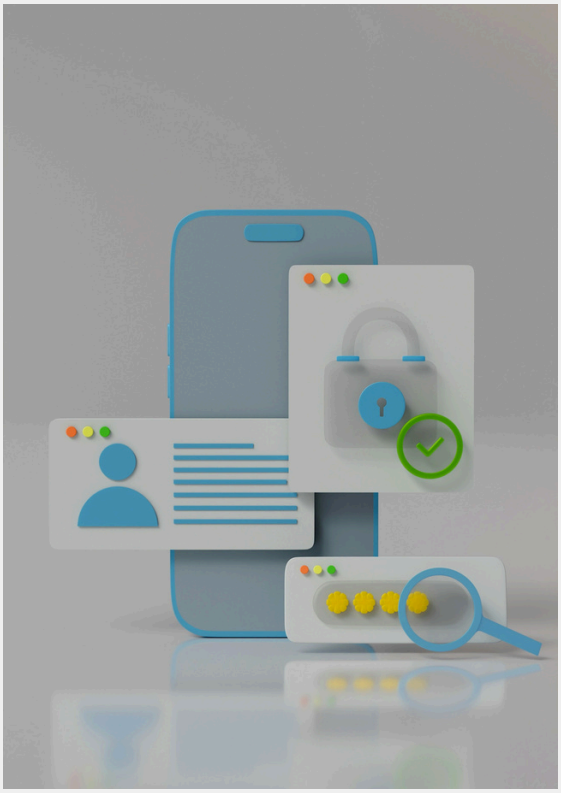
5.1. Grounds for collection and processing

- Consent

A Data Fiduciary is required to obtain consent from the Data Principal prior to collecting Personal Data for the specified purposes and legitimate uses.

- Consent Notice

The Data Fiduciary is obligated to furnish a notice to the Data Principal, comprehensively detailing crucial



information (the manner of which shall be prescribed in the rules). This notice should explicitly outline:

a. the personal data and the purpose for which the same is proposed to be processed.

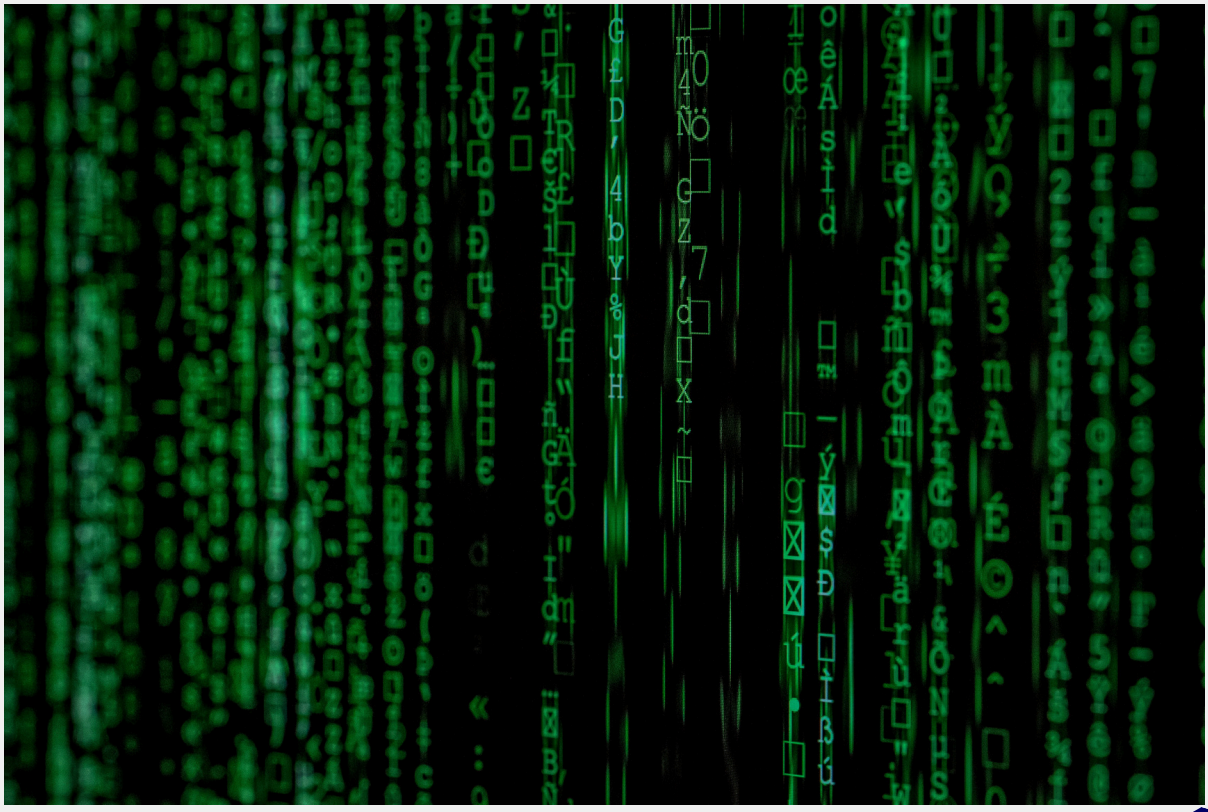
b. the manner in which she may exercise her rights.

c. the manner in which the Data Principal may make a complaint to the Board.

Further, it is important for the Data Principal to ensure that the consent must be freely given, specific, fully informed, unconditional, and unambiguous, requiring a clear affirmative action from the Data Principal. It is crucial that the request for consent and any related information or communication presented to the Data Principal is conveyed in a language that is clear and easily comprehensible. Additionally, it must be ensured that the Data Principal is able to access the request and related information in either English or any other language specified in the Eighth Schedule to the Constitution of India.

- Withdrawal of Consent

It has been further specified that while the consent is the basis of processing of the personal data, the



Data Principal shall also be given the right to withdraw consent at any point of time as easily as the consent was given. However, as regards the withdrawal, it has been further specified that, "such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal". Moreover, such a withdrawal makes it mandatory for the Data Fiduciary to end the processing of the personal data of the Data Principal (unless specifically provided by the DPAPA).

5.2. Data storage and retention timelines

While no specific timelines have been prescribed for the retention of personal data, a Data Fiduciary is required to store personal data of the Data Principal only for specified purposes which indicates that as soon as the specified purpose is over, the personal data shall not be retained.

5.3. Data correction, completion, updating or erasure of data

Upon withdrawal of consent by the Data Principal (even before the completion of the specified purpose of the data collected), the Data Fiduciary and its Data Processors shall erase or cease to process the personal data of the Data Principal within a reasonable time (which is yet be specified by the rules). Further, the Data Principal can request corrections, completion of missing information, or updates to any inaccurate or incomplete data held by a Data Fiduciary.

5.4. Data protection and security practices and procedures

As a general obligation, the Data Fiduciary is mandated to implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.

5.5. Disclosure, sharing and transfer of data

As regards the disclosure, sharing or transfer of personal data of the Data Principal, the DPDPA provides that information regarding the extent and purpose of sharing of the personal data needs to be disclosed to the Data Principal and consent for the same needs to be sought by way of a consent notice.

5.6. Cross border transfer of data

The Central Government has the power to restrict the transfer of personal data by a Data Fiduciary for processing to specific countries or territories outside India by notifying the list of such countries.

5.7. Grievance redressal

A Data Fiduciary or the Consent Manager shall establish an effective and readily available mechanism to redress the grievances of Data Principals in case of any act or omission or regarding the performance of their obligations in relation to the personal data of such Data Principal.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

- Right to withdraw consent

The DPDPA recognizes the right to withdraw consent, in exercise of which, the Data Principal can withdraw consent provided previously for the purpose of processing of their personal data for a specified purpose. It has also been specified that upon withdrawal of consent, the Data Fiduciary and its Data Processors shall cease to process the personal data of the Data Principal within a reasonable time. The ease of exercising the option to withdraw consent shall be comparable to the ease with which consent was originally given.

- Right to grievance redressal and appeal

A Data Principal shall have the right to a means of grievance redressal provided by a Data Fiduciary or a Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of his/her rights.

- Right to access information

The Data Principal can exercise their right of accessing the following information about their personal data:

(1) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data;

(2) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

(3) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.

- Right to nominate

A Data Principal has been conferred the right to nominate any other individual who can exercise the rights of the data principal in the event of death or incapacity of the Data Principal.

6.2. Duties

The Data Principals are required to perform, inter alia, the following duties:

a)to ensure not to impersonate another person while providing his/her personal data;

b)to ensure not to suppress any material information while providing his/her personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;

c)to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board; and

d)to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure.

Processing of Children or Minors' Data

The DPDPA defines a 'child' as an "individual who has not completed the age of eighteen years". As regards processing of personal data relating to children, the DPDPA provides that prior to processing any personal data of a child, the Data Fiduciary shall obtain verifiable consent of the parent of such child. The DPDPA further provides for the following aspects as regards processing of personal data of a child:

i. The Data Fiduciary shall not undertake such processing of personal data which is likely to cause detrimental effect on the well-being of a child.

ii. The Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

The DPDPA provides for formation of the Data Protection Board of India ("Board") which shall inter alia be responsible for adjudication of any complaints with respect to breach of any provisions of the statute. The Board shall consist of a chairperson and such other members as of the Central Government would specify.

8.2. Role, functions and powers of authorities

- Role, functions and powers of principal data regulation authority

The DPDPA has prescribed that the Board shall have the following powers and functions:

a. on receipt of an intimation of personal data breach, to direct any urgent remedial or mitigation measures, and to inquire into such personal data breach and impose penalty.

b. on a complaint made by a Data Principal in respect of a personal data breach or a breach in observance by a Data Fiduciary of its obligations or the exercise of rights by the Data Principal, or on a reference made to it by the Central Government or a State Government, or in compliance of the directions of any court, to inquire into such breach and impose penalty.

c. on a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to their personal data, to inquire into such breach and impose penalty.

d. on receipt of an intimation of breach of any condition of registration of a Consent Manager, to inquire into such breach and impose penalty.

e. on a reference made by the Central Government in respect of the breach by an intermediary, to inquire into such breach and impose penalty.

The Board may also direct the parties to attempt resolution of the dispute through mediation.

- Role, functions and powers of additional or ancillary data regulation authorities (if applicable)

N/A

8.3. Role, functions and powers of civil/criminal courts in the field of data regulation

An appeal from an order of the Board will lie to the Telecom Disputes Settlement and Appellate Tribunal (which has been designated as the Appellate Board under the DPDPA) within a period of 60 days from the date of the order passed by the Board. The Appellate Tribunal has the power to either confirm, modify or set aside the order passed by the Board. The DPDPA mentions that the Appellate Board shall endeavour to dispose of the appeal within six months from the date on which the appeal is presented to it. An appeal from the order of the Appellate Board will lie before the Supreme Court of India.

Consequences of non-compliance

9.1. Consequences and penalties for data breach

The DPDPA prescribes that any breach on the part of the Data Fiduciary to take reasonable security safeguards to prevent personal data breach could result in damages to the tune of INR 250 crores (approx. 33 million USD).

9.2. Consequences and penalties for other violations and non-compliance

The DPDPA also prescribes penalties for various other breaches of the provisions of the statute. These are listed as follows:

i. Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach – Up to INR 250 crores (approx. 33 million USD).

ii. Breach in observance of additional obligations in relation to children - Up to INR 200 crores (approx. 26 million USD).

iii. Breach in observance of additional obligations by a Significant Data Fiduciary - Up to INR 150 crores (approx. 20 million USD).

iv. Breach in observance of the duties by the Data Principal – Up to INR 1000 (approx. 33 USD 12).

v. Breach of any term of voluntary undertaking accepted by the Board – Up to the extent applicable for the breach in respect of which the proceedings were instituted

vi. Breach of any other provision of this Act (or the rules made thereunder) - Up to INR 50 crores (approx. 7 million USD).

Conclusion

The enactment of the DPDPA has been a major positive development in India in the field of data protection. While the statute is yet to be officially notified (subsequent to which it will come into force), businesses in India have already started the process of putting in place policies and mechanisms for observing compliance with the provisions of the statute. The enactment of this statute has put India at par with the other nations in terms of having a robust data protection legislation. Further, the magnitude of penalties (which are much higher than the GDPR) will ensure that businesses will take concrete steps to ensure that they are compliant with the provisions of the statute.

Contact Us

+91-11-41023400

www.ahlawatassociates.com

gaurav.bhalla@ahlawatassociates.in

Plot No. 66, LGF
#TheHub, Okhla Phase III, Okhla Industrial Estate
New Delhi, 110020 India