FAQS ON THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

LexOrbis | Intellectual Property Attorneys & Advocates

PREFACE

The Digital Personal Data Protection Act of 2023 represents a significant milestone in the ongoing evolution of digital privacy and security. The legislation was enacted to address the escalating concerns surrounding the unauthorised use and mishandling of personal data and aims to establish a comprehensive framework for safeguarding individuals' information in the digital realm.

The Act begins by defining the scope of personal data it covers, recognising the expansive nature of digital footprints in contemporary society. The legislation seeks to create a broad and inclusive protective umbrella by adopting a comprehensive definition.

One of the critical features of the Act is that it mandates that, barring some legitimate uses as defined, organisations must obtain explicit and informed consent from individuals before collecting, processing, or sharing their personal data. This shift towards a consent-centric model empowers individuals to exercise greater control over their digital identities, fostering a more transparent and ethical data ecosystem.

Furthermore, the legislation introduces stringent security measures to fortify the storage and transmission of personal data. Companies handling such information are now obligated to implement state-of-the-art encryption protocols and robust cybersecurity measures. The Act recognises that safeguarding personal data is not only a legal obligation but also an ethical imperative in the digital age.

In response to the increasing prevalence of data breaches and cyber-attacks, the Act incorporates provisions for prompt and transparent disclosure. Organisations must promptly notify affected individuals in the event of a data breach, allowing them to take necessary precautions and mitigate potential harm.

The Act also establishes a regulatory body with the authority to enforce compliance and mete out penalties for violations. This enforcement mechanism adds teeth to the legislation, ensuring that organisations have a tangible incentive to adhere to the stipulated guidelines. Penalties may include fines, suspension of data processing activities, or even legal action, depending on the severity of the infringement.

The Digital Personal Data Protection Act, 2023, marks a significant stride towards fortifying the privacy and security of individuals in the digital landscape. By placing user consent at the forefront, bolstering cybersecurity measures, and instituting a robust enforcement framework, the legislation endeavours to strike a delicate balance between fostering innovation and safeguarding personal data.

INDEX

mail@lexorbis.com | www.lexorbis.com

1. What is the current law governing digital personal data in India?

The current law governing digital personal data protection in India is the Digital Personal Data Protection Act, 2023. It will override some of the provisions and rules of the Information Technology Act, 2000.

2. What is the Digital Personal Data Protection Act, 2023 (DPDP Act)?

The Digital Personal Data Protection Act of 2023 (DPDP Act) is an exhaustive legal framework established to regulate the processing of digital personal data. This pertains to data collected either online or offline and subsequently digitised within the territorial boundaries of India. Additionally, the Act applies to processing digital personal data outside Indian territory if it involves providing goods or services to the data principals within India.

3. When was the DPDP Act enacted?

The DPDP Bill was initially presented to the Lok Sabha on August 3, 2023. It was subsequently passed by both the Lok Sabha and Rajya Sabha on August 7 and August 9, 2023, respectively. Finally, the DPDP Act was enacted into law on August 11, 2023, after receiving the President's assent. This legislation, which has been in the works for some time, has now been effectively implemented, bringing about significant changes to the regulatory framework governing data privacy and protection.

4. What is “Personal Data” under the DPDP Act?

“Personal Data” means any data about an individual who is identifiable by or in relation to such data. Further, anonymised data shall not be considered as personal data under the DPDP Act.

mail@lexorbis.com | www.lexorbis.com

5. What does the term “Digital Personal Data” mean as per the DPDP Act?

The DPDP Act defines “Digital Personal Data” as personal data in digital form.

6. What does the term “Data” mean as per the DPDP Act?

As per the DPDP Act, “data” refers to 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.

7. Who is a Data Principal under the DPDP Act?

The term “data principal” denotes the individual to whom personal data relates. In cases where personal data relates to a child, the data principals extend to encompass the parents or lawful guardians of the child. Similarly, when personal data pertains to an individual with a disability, their lawful guardians, acting on their behalf, become data principals.

8. To whom does the Digital Personal Data Protection Act, 2023 apply?

The DPDP Act applies to:

a) the processing of digital personal data within the territory of India where the personal data is collected
   i. in digital form or
   ii. in non-digital form and digitised subsequently,

b) the processing of digital personal data outside the territory of India if such processing is in connection with any activity related to the offering of goods or services to Data Principals within the territory of India.

mail@lexorbis.com | www.lexorbis.com

9. What are the exemptions under the DPDP Act?

The DPDP Act shall not apply to the following:

a) Personal data processed by an individual for any personal or domestic purpose and
b) Personal data that is made or caused to be made publicly available by
    i. the Data Principal to whom such personal data relates; or
    ii. Any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

10. Which activities are regulated by the DPDP Act?

The DPDP Act regulates the processing of personal data, which may include the set of manual or automated operations, wholly or partly for the following activities:

a) Collecting or recording personal data
b) Organising, structuring, indexing, or storing personal data
c) Retrieving or using personal data
d) Adapting, aligning, or combining personal data
e) Sharing or disclosing by transmission, dissemination, or otherwise making personal data available
f) Restricting, erasing, or destructing personal data

11. What are the grounds for processing personal data?

A person may process the personal data of a Data Principal only in accordance with the provisions of this DPDP Act and for a lawful purpose,

a) for which the Data Principal
b) has given her consent or
c) for certain legitimate uses (without consent)

mail@lexorbis.com | www.lexorbis.com

"Lawful purpose" means any purpose which is not expressly forbidden by law.

12. What are the requirements relating to privacy notice to a data principal?

Where the basis is "consent", every request made to a data principal for consent must be accompanied or preceded by a privacy notice given by the data fiduciary to the data principal, informing her as specified under the Act. Such privacy notice must be served to the data principal in writing via letter, fax or email to seek their consent for processing their personal data. The notice must also specify the purpose for which the data needs to be processed by the data fiduciary. Additionally, the privacy notice must be accessible in English or any of the 22 national languages, providing the data principal with a choice to provide consent in their preferred language.

13. What constitutes a "personal data breach" under the DPDP Act, and what are the implications of such a breach?

"Personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data that compromises confidentiality, integrity, or availability of personal data.

14. What are the characteristics of "consent" under the DPDP Act?

a) Consent given by the Data Principal must be free, specific, informed, unconditional and unambiguous with clear affirmative action. It shall signify an agreement to process her personal data for the specified purpose and be limited to such personal data as is necessary for such defined purpose.

mail@lexorbis.com | www.lexorbis.com

b) Consent that constitutes an infringement of the provisions of this DPDP Act, the rules made thereunder, or any other law for the time being in force will be invalid to the extent of such infringement.
c) Every request for consent is required to be presented to the Data Principal in a clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights.
d) Where consent given by the Data Principal is the basis of the processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.

15. What is the meaning of "Deemed Consent" under the DPDP Act?

The DPDP Act recognises "deemed consent" as a form of consent from data principals when they are considered to have granted approval for the processing of their personal data without explicitly stating so. Such consent generally arises when data principals voluntarily provide their personal data to the data fiduciary without any explicit objection to its usage.

16. Who is a "Data Fiduciary"?

"Data Fiduciary" means any person who, alone or in conjunction with others, determines the purpose and means of processing personal data.

Here is a simple example: X, an individual, registers herself on an online marketplace operated by Y, an e-commerce service provider, for a lawful and specified purpose. Here, Y determines what needs to be done with the Personal Data and how it will be used.

17. Who is a Significant Data Fiduciary?

Significant Data Fiduciary means a Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government. It will be determined based on multiple factors around the nature of personal data and volume, etc. There is a likelihood that this would cover entities with access to personal data that will be termed as sensitive, such as health information or children's personal data.

18. Who is a Data Processor?

A Data Processor is any person who processes personal data on behalf of a Data Fiduciary.

For example, an organisation, Company (X), engages a visiting card vendor (Y) to print the cards for its employees. X will be the Data Fiduciary as it controls the "why", i.e., the reason for the card to be printed and how it will be printed.

On the other hand, Y just does what X tells it to do. Y will not do anything beyond the mandate of printing the cards as per the instructions provided by X, and therefore, Y is the Data Processor.

19. How is a "Person" defined in the DPDP Act?

Person includes-

a) an individual;
b) a Hindu undivided family;
c) a company;
d) a firm;
e) an association of persons or a body of individuals, whether incorporated or not;
f) the State; and
g) every artificial juristic person not falling within any of the preceding sub-clauses;

h) It means that the Data Fiduciary and Data Processor can be an individual or any form of the above structures.

20. Who is a Consent Manager under the DPDP Act?

"Consent Manager", as defined under the Act, means a person registered with the Data Protection Board of India who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Consent Manager is designed to be a Third Party and not the Data Fiduciary.

21. What are the responsibilities of a Consent Manager?

The role of a consent manager is to serve as a conduit between the Data Fiduciary and the Data Principal, ensuring that the latter's consent preferences are respected. The consent manager is responsible for managing consent processes for data sharing, and for protecting the privacy and rights of the Data Principal. To this end, the consent manager must adhere to the technical, operational, financial, and other conditions set by the DPDP Act.

22. What is "Legitimate Use" under which a Data Fiduciary can process personal data under the DPDP Act?

Legitimate use in terms of the DPDP Act are use cases wherein consent is not required, and the Data Fiduciary can process the personal data of a Data Principal for various lawful uses. Some of the legitimate uses are as follows:

a) For the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data;

b) For the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;

c) For fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

d) For compliance with any judgment, decree or order issued under any law for the time being in force in India or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

e) For responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;

f) For taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;

g) For taking measures to ensure the safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order; and

h) For the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

23. What are the Rights and Duties of the Data Principal?

The DPDP Act provides that the Data Principal shall have the following rights:

a) Right to access information about personal data: The Data Principal has the right to request information about their personal data being processed, a summary of personal data being

processed, and the identities of all other data fiduciaries and data processors with whom their data has been shared.

b) Right to correction and erasure of personal data: A Data Principal has the right to request data fiduciaries to correct, complete, update and erase his personal data. A Data Principal can also request such erasure when it is no longer needed for the purpose for which it was processed.

c) Right to redress grievances: A Data Principal has the right to register his grievances with data fiduciaries, who must provide easily accessible grievance redressal mechanisms. A Data Principal is required to exhaust these grievance redressal options before approaching the Data Protection Board.

d) Right to nominate: A Data Principal has the right to nominate any other individual to exercise his rights on his behalf in case of death or incapacity.

e) Though not listed as a right under the relevant Chapter of the DPDP Act, the right to withdraw consent is another right with the Data Principal. The consequence of this is that the Data Fiduciary will cease processing. However, the Data Principal will be responsible for the consequences of withdrawal after exercising this right.

In the DPDP Act, there are corresponding duties of the Data Principal to:

a) to comply with the provisions of all applicable laws for the time being in force;

b) to ensure that she does not impersonate another person while providing her personal data for a specified purpose;

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

d) to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Data Protection Board of India; and

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

24. Are there specific conditions for processing the personal data of certain categories of data principals?

There are specific conditions for processing the personal data of a child and a person with disabilities. Before processing any personal data of a child or a person with disabilities who has a lawful guardian, the Data Fiduciary is required:

a) To obtain verifiable consent of the parent of such child or the lawful guardian.

b) A Data Fiduciary is not permitted to process personal data that is likely to cause any detrimental effect on a child's well-being.

c) A Data Fiduciary cannot undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

d) The Government. may prescribe certain classes of Data Fiduciaries that will be exempted from:

   i. the restriction relating to the processing of data relating to a child/a person with a disability; and

   ii. the restriction relating to tracking or behavioural monitoring of children or targeted advertising directed at children.

Where the Central Government is satisfied that the Data Fiduciary handling a child’s personal data is doing so in a verifiable, safe manner, it can exempt such data Fiduciary from the applicability of all or any of the obligations mentioned above.

25. Can personal data be transferred outside India under the DPDP Act?

The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

The DPDP Act envisages a blacklist of countries where the personal data cannot go. For all other countries, transfer is allowed. The only exception to this rule is if there is any other overriding law that mandates that personal data will not be transferred outside the country.

26. What are the exemptions for processing personal data?

Most of the provisions of Chapter II (Obligation of Data Fiduciary), Chapter III (Rights and Duties of Data Principal), and Section 16 (Special Provisions) do not apply to:

a) the processing of personal data that is necessary for enforcing any legal right or claim;
b) the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function;
c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India;
d) personal data of Data Principal not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India;
e) the processing is necessary for a scheme of compromise arrangement or merger, or amalgamation of two or more companies or reconstruction by way of demerger of a company, or transfer of undertaking of one or more companies to another

company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force;

f) the processing to ascertain the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force;

g) With respect to the processing of personal data by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognisable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and (ii) necessary for research, archiving or statistical purposes if the personal data is not to be used to make any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.

27. What is the "Data Protection Board of India"?

The DPDP Act outlines the establishment of the Data Protection Board of India (DPBI) to serve the objectives of the Act. The Board is composed of a Chairperson and additional Members, as determined by the Central Government.

28. What are the primary functions of the DPBI?

The key functions of the Data Protection Board of India include:

a) Conducting Inquiries
b) monitoring compliance and imposing penalties,

c) directing data fiduciaries to take necessary measures in the event of a data breach and
d) hearing grievances made by affected persons.

29. What is the Appellate Authority for appeals against the decisions of the DPBI?

If any person is aggrieved by an order or instruction given by the DPBI under this Act, they can file an appeal with the Appellate Tribunal within sixty days from the date of receipt of the order or direction. If an appeal cannot be resolved within six months, the Appellate Tribunal must provide written reasons for the delay in concluding the appeal.

30. What is the process to be followed by data fiduciaries in case of a personal data breach?

In the event that personal data is breached, it is the responsibility of the data fiduciary to provide prompt notification to both the DPBI and all affected data principals. The notification must include comprehensive details pertaining to the nature of the leaked personal data.

31. What are the penalties for non-compliance under the DPDP Act?

The penalties for non-compliance range from INR 10,000 to INR 200 crore, with a prescribed upper limit of INR 250 crore as per the Act.

The DPDP Act specifies penalties for various offences, such as:

a) up to INR 10 thousand for breach of duties by data fiduciary,
b) up to INR 200 crores for non-fulfilment of obligations in relation to children,
c) up to INR 250 crores for failure to take security measures to prevent data breaches.

The breach timelines for notification by the Data Fiduciary to the Data Protection Board of India in the DPDP Act are not yet specified. However, when the rules are notified, there needs to be a harmonisation to the "Guidelines on Information Security Practices" issued by the Indian Computer Emergency Response Team ("CERT").

32. Will the Information Technology Act, 2000 remain applicable to persons covered under the DPDP Act?

Yes. The persons covered under the DPDP Act shall have to continue compliance with the Information Technology Act, 2000. It is noteworthy that the provisions pertaining to compensation for negligent handling of sensitive personal data, as delineated under Section 43A of the Information Technology Act (IT Act), and the Sensitive Personal Data or Information (SPDI) Rules have been repealed subsequent to the enactment of the Data Protection and Privacy Bill (DPDP Act). It is pertinent to note that in the event of any inconsistency between the application of data protection laws, the DPDP Act shall supersede the IT Act.

33. Which provisions of the DPDP Act and the General Data Protection Regulations (GDPR) are similar?

There are numerous similarities between compliances under the DPDP Act and the GDPR:

a) The rights of data principals have been recognised by both the legislations, including the right to access information about personal data and the right to correction and erasure of personal data. Further, the legislations require data fiduciaries to implement requisite measures to safeguard personal data against unauthorised access, disclosure, or modifications.

b) Additionally, the DPDP Act allows for the processing of personal data for certain specific circumstances without the requirements of consent from the data principals. The GDPR

also grants such authority to data controllers conditional to the fulfilment of certain obligations.

c) The DPDP Act recognises the concept of classifying a data fiduciary as a "Significant Data Fiduciary" on the basis of the volume of sensitivity of personal data, which is parallel to the concept of data protection officers under the GDPR.

d) The Data Privacy and Protection Directive (DPDP) and the General Data Protection Regulation (GDPR) also share a number of similarities with respect to the requisites for obtaining consent for the processing of personal data. Specifically, both regulations require that the consent of the data subject be freely given, specific, and informed.

Furthermore, they stipulate that a legal basis for processing personal data must exist. A further obligation common to both regulations is that the data fiduciary/controller must furnish proof that the consent was obtained in conformity with the relevant laws. The DPDP goes one step further by mandating that the request for consent be made available in a selection of languages that the data subject may choose from, thereby enhancing accessibility requirements.

CHOOSING LEXORBIS

With a complete range of IP Services and a qualified team of trained professionals, our working philosophy is to tailor our services to individual needs and help clients navigate all stages of the intellectual property lifecycle. Our attorneys, while focusing on quality as their first goal, use their diverse experience and knowledge to achieve the kind of partnership that leads to mutual trust and respect.

New Delhi

709-710 Tolstoy House,
15-17 Tolstoy Marg,
New Delhi – 110001

Mumbai

146 Jolly Maker Chamber II,
Vinay K Shah Marg, Nariman Point,
Mumbai – 400021

Bengaluru

606-607, Gamma Block,
Sigma Soft Tech Park No. 7, Whitefield Main Road,
Varthur Hobli, Bengaluru – 560066

Chennai

Century Centre, 3rd Floor, No. 75 (Old no. 39)
TTK Road, Alwarpet
Chennai – 600018

LexOrbis | Intellectual Property Attorneys & Advocates

mail@lexorbis.com / www.lexorbis.com /