DENTONS LINK LEGAL

FAQs

Digital Personal Data Protection Act 2023

Grow | Protect | Operate | Finance

1. WHAT IS THE CURRENT LEGISLATIVE FRAMEWORK FOR PROTECTION OF PERSONAL DATA IN INDIA?

In 2017, the Supreme Court of India recognized the right to privacy as a fundamental right in the landmark judgment of *Justice KS Puttaswamy v Union of India* and held that right to privacy is protected as an intrinsic part of the right to life and personal liberty and forms a part of the freedoms guaranteed by the Indian Constitution. The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") is a result of efforts made by the Indian Government over several years to introduce a cross-sector legislation on data privacy.

The DPDP Act has received Presidential assent on August 11, 2023, after being passed in both the houses of the Indian Parliament. Though the DPDP Act is legally a 'statute' but the provisions of DPDP Act have not yet come into effect. The provisions of DPDP Act will come into force on a date as may be notified in the official gazette by the Central Government. The Central Government may opt to enforce the provisions of DPDP Act in a phased manner.

Till the time the provisions of DPDP Act come into force, the existing legislative framework for protection of data in India persists. Accordingly, the extant law on data protection in India continues to be fragmented and is broadly contained in the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**") framed under the IT Act. The SPDI Rules regulate the collection, use, processing and transfer of sensitive personal data or information ("**SPDI**") which includes passwords, medical records, biometric information etc.

In addition to the general data protection framework as discussed above, sector-specific regulations and rules issued by the Reserve Bank of India, the Securities Exchange Board of India and Insurance Regulatory and Development Authority of India also regulate data protection.

2. WHY HAS THE INDIAN GOVERNMENT INTRODUCED THE DPDP ACT DESPITE THE EXISTING FRAMEWORK?

The SPDI Rules suffer from various conceptual and procedural flaws including drafting defects. With the introduction of the DPDP Act, the Government has tried to address loopholes in the SPDI Rules and bring India's privacy laws at par with international standards. The DPDP Act primarily aims to bring about a significant change in the data protection regime by seeking to protect the rights of data principals (*defined in FAQ No. 5*) and regulate data fiduciaries (*defined in FAQ No. 5*), including companies and businesses.

3. IS INDIA A SIGNATORY TO ANY INTERNATIONAL AGREEMENTS OR TREATIES ON DATA PROTECTION?

India is a signatory to the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, both of which acknowledge the right to privacy.

4. HOW IS "PERSONAL DATA" DEFINED?

The SPDI Rules define 'Personal Information' as *any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*.

On the other hand, the DPDP Act defines 'Personal Data' as *any data about an individual who is identifiable by or in relation to such data*. This includes identifiers like name, phone number, Aadhaar, PAN.

While the scope of the SPDI Rules is limited to regulating processing of only SPDI (*passwords, medical records etc.*), the DPDP Act contemplates a much wider scope. Once notified, the DPDP Act will regulate processing of '*digital personal data*', i.e., personal data, which is either collected in digital form, or which, where collected in non-digital form is digitised subsequently. Having said that, non-digital personal data and non-personal data would fall outside the purview of the DPDP Act.

5. DOES THE INDIAN DATA PROTECTION FRAMEWORK CONTEMPLATE 'CONTROLLER', 'PROCESSOR' AND 'DATA SUBJECT'?

While the SPDI Rules do not define 'Controller', 'Processor' and 'Data Subject', the DPDP Act provides for the following:

(i) Equivalent to a 'Controller' under the European Union's General Data Protection Regulation ("**EU-GDPR**"), the DPDP Act defines **Data Fiduciary** *as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data*.

(ii) **Data Processor** is defined as *any person who processes personal data on behalf of a Data Fiduciary*.

(iii) **Equivalent** to a 'Data Subject' under the EU-GDPR, the DPDP Act defines **Data Principal** as *the individual to whom the personal data relates. In the case of a child, data principal includes the parents or lawful guardian of such a child. Similarly, in the case of a person with disability, it includes her lawful guardian, acting on her behalf*. Accordingly, the DPDP Act seeks to only protect personal data of natural individuals.

6. DO INDIAN DATA PROTECTION LAWS HAVE EXTRATERRITORIAL APPLICABILITY?

While the SPDI Rules primarily apply only to entities/ persons located in India, this will change with the DPDP Act.

The DPDP Act specifically provides for an extra territorial applicability, i.e., once in force, it will apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to '*offering'* of goods or services to data principals within the territory of India.

7. WHAT ARE THE KEY OBLIGATIONS OF A DATA FIDUCIARY UNDER THE EXTANT LEGAL FRAMEWORK AND THOSE UNDER DPDP ACT?

Till the DPDP Act is notified, entities are mandated to be transparent in their processing activities as per the SPDI Rules which includes informing the information provider that SPDI is being collected, the purpose of collection, intended recipients of the SPDI etc. The SPDI Rules also mandate obtaining prior written consent for collecting and processing SPDI. Entities must exercise principles of purpose limitation, and data minimization in their processing activities. Having said that, till date there has been little to no enforcement of these obligations under the SPDI Rules.

Upon notification, some of the key obligations of a data fiduciary under the DPDP Act will be as under:

(i) data fiduciaries may process personal data only in accordance with the DPDP Act for a lawful purpose.
(ii) a data fiduciary to obtain consent for processing after providing a notice describing the type of personal data sought to be collected, a list of purposes of processing etc. For a data fiduciary's obligations *vis-à-vis* consent, please refer to our response to FAQ No. 9.
(iii) general obligations including (a) compliance with the DPDP Act; (ii) implementation of appropriate technical and organizational measures; and (iii) protection of personal data in its possession.

In addition to the above, the DPDP Act also envisages the concept of Significant Data Fiduciaries, a sub – set of data fiduciaries to be determined based on a specified criterion such as volume and sensitivity of the data processed by them, the risk of harm to the data principal, potential impact on the sovereignty and integrity of India and other such factors. Significant Data Fiduciaries are subject to additional obligations like appointing a data protection officer, conducting audits and data protection impact assessments.

8. DO ADDITIONAL OBLIGATIONS APPLY TO PROCESSING OF PERSONAL DATA OF CHILDREN OR A PERSON WITH DISABILITY?

The SPDI Rules do not specifically address children and their data. On the other hand, the DPDP Act imposes additional obligations on data fiduciaries in relation to processing of personal data of children and persons with disability.

The DPDP Act mandates the data fiduciaries to obtain '*verifiable consent*' from parents and legal guardians before processing personal data of children (*individuals below 18 years of age*) and persons with disability respectively. In its present form, the DPDP Act does not set out the manner of obtaining such verifiable consent, however, the same is expected to be prescribed under the rules to be issued pursuant to the DPDP Act.

The DPDP Act further prohibits: (i) tracking or behavioral monitoring of, and targeted advertising directed at, children; and (ii) processing of children's data that is likely to cause any detrimental effect on the well-being of a child.

9. HOW DOES THE DPDP ACT DEAL WITH CONSENT' OF DATA PRINCIPAL?

Under the DPDP Act, personal data can be processed only with the consent of the data principal, except where the personal data is being processed for certain legitimate uses discussed in FAQ No. 10 below.

The DPDP Act requires that the consent of the data principal is free, specific, informed, unconditional and unambiguous and is given by way of a clear affirmative action. There is no concept of a deemed consent under the DPDP Act.

Consent under the DPDP Act should signify an agreement to the processing of the data principal's personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. Therefore, under the DPDP Act, if a data principal accords consent, but a part of such consent does not meet the requirement of a valid consent under the DPDP Act, then such consent shall be invalid to the extent of such infringement.

10. WHAT ARE LEGITIMATE USES FOR PROCESSING OF PERSONAL DATA UNDER THE DPDP ACT?

The DPDP Act permits the processing of personal data of data principals for certain specified legitimate uses. The legitimate uses where a data fiduciary would not be required to seek consent for the collection and processing of personal data are:

(i) where a data principal voluntarily provides her personal data to the data fiduciary and has not indicated to the data fiduciary that she does not consent to the use of her personal data;
(ii) for the State or any of its instrumentalities to provide or issue benefits or services to the data principal where the data principal has (i) previously consented to the processing of her personal data for

availing any benefits or services from the State or any of its instrumentalities; or (ii) such personal data is available in digital form or in non-digital form and digitized subsequently from any database, register, book or other document maintained by the State or any of its instrumentalities;

(iii) for the performance of any function by the State or any instrumentality of the State under any law currently in force in India or in the interest of sovereignty and integrity of India or security of the State;

(iv) for compliance with any judgment or order issued under the law in force in India, or any judgement or order relating to contractual claims of a civil nature under any law in force outside India;

(v) responding to a medical emergency involving threat to life or immediate threat to health;

(vi) for taking measures to ensure safety of, or provide assistance or services to, any individual during disaster, or any breakdown of public order; and

(vii) for purposes relating to employment or those related to safeguarding the employer from loss or liability.

Under the DPDP Act, there is no requirement to provide prior or post-facto notice by the data fiduciary to the data principal in case of processing of personal data for any specified legitimate uses.

11. WHAT ARE THE RIGHTS OF A DATA PRINCIPALS VIS-À-VIS THEIR PERSONAL DATA UNDER THE EXTANT LEGAL FRAMEWORK AND THOSE UNDER DPDP ACT?

At present, the SPDI Rules provide the following rights to data principals, namely,

(i) ***Right to review data***: Data principals have the right to review the SPDI provided.

(ii) ***Right to correction of data***: Data principals have the right to seek correction/ amendments to their SPDI.

(iii) ***Right to withdraw consent***: Data principals have the option to withdraw their consent at any time by giving a written notice.

(iv) ***Right to be forgotten***: While the SPDI Rules, per se, do not extend the right to be forgotten to the providers of SPDI, there have been judicial precedents whereby courts have recognized this right in specific situations.

As compared to the SPDI Rules, the DPDP Act envisages additional rights of data principals such as:

(i) ***Right to access***: The DPDP Act provides data principals the right to obtain information regarding the personal data processed along with the identities of all the data fiduciaries and data processors with whom the personal data has been shared.

(ii) ***Right to correction and erasure of personal data***: The DPDP Act extends the right of correction and erasure to data principals. Consequently, upon a request by data principals, data fiduciaries are required to correct, complete, and update personal data, as the case may be. Similarly, upon a request to erase personal data, data fiduciaries are required to comply with the same unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

(iii) ***Right of grievance redressal***: Data fiduciaries are required to offer readily available grievance redressal mechanisms to data principals. The DPDP Act emphasizes that the data principal must exhaust all options for grievance redressal before approaching the Data Protection Board of India ("**Board**"), the regulatory body to be established under DPDP Act.

(iv) **Right to *nominate***: The DPDP Act grants data principals the right to nominate an individual in case of death or incapacity.

(v) ***Right to withdraw consent***: The DPDP Act enables a data principal to withdraw consent for the processing of personal data by a data fiduciary when such personal data is processed based on consent only.

Interestingly, the DPDP Act also imposes certain duties on the data principals which, *inter alia*, include compliance with '*all applicable laws*', furnishing only verifiably authentic information, not registering false or frivolous grievances or complaints with a data fiduciary or the Board.

12. DO DATA FIDUCIARIES NEED TO FORMULATE A PRIVACY POLICY?

Whilst the SPDI Rules mandate entities processing SPDI to have a privacy policy in place and publish the same on its website, the DPDP Act appears to have waived the requirement of formulating a privacy policy by the data fiduciaries.

13. DOES THE LAW LIMIT THE AMOUNT OF PERSONAL DATA THAT MAY BE HELD OR THE DURATION FOR WHICH SUCH DATA MAY BE HELD?

Data Minimisation

Both the SPDI Rules as well as the DPDP Act provide that only those items of personal data necessary for attaining a specified purpose must be collected.

Data Retention

The SPDI Rules provide that SPDI is not permitted to be retained for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force. Similarly, the DPDP Act also imposes an obligation on data fiduciaries to erase personal data, upon withdrawal of consent or as soon as the specified purpose is no longer being served, whichever is earlier.

14. ARE THERE ANY RESTRICTIONS ON CROSS-BORDER TRANSFER OF PERSONAL DATA?

Presently, the SPDI Rules allow cross-border transfer of SPDI provided the recipient entity ensures the same level of data protection. Moreover, transfer is permissible only if it is necessary for the performance of a lawful contract or where the data principal has consented to such data transfer. In addition to this, there are certain sector specific data localization restrictions placed on transfer of personal data.

The DPDP Act provides that the Central Government may restrict the transfer of personal data to such countries outside India as may be notified. In essence, the DPDP Act contemplates a 'negative list' of countries to which data transfers would be barred. The criteria and principles for barring a jurisdiction are yet to be specified and notified.

15. DOES THE LAW MANDATE THE APPOINTMENT OF A DATA PROTECTION OFFICER?

The SPDI Rules do not, per se, mandate the appointment of a 'data protection officer'. Having said that, the SPDI Rules require entities to designate a 'Grievance Officer' and publish the details of such person on its website. The Grievance Officer is mandated to redress the grievances within one month from the date of receipt of grievance.

The DPDP Act also mandates data fiduciaries to establish an effective mechanism to redress the grievances of data principals and publish details of the person to whom questions may be raised about its processing activities. Additionally, as mentioned in FAQ No. 7, the DPDP Act envisages the appointment of a 'Data Protection Officer' by Significant Data Fiduciaries.

16. WHAT AUTHORITY(IES) ARE RESPONSIBLE FOR ENFORCING INDIAN DATA PROTECTION LAWS?

At present, there is no specific regulatory authority for data protection in India. The Ministry of Electronics and Information Technology ("**Ministry**") is responsible for administering the IT Act and issuing the rules and other clarifications under the IT Act. While the adjudicating officers appointed under the IT Act are responsible for enforcing the provisions of the IT Act and the SPDI Rules, till date, there have not been any well-known instances of a data fiduciary having been penalized for non-compliance of the SPDI Rules.

The DPDP Act, in turn, proposes to establish the Board, an adjudicatory body, to regulate protection of digital personal data in India. The Board will function digitally and will be digital by design in terms of receipt of complaints, hearings, pronouncement of decisions, and other functions. Further, the Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**") has been designated as the appellate tribunal under the DPDP Act and any appeals from orders and directions of the Board will be required to be made before the TDSAT.

17. HOW ARE DATA BREACHES REGULATED UNDER THE CURRENT LEGISLATIVE FRAMEWORK AND HOW IS IT DIFFERENT UNDER THE DPDP ACT?

Currently, data breaches are regulated by the provisions of the IT Act and the rules thereunder. The Ministry has constituted the Indian Computer Emergency Response Team ("**CERT**"), which acts as the nodal agency to receive, investigate and respond to all data breach notifications. Specified cyber security incidents are required to be reported by entities to the CERT in a time bound manner.

In contrast to the current enforcement mechanism for data breaches, the DPDP Act obligates the data fiduciary or the data processor to notify the Board and the affected data principal in the event of a personal data breach.

A "Personal Data Breach" has been defined under the DPDP Act as any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

The DPDP Act also prescribes specific penalties for: (a) breach in observing the obligation to take reasonable security safeguards to prevent Personal Data Breach; (b) breach in observing the obligation to give the Board or the affected data principals notice of Personal Data Breach; (c) breach in observing of additional obligations of significant data fiduciaries; (d) breach of any term of voluntary undertaking accepted by the Board in respect of any matter related to observing the provisions of the DPDP Act; and (e) general breach of any provisions of the DPDP Act or any rules framed under it. The most significant penalties under the DPDP Act are for failure to comply with the data-breach obligations under the DPDP Act.

For ascertaining the quantum of penalty to be levied, factors, such as nature, gravity, and duration of non-compliance, type of personal data affected, or repetitive nature of non-compliance, will be taken into account by the Board.

18. WHAT ARE THE RELEVANT PENALTIES FOR VIOLATION OF THE DATA PROTECTION LAWS?

As per the IT Act and the SPDI Rules, any negligence by a body corporate owning, controlling, or operating a computer resource that holds, processes, or deals with SPDI, which results in wrongful gain or loss to any person, attracts damages by way of compensation. Further, any person, including an intermediary when providing services under the terms of a lawful contract, disclosed information in breach of that contract, breached privacy.

The financial and criminal liabilities under the IT Act and SPDI Rules is up to INR Five Hundred Thousand with maximum imprisonment of up to 3 years for non-cognizable offences which is bailable and compoundable, however, having certain exceptions.

Under the DPDP Act, the maximum monetary penalty is up to INR 2.5 billion, whereas there is no mention of any criminal prosecution, and the legislature has heavily relied upon monetary penalty as a strong deterrence against the breaches and compromise of personal data. The schedule annexed to the DPDP Act prescribes different monetary penalties for specific breaches of the provisions of the DPDP Act or any rules made under it. Any sums realized by way of penalties under the DPDP Act will be credited to the Consolidated Fund of India.

However, for cognizable and serious offences committed by the organisations / individuals, which compromises of personal and sensitive data breach, the relevant provisions of the Indian Penal Code, 1860 and the Code of Criminal Procedure, 1973 would be applicable.

19. HOW ARE CYBERSECURITY AND DATA PROTECTION LINKED?

There have been several instances of hacks, and unauthorized data access. This significantly highlights why organizations need both data protection and cybersecurity. Cybersecurity is a technical way of implementing data privacy choices. Generally, unauthorized access is a significant threat that interconnects all types of breaches. By combining the data protection and cyber-security strategies, the organisation will have total control of all stages of the organisation's data lifecycle. It will also be easier for the organisations to comply with all the applicable regulations.

20. DOES THE DATA PROTECTION LAW COVER INTERCEPTION OF COMMUNICATIONS, ELECTRONIC MONITORING AND SURVEILLANCE OF INDIVIDUALS?

Pursuant to the introduction of EU-GDPR and the Schrems Judgments[1], organizations in the EU, looking to transfer data to India, are mandated to undertake Transfer Impact Assessments ("**TIAs**"). Such TIAs are intended to evaluate whether the Indian legal framework ensures adequate protection of personal data transferred to India, basis certain parameters. One key parameter in this regard is laws governing access of data by government intelligence and law enforcement agencies.

In India, data may be accessed by government intelligence and law enforcement agencies by exercising powers under the IT Act and the Indian Telegraph Act, 1885.

The DPDP Act also exempt data processing from privacy protections by any 'instrumentality of the State 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 cognizable offence relating to any of these'. It further allows the Government to exempt certain data fiduciaries from any provision of the DPDP Act by way of a notification. These provisions signify that the Government has wide powers under the DPDP Act to exempt itself from any data protection related obligations.

[1] *Schrems I and Schrems II Judgments passed by the Court of Justice of the European Union*