Frequently Asked Questions on Data Protection Laws in India

Data is increasingly becoming an important and all-pervading aspect of our lives. Proper and intelligent usage of data by companies or individuals may give them a competitive edge over their competitors. However, with this comes the problem of accountability and fair usage. Data privacy and protection is as important as the efficient use of data and for that purpose being aware of the data protection laws that apply to an individual and the rights that a person may enjoy with respect to his data is extremely critical.

This primer covers a basic understanding of the Data protection laws in India.

1. What are the laws and regulations governing data protection in India?

Currently, the general Indian framework on data privacy and protection is provided under the Information Technology Act, 2000 ("IT Act") and its ancillary rules, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("IT Rules").

The Supreme Court in its landmark judgment of Justice K.S. Puttaswamy (Retd.) and Anr. Vs. Union of India and Anr. has recognized the right to privacy of an individual as a Fundamental Right as under Part III of the Constitution. Pursuant to this, the privacy of any individual, which extends to data privacy, may only be

violated by a procedure established by law and on the condition of this procedure being fair, just and reasonable and that such violation shall undergo the highest standard of scrutiny and can only be justified in cases of a compelling state interest.

Other than the general data protection framework as discussed above, there are certain industry specific regulations dealing with data privacy and protection.

In the telecommunications sector, the telecom service providers have certain obligations like proper maintenance of records, and prohibitions on bulk encryption or export of any data outside the country. Similarly, in the banking and the insurance sectors, the Reserve Bank of India and Insurance Regulatory and Development Authority, respectively, have time and again laid down norms for information security and the storage of data. Further, the Securities Exchange Board of India, the securities market regulator in India, through timely circulars has also laid down data processing norms for clearing corporations, depositories and stock exchanges.

The Personal Data Protection Bill, 2019 ("PDP Bill") which is a comprehensive cross-sector legislation on the subject has been introduced in the Parliament and is presently being considered by a joint parliamentary committee. The key features of the PDP Bill have been discussed at Questions 12 through 19.

2. What are the categories of information under the IT act?

The categories of information provided for under the IT Act are 'Personal Information' and 'Sensitive Personal Data or Information'.

3. What qualifies as Personal Information?

Personal Information ("Personal Information") is defined as any information which relates to a natural person and is capable of identifying such person, either in combination with other similar information that is available with a body corporate or otherwise.

4. What qualifies as Sensitive personal data or information?

Sensitive Personal Data or Information ("Sensitive Personal Data or Information") is a subset of personal information and consists of information relating to the finances, health records, passwords, biometric information, or sexual orientation of an individual, etc. However, any information that is legitimately available in the public domain is not Sensitive Personal Data or Information.

5. Which entities are to comply with the provisions under the present legal frame work?

Under the current legal framework, all entities including any company, firm, sole proprietorship or other association of individuals engaged in commercial or professional activities, ("Body Corporate") that are engaged in the process of collecting, processing, storing or handling of Sensitive Personal Data or Information and are doing so through an electronic medium are responsible for complying with the provisions of the IT Act and the rules formed thereunder.

6. Which entities are not covered under the present legal framework?

The current legal framework does not impose any obligations on natural persons for collecting and processing information. Further, the collection of any kind of personal

information that does not fall under the category of Sensitive Personal Data or Information or any data that has not been collected using an electronic medium are also not covered under this framework. Additionally, the IT Rules do not apply to Body Corporates operating outside India's territorial jurisdiction.

7. What is the law governing collection of Sensitive Personal Data or Information?

Sensitive Personal Data or Information can only be collected from an individual who has given consent for such collection. Any Body Corporate that is engaged in the collecting of Sensitive Personal Data or Information has to ensure that the collection is for a lawful purpose, associated with the activities of the Body Corporate and that the collection of Sensitive Personal Data or Information is necessary for such activity. An individual is allowed to withdraw his / her consent to collect and use data.

8. What is the law governing using and storage of Sensitive Personal Data or Information?

A Body Corporate must ensure that the Sensitive Personal Data or Information is used for the same purpose for which it has been collected. Specific consent of the relevant individual must have been taken for the usage of data for the particular purpose and the consent from the individual must be obtained in writing. A Body Corporate must also ensure that they have created a privacy policy for the handling and storage of Sensitive Personal Data or Information and that such policy is readily available on their respective website. The Sensitive Personal Data or Information can be retained only as long as it is needed. Additionally, a Body Corporate must permit the concerned individual to review and amend any data which might be inaccurate or outdated.

9. What is the law governing transfer of Sensitive Personal Data or Information?

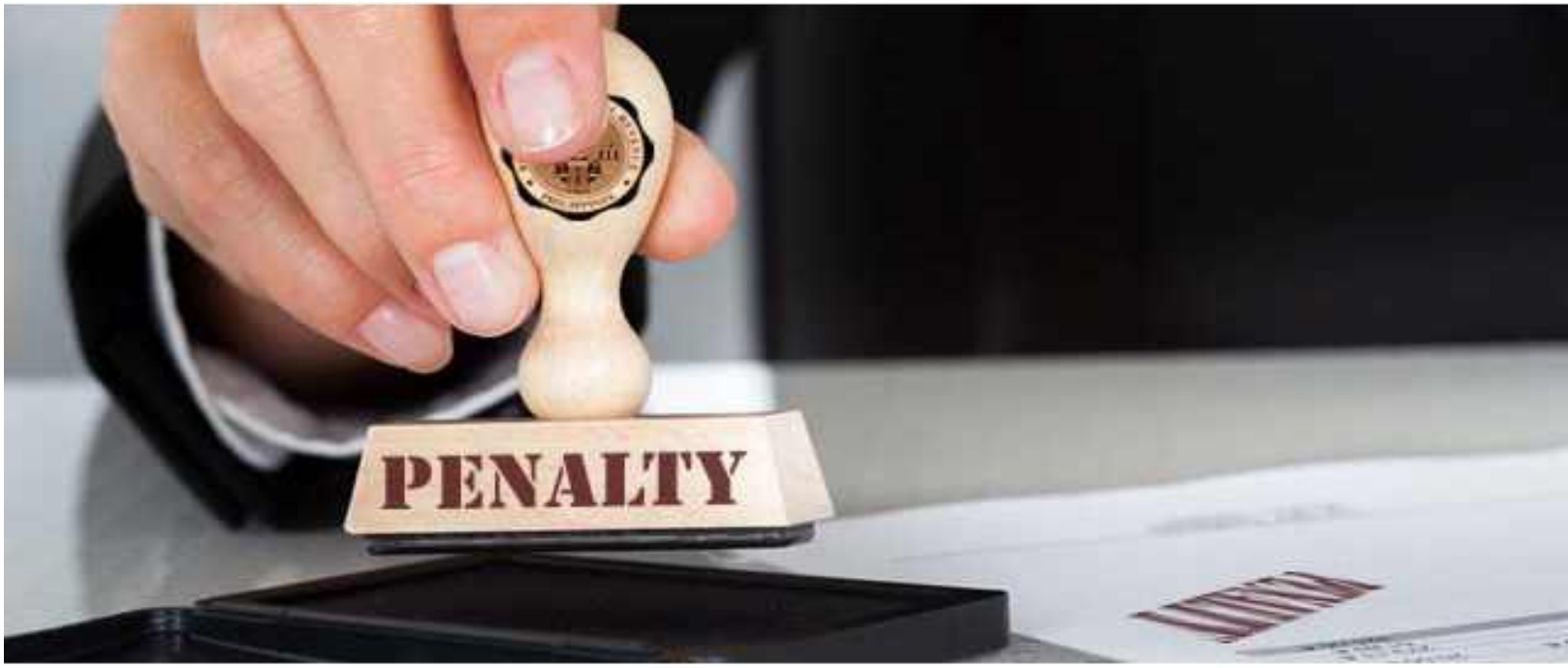
Before any transfer of Sensitive Personal Data or Information takes place, consent of the individual to whom the data pertains, must be taken. It must be ensured that the transferee provide the same level of data protection as the transferor is obligated to provide under the law.

10. What are the penalties for contravention under the present IT Act?

If any person has or gains access to the Personal Information of an individual by virtue of providing a service under a contract and discloses such Personal

Information without authorization, with the wrongful intent of causing harm to the individual, that person shall be liable for a fine of up to INR 500,000 and / or imprisonment up to 3 (three) years. In cases where the offence has been committed by a company, every person who at the time of the commission of offence was in charge of the company for the conduct of its business shall be liable to be proceeded against and punished accordingly.

If any person or Body Corporate that is involved in the collecting, handling, or processing of Sensitive Personal Data or Information of an individual, does not implement sufficient security measures to protect the Sensitive Personal Data or Information, it shall be liable to pay damages by way of compensation to the individual who suffers the wrongful loss. Under the IT Act, no cap has been set out for the compensation that may be awarded to the affected person.



www.acuitylaw.co.ir

11. What is the PDP Bill, 2019?

The PDP Bill, 2019 is the comprehensive cross-sector legislation on data protection that has been formulated to lay down the principles of data processing and has been introduced in the Parliament. It is presently being considered by a joint parliamentary committee. The Bill will come into force when it is passed by both houses of the Parliament and thereafter is notified in the Official Gazette post receipt of approval from the President of India.

12. Who shall the PDP Bill apply to and to what categories of information?

The PDP Bill has a much larger ambit than the present system for data protection. The PDP Bill applies to all person or Body Corporate, Indian or foreign that have a business connection to India, even if they principally operate outside the country. The PDP Bill has both territorial and extra-territorial application as long as there is any nexus with any Indian person or Body Corporate.

The PDP Bill is not limited to persons or Body Corporates that process data via an electronic mode and applies to data processing of any kind. Additionally, most parts of the bill apply to all Personal Data ("PD") with higher obligations for protection of Sensitive Personal Data ("SPD") and Critical Personal Data.

Personal Data means any data relating to a natural person who is identifiable by reference to the above data, whether online or offline.

Sensitive Personal Data means such Personal Data which is related to the financial, health, biometric, or genetic aspects of the Data Principal or information related to the sexual orientation, caste or tribe, or religious or political affiliations of the Data Principal.

Critical Personal Data mean such Personal Data that may be notified by the Central Government as such. Critical Personal Data shall only be processed in India.

13. Who is Data Principal?

The natural person to whom the processed data pertains to is the Data Principal. Protection under the PDP Bill is generally afforded to the Data Principal.

14. Who is a Data Fiduciary?

A Data Fiduciary is any person, Body Corporate or State entity, who alone or along with others determines the purpose and method of processing of Personal Data.

15. Who is a Data Processor?

A Data Processor is any person, Body Corporate or State entity that processes personal data on behalf of a Data Fiduciary under contract or otherwise. The Data Processor while processing data on behalf od the Data Fiduciary must implement appropriate security safeguards.

16. What are the important characteristics of the PDP Bill?

The following are some of the key characteristics of the PDP Bill:

(i) It provides for storage of all SPD within the territorial limits of India. Data may be transferred outside India but subject to appropriate safeguards as are laid down.

(ii) It confers on the Data Principals, the right to be forgotten, the right to data portability and the right to access, correction and erasure of personal data.

(iii) It provides for 'consent managers' who shall be responsible for bridging the gap between the Data Principal and the Data Fiduciary.

(iv) their lays down obligation on a Data Fiduciary to send a data breach notification to the Data Principal in any case of breach.

(v) It provides for the establishment of a Data Protection Authority which shall be a cross-sector regulatory authority for data protection. It shall be responsible for the implementation of the PDP Bill.

17. What are the penalties for contravention under the PDP Bill?

Penalties for contravention of key provisions of the PDP Bill range from INR 50 million to INR 150 million or 2-4% of the worldwide turnover of the entity depending on the nature of the offence. It also imposes criminal penalties for certain contraventions which may extend to imprisonment for up to 3 years and / or a fine of up to INR 200,000. In cases where the offence has been committed by a company, every person who at the time of the commission of offence was in charge of the company for the conduct of its business shall be liable to be proceeded against and punished accordingly.

The Bill also provides for compensation that is payable to the adjudicating authority for harm suffered as a result of an infringement.

18. What is the Data Protection Authority formed under the PDP Bill?

The Data Protection Authority as formed by the PDP Bill shall be responsible for the implementation of the law once it has been enacted and notified. It shall be responsible for making regulations under the PDP Bill. It shall approve the codes of practice for Data Fiduciaries, register consent managers and undertake actions that are crucial for the sustenance of the country's data protection regime.

19. What kinds of transactions are exempted under the provisions of the PDP Bill?

Certain transactions are exempt from the applicability of the PDP Bill such as: (a) to small businesses or (b) data collected for domestic purposes. A small business shall be qualified as such by the Data Protection Authority depending on the turnover of the business, or the purpose of collection of the data or the volume of data processed. Outsourcing agencies may also be exempted by the Central Government from certain obligations under this system. Additionally, the Central Government has wide powers with respect to its obligations, which may be relaxed on various grounds of public interest and may exempt agencies operating under it. This ground of discretion is fairly broad and gives the government significant leeway.