INSIGHT

India: Draft Digital Personal Data Protection Rules, 2025 - Reporting of personal data breaches

2 hours ago

Summary

India's Digital Personal Data Protection Act, enacted on August 11, 2023, will supersede Section 43A of the IT Act and the SPDI Rules upon coming into force. The Ministry of Electronics and Information Technology released draft rules for public consultation on January 3, 2025, detailing the process for reporting personal data breaches. These Draft Rules require data fiduciaries to notify the Data Protection Board and affected data principals promptly, providing comprehensive details of the breach and measures taken. Additionally, these reporting obligations are supplementary to existing cybersecurity incident reporting requirements to CERT-In and sectoral regulators like SEBI, IRDAI, and RBI.

India's Draft Rules under the new data protection act detail breach reporting protocols.

On August 11, 2023, India enacted the Digital Personal Data Protection Act (the Act). Once the provisions of the Act are brought into force, it will replace Section 43A of the Information Technology Act, 2000 (the IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the SPDI Rules). The Act is proposed to come into force in a phased wise manner, i.e., as and when the Central Government notifies the provisions of the Act and also issues rules under the Act (the Rules).

On January 3, 2025, i.e., 16 months after the enactment of the Act, the Ministry of Electronics and Information Technology (MeitY) released the draft Digital Personal Data Protection Rules, 2025 (the Draft Rules) under the Act for public consultation along with an explanatory note on the Draft Rules. The intent of the explanatory note is to provide a brief overview of the Draft Rules as well as an insight into the guiding principles followed in the framing of the Draft Rules.

The Draft Rules offer guidance on the operational aspects of the Act. In part one of this Insight series, Rachit Bahl, Rohan Bagai, and Karishma, from AZB & Partners, discuss the provisions introduced under the Draft Rules for reporting personal data breaches and the processes that are required to be put in place by a data fiduciary (the person who determines the purpose and means of processing of personal data) in case of such personal data breach.

Personal data breach

The Act defines 'personal data breach' as 'any unauthorized 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.'

Accordingly, the obligations prescribed under the Draft Rules for reporting a personal data breach will be applicable, not only in instances of unauthorized processing/access of personal data involving mala fide intention but also where the breach occurs by way of an accident.

The ultimate responsibility lies with the data fiduciary to ensure that the personal data in its possession or under its control (including processing undertaken by its data processors) is protected by taking reasonable security safeguards to prevent personal data breaches.

Intimation of a personal data breach

Intimation to Data Protection Board

The data fiduciary, upon becoming aware of the personal data breach, must provide a preliminary notification to the Data Protection Board (the Board) without delay, with a description of the breach including its nature, extent, timing, location, and potential impact.

Subsequently, within 72 hours of becoming aware of the personal data breach (or within such extended timeline as permitted by the Board on a request made in writing), the Board also needs to be provided with updated information including broad facts related to the breach and circumstances that led to the event, measures implemented or proposed to be implemented by the data fiduciary to mitigate risk, findings of the investigation regarding who caused the breach, and remedial measures taken to prevent recurrence of such breach.

Intimation to data principals

In addition to notifying the Board, the data fiduciary must also notify the affected data principals without delay through their user account or any other mode of communication opted by the data principal. This intimation must be clear and straightforward providing details on the following aspects:

- description of the breach;
- nature, extent, timing, and location of occurrence;
- potential consequences of the breach relevant to the data principal;
- measures implemented and being implemented by the data fiduciary, if any, to mitigate the risk; and

- safety measures that a data principal may take to safeguard their interests.

The intimation to data principals should also include the contact details of a person who may be contacted by the data principal for any queries regarding the personal data breach. Such a person should be capable of addressing the queries of data principals and responding on behalf of the data fiduciary.

The aforementioned intimation of personal data breaches may be given to data principals using any email address, profiles, user handles, mobile number, etc. that the data principal has registered with the data fiduciary and uses to access the services of such data fiduciary.

A report on intimations given by the data fiduciary to the affected data principals also needs to be provided to the Board within 72 hours of becoming aware of the personal data breach (or within such extended timeline as permitted by the Board on a request made in writing). Therefore, the data fiduciaries might as well be required to produce a copy of such intimations.

Reporting obligations under the Draft Rules not in derogation of other reporting obligations

The reporting requirements prescribed under the Draft Rules are in addition to the reporting obligations under the Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, notified under the IT Act, that require reporting of cybersecurity incidents (which includes data breaches and data leaks) to the Indian Computer Emergency Response Team (CERT-In) within six hours of noticing such incidents or being brought to notice about such incidents, as well as sectoral reporting requirements to be made to the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Reserve Bank of India (RBI), as applicable.

Rachit Bahl Senior Partner
rachit.bahl@azbpartners.com
Rohan Bagai Senior Partner
rohan.bagai@azbpartners.com
Karishma Senior Associate
karishma.sumi@azbpartners.com
AZB & Partners, India

Topics: Breach Notification | Privacy Overview | Privacy Rights

Jurisdictions: India