Global Data Privacy and Cybersecurity Handbook - India

Breach Notification Requirements

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 22 December 2023*

Yes.

Per DPDP Act, a personal data breach includes any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data. The DPDP Act requires a data fiduciary and data processor to inform each affected data principal as well as the DPBI, in case of a personal data breach. The DPDP Act prescribes reporting for all types of personal data breaches, regardless of the sensitivity of the breach or its impact on a data principal. The form and manner of reporting, materiality threshold and timeline for reporting is yet to be prescribed.

Further, the Cyber Security Directions require entities to mandatorily report cyber security incidents to India [Computer Emergency Response Team (**CERT-In**)](https://cert-in.org.in/) within six hours of noting such incidents or being notified of such incidents. The Cyber Security Directions have listed certain "cyber security incidents," including "unauthorized access of IT systems or data," that must be mandatorily reported by entities to the CERT-In.

Therefore, once the implementation of the DPDP Act is clarified, all entities would be required to follow dual reporting in the event of a personal data breach, both to the CERT-In and the Data Protection Board of India.

# Controllers/ Owners have to notify:

*Last review date: 22 December 2023*

☒        data protection authorities

☒        cybersecurity authorities

☒        affected individuals

☒        other

Please refer to our response to “Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?” and"Are there any additional sector-specific or non-personal data security breach notification requirements?".

# Processors/ Agents have to notify:

*Last updated: 22 December 2023*

☒        controller/ owner

☐        data protection authorities

☒        cybersecurity authorities

☐        affected individuals

☒        others

Please refer to our response to "Are there any additional sector-specific or non-personal data security breach notification requirements?"