Areas of overlap between the CERT-In Directions and the DPDP Act

Indian Computer Emergency Response Team (CERT-In), the national agency for executing various functions in the field of cyber security under section 70B of the Information Technology Act, 2000. It is in constant analysis of cyber threats and incidents which are tracked and reported. In order to safeguard data/information and Information and Communication Technology (ICT) infrastructure, it often issues advisories to organisations and users. To facilitate coordination response activities and emergency measures related to cyber security incidents, CERT-In requires service providers, intermediaries, data centres, and corporate entities to provide relevant information.

Digital Personal Data Protection Act, 2023, an act enacted to regulate the processing of digital personal data, balancing individuals' right to privacy with the necessity of handling such data for legitimate purposes and other related or incidental matters. This Act emphasises on the role of significant data fiduciary (SDF), identified by the government based on the volume, sensitivity of personal data handled, and associated risk factors. This act impacts the majority of organizational areas, inclusive of legal, IT, human resources, sales and marketing procurement, finance, and information security because of the type and volume of personal data that is collected, stored, processed, retained, and disposed of in India.

Areas of Overlap

1. Applicability

   Both the instruments are applicable to entities such as service providers, intermediaries, data centres, cloud providers, VPN providers, and any entity processing digital data in India. CERT-In aims on entities specifically, whereas DPDP regulates processing activity irrespective of entity type.

2. Breach Notification

   Mandatory reporting of cyber incidents as mentioned under Annexure I to CERT-In within 6 hours of noticing such incident or being brought to notice about such incident. Such incidents can be reported to CERT-In via email, phone and fax.

   Under Rule 7 of DPDP Act. the Board must be informed about the Data Fiduciary within 72 hours without delay, or for a longer period if allowed by the Board, a detailed report must be submitted. This prioritizes individuals and mitigates damages.

3. Data Retention and Erasure

   All service providers, intermediaries, data centres, body corporate and government organisations to compulsorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. This data is to be provided to CERT-In along with reporting of any incident or when ordered/directed by CERT-In.

   DPDP under Sec.8 requires data fiduciaries/ processors to implement appropriate security safeguard and controls, including safeguards over personal data storage and retention, aligned with data minimization and purpose limitation. The act also provides Right to Erasure i.e, right to delete the data when no longer in need.

4. Appointment of Compliance Office

All users and organizations to maintain their information with CERT-In through Know Your Customer (KYC). Transaction records to be maintained by the service providers in manner that it can be traced, such information shall be inclusive of all information such as IP addresses of users, with timestamps and time zones and transaction ID. It requires designation of Point of Contact (POC) for communication and compliance process and cyber incident coordination.
The DPDP Act, 2023 mandates under section 10(2) appointment of Data Protection Officer who shall represent the Significant Data Fiduciary, officer shall be responsible to the Boards of Directors or similar governing body of SDF and will be the point of contact for grievance redressal mechanism under the provisions of this Act.

5. Providing Assistance
   As required by the direction of CERT-In, the service provider/ intermediary/ data centre/ body corporate is mandatorily required to take action or give information or any such assistance to CERT-In, which will further help in mitigating the risk to cyber security and strengthen cyber security situational awareness.
   According to section 8(6) of the Act, in the event of data breach, the Data Fiduciary (Data providers) must notify the Data Protection Board and every affected Data Principal as prescribed in the Act.

Conclusion

Both the instruments aim to strengthen the Digital field of India through ensuring cyber security and personal data protection. The CERT-In direction puts more emphasis on real-time threat monitoring, cyber security breach and infrastructure readiness whereas. The DPDP Act emphasis on more transparent, legal, and privacy-conscious data processing. Together these instruments can aim to achieve robust foundation to achieve cyber security and data protection with changes required as and when needed, as the digital and technology ecosystem continue to evolve which would further lead to new risks.