DATA BREACHES UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

A SNAPSHOT

Touchstone Partners

Applicable to digital personal data processed by Data Fiduciaries (data controllers), whether directly or through data processors:

In India: where data is collected in digital form or is digitised subsequently if collected in non-digital form.

Outside India: if processing is connected to any activity related to offering of goods or services to data subjects ('data principals') in India.

Several provisions do not apply to BPOs: where personal data of data principals outside India is processed pursuant to any contract entered into with any person outside India by any person based in India.

Overseas Profiling: digital personal data processed outside India for profiling purposes only (without being connected to any activity related to offering of goods or services to data principals in India). We believe overseas profiling (which was covered in previous iterations of the proposed law) was not ultimately included due to perceived difficulties in ensuring compliance.

You are a Data Fiduciary if you determine the purpose and means of processing of personal data such as:

Consumer personal data

Employee personal data

Primary responsibility for Compliance

Is on the Data Fiduciary, and not on the data processors that it may engage.

Compliance Measures: a Data Fiduciary is required to ensure that that it (and any data processors engaged on its behalf) take reasonable security safeguards to prevent data breaches. A Data Fiduciary must also implement appropriate technical and organisational measures to ensure effective compliance.

No standards have been prescribed in this regard presumably because these will continue to evolve but companies (and their data processors) should start putting systems and processes in place to cover:

- **Privacy by Design.**
- **Safeguards:** such as encryption, monitoring, data back-ups and staff training.
- **Incident management protocols:** such as a data breach response team, mitigation/remediation actions, forensics analysis and notification templates (to the Data Protection Board, data principals, CERT-In and law enforcement).

Breach Reporting

Notice to Data Principals: In the event of a breach, a Data Fiduciary is required to notify the DPB and each affected data principal. A previous iteration of the proposed law required notification to the regulator first, followed by the data principals if the regulator required so (basis the severity of harm and the need for the data principals to take mitigating steps).

Time Period: The form and manner of reporting are to be notified by way of rules to be issued. A previous iteration of the proposed law provided a 72-hour period within which breaches were required to be reported - the working assumption should be that a similar period will apply (but see the reporting requirement to the CERT-In).

CERT-In Notification: The parallel requirement to report data breaches to the Computer Emergency Response Team (the CERT-In) continues to apply. Data breaches are currently required to be notified to the CERT-In within 6 hours, so there may be different timelines for reporting the same incident. There is potential for inconsistent directions to be received from the DPB and the CERT-In with respect to the same incident.

Powers of the DPB with respect to Breaches

The DPB can:

- Act upon notification by data fiduciaries, or a complaint by data principals, or a reference from the government, or a court direction. Accordingly, if a global data breach (with an "India connection") occurs but is not notified to the DPB, it may nevertheless come to the attention of the DPB if it is raised by an affected data principal in India or the government.

The DPB can:

- Make inquiries into such breaches.
- Direct urgent remedial / mitigation measures to be undertaken.

Penalties

Monetary Penalties:

- Up to INR 250 crore (USD 30 million approx.) for failure to take reasonable security safeguards.
- Up to INR 200 crore (USD 24 million approx.) for failure to notify a reportable breach.

We believe that such penalties will apply to each incident (or related series of incidents) and not based on each data principal that is affected (which is the position being reported in certain press coverage at present).

No Criminal Sanctions: under the DPD Act.

Factors Affecting Penalty Quantum:

- Severity and duration of the breach.
- Nature of the personal data affected.
- The repetitive nature of the breach.
- Whether any gain has been realised or loss avoided by the data fiduciary.
- The mitigating action taken and the timeliness and effectiveness of such action.
- The proportionality of the monetary penalty.
- The likely impact of the penalty on the data fiduciary.

It will therefore be important to have effective incident management plans in place as this will be an important determining factor with respect to the quantum of penalties that are imposed.

Other Aspects

Compensation

The penalties are to be paid to the Consolidated Fund of India and the new law does not specifically contemplate the award of compensation to affected data principals.

We think it is likely that data principals will approach civil courts for compensation.

Blocking Access

If a monetary penalty by the DPB is imposed on a Data Fiduciary in two or more instances, and if considered in the interest of the general public, the DPB may make a written reference to the government advising blocking of access to Indian data principals by such a non-compliant Data Fiduciary.

Voluntary Undertaking Process

Data fiduciaries can offer a voluntary undertaking at any stage of a proceeding before the DPB.

Acceptance of the DPB stops proceedings before the regulator.

Failure to adhere to the terms of the voluntary undertaking restarts proceedings.

Anuj Bhatia
Partner
anuj.bhatia@touchstonepartners.com

Shruti Bhat
Counsel
shruti.bhat@touchstonepartners.com