Data Protection Impact Assessments under the DPDP Act, 2023

Introduction

With the enactment of the Digital Personal Data Protection Act, 2023 (**DPDP Act**) and Digital Personal Data Protection Rules, 2025 (**DPDP Rules**), India is undergoing a regulatory transition towards a comprehensive and unified data protection regime. Implementation is being undertaken in phases, affording businesses a compliance window to adapt before full enforcement takes effect on May 13, 2027. One of the compliance requirements provided under the DPDP Act relates to conducting Data Protection Impact Assessments (**DPIA**), which will be both a statutory requirement as well as a critical compliance measure.

Our latest primer series examines the statutory architecture of DPIAs, sets out the objective underlying such an assessment, and outlines its critical aspects.

Objective of conducting DPIA

A DPIA is designed to operationalize a systematic and pre-emptive process for identifying and mitigating privacy risks in advance of the commencement of any data processing activity. A DPIA ensures a structured evaluation, management, and containment of potential risks or harms that could jeopardize the statutory rights of data principals, while establishing a verifiable baseline of organizational compliance.

Statutory basis and mechanics of DPIA

Section 10(2)(c)(i) of the DPDP Act imposes an obligation on entities that will be designated as Significant Data Fiduciaries (**SDFs**).[1] to conduct a DPIA in twelve-month intervals from the date of its notification, along with an audit[2] to ensure effective observance of the DPDP Act and the DPDP Rules. The designated personnel conducting the DPIA and the audit is also required to submit a report of significant findings directly to the Data Protection Board of India (**DPBI**). Under the DPDP Act, a DPIA should include: (i) a description of the rights of the data principals and the purpose of processing their digital personal data (**DPD**), (ii) an assessment and management of the risk to those rights, and (iii) such other matters as may be prescribed.

At its core, the DPIA exercise requires an organization to map the DPD it processes, evaluate the risks such processing poses to the rights of the data principals, and implement corresponding safeguards before those risks materialize.

---

1 SDFs are entities notified by the Central Government based on the volume and sensitivity of DPD processed, risks to individuals, and potential impacts on national security or public order.

2 Rules 13(1) and (2), DPDP Rules.

Substantively, the DPIA functions as the compliance mechanism through which an SDF demonstrates that its processing activities withstand the proportionality framework articulated in the *Puttaswamy* Judgement[3] of the Supreme Court of India, comprising the legal basis, necessity and proportionality. In this sense, a DPIA is not just a procedural formality but the evidentiary mechanism against which an SDF's processing of DPD will be tested against constitutional standards.

In practice, a DPIA functions as a comprehensive due diligence tool, requiring SDFs to **evaluate**, **identify**, **assess** and **mitigate risks in** their data governance framework. This entails a structured process across four stages: (i) evaluating the nature, scope and purpose of processing activity against the legal standards, (ii) identifying specific vulnerabilities across the data lifecycle of collection, storage, transfer and eventual erasure of data, (iii) assessing the likelihood and severity of harm such vulnerabilities may pose to the rights of the data principals, and (iv) mitigating the identified risks through technical and organizational safeguards.

Relevance of DPIA beyond mere compliance obligation on SDFs

While the statutory framework confines the mandatory conducting of a DPIA to designated SDFs, the utility of the exercise extends well beyond merely meeting compliance requirements. It is a critical exercise for any data fiduciary who is looking to establish and maintain a strong data governance ecosystem. Therefore, it should be looked at as a prudent practice for any organization processing DPD. It functions as a strategic governance mechanism that institutionalizes 'privacy-by-design, proactively surfaces systemic vulnerabilities before they culminate in security incidents and other risks and establishes an auditable record of organizational accountability that is vital for sustaining market trust. Accordingly, for non-SDF entities, the proactive implementation of DPIA offers the following legal and commercial safeguards:

- **Risk Mitigation:** The DPDP Act imposes penalties of up to INR 250 crore for non-compliance. In regulatory inquiries by the DPBI, outcomes are likely to turn on whether a business demonstrates systemic care or negligence. A documented DPIA furnishes contemporaneous and defensible evidence of proactive risk management and robust compliance.
- **Preventing costly redesigns:** Evaluating privacy considerations late in a business lifecycle can lead to adopting ineffective and unresponsive data governance systems. For instance, if a health tech app is found to collect biometric data with no retention period after it has been launched, fixing it may require re-architecting the database and re-obtaining user consent. Conducting a DPIA at the design stage, by contrast, surfaces such vulnerabilities and gaps early, allowing them to be systematically addressed before deployment and avoiding these costs altogether.
- **Mitigating potential exposure on account of actions of third parties:** Under the DPDP Act, data fiduciaries remain accountable for statutory breaches committed by their third-party vendors and data processors. A DPIA enforces a robust and structured evaluation of downstream vendors handling DPD, establishing systematic control over vendor-driven exposure.
- **Preserving enterprise and transactional value:** A business with a documented history of data mapping and risk assessment demonstrates governance maturity. A robust data ecosystem will add efficiencies to potential transactions, assist in carrying out due diligence more effectively, minimize delays in closing transactions and protect valuations.

DPIA as a process

It is important to conduct the DPIA meaningfully to ensure that the exercise yields the desired outcome. As a process, DPIA involves broadly involves (i) mapping an entity's departments, teams and individuals, and the systems each uses, (ii) categorizing and classifying their data into personal and non-personal, (iii) screening for high-risk indicators such as children's data, biometric identifiers, automated decision making, and escalating to a full assessment in cases where such indicators are found, (iv) assessing existing measures to establish a baseline standard, (v) identifying gaps against this baseline and their potential adverse impacts on data principals, (vi) mapping specific controls to each risk, rather than relying on generalized safeguards, (vii) verifying access, nomination and grievance pathways, ensuring consent withdrawal

[3] *Justice KS Puttaswamy (retd.) & Anr. v. Union of India*, 2017 SCC OnLine SC 996, at para 325.

propagates downstream, and fixing a review schedule prior to deployment, and (viii) treating DPIA as a living document, to be revised upon material change in architecture, scope or vendor integration.

Key takeaways

DPIA is a prudent governance practice for any entity processing DPD, irrespective of statutory classification. Institutionalizing this as a periodic compliance exercise ensures that privacy risks are identified and mitigated well in advance. A DPIA should not be reduced to a mere inventory of data flows; it should be treated and conducted as a thorough and structured exercise to maximize the benefits. Embedding DPIA practices at the initial stages will also be significantly more cost-effective than retrofitting fixes and addressing serious gaps at a later stage, thus helping organizations avoid operational disruptions.

We hope you have found this information useful. For any queries/clarifications, please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email – *ravisekharnair@elp-in.com*

Abhay Joshi, Partner – Email – *abhayjoshi@elp-in.com*

Gauri Gupta, Associate – Email – *gauriqupta@elp-in.com*

Priyanjali Singh, Associate – Email – *priyanjalisingh@elp-in.com*