The DPDPA's Enforcement Gap: Limited Remedies for Data Principles and Independence of the DPB

INTRODUCTION

The enactment of the Digital Personal Data Protection Act, 2023 (**DPDP Act**) marked a significant milestone in India's data protection landscape. Following the Supreme Court's recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others (2017),* the DPDP Act established a dedicated legal framework governing the processing of digital personal data and introduced corresponding rights and obligations for data principals and data fiduciaries.

At the centre of this framework lies the Data Protection Board of India (**DPB**), the statutory regulatory body charged with enforcing compliance, adjudicating contraventions and imposing monetary penalties for the violations of the DPDP Act. The Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) notified by the Ministry of Electronics and Information Technology (**MeitY**) on November 15, 2025, translate the broad principles of the DPDP Act into concrete operational requirements. The DPDP Rules adopt a three-stage implementation structure, comprising immediate institutional setup, one year phase for activating the Consent Manager ecosystem and an eighteen-month phase for activating core operational compliance.

However, as the implementation progresses, attention has now turned to the adequacy of the enforcement architecture particularly regarding the remedies available to data principals and the institutional independence of the DPB. Unlike the General Data Protection Regulation (**GDPR**), the DPDP Act does not provide a direct statutory right to compensation for individuals affected by data breaches or unlawful processing. Further, the DPDP Act requires the data principals to first engage with the data fiduciary's grievance redressal mechanism before approaching the DPB.

This primer examines the limitations that the DPDP Act's enforcement framework casts on individual remedies and assesses whether the current structure adequately safeguards the rights of the data principals.

THE ENFORCEMENT ARCHITECTURE UNDER THE DPDP ACT

The DPDP Act adopts a regulatory enforcement model with the DPB serving as the regulatory authority responsible for addressing contraventions and imposing penalties. However, under the scheme of the DPDP Act, the DPB will not be the first forum for addressing the grievances of the data principals.

- ***The Requirement to Exhaust Internal Grievance Mechanisms***

Section 13 of the **DPDP Act** requires every data fiduciary and consent manager to establish an effective grievance redressal mechanism. The provision confers upon the data principals the right to have their grievances addressed by the entity responsible for processing their personal data. The DPDP Rules supplement this requirement. **Rule 14** requires data fiduciaries and consent managers to publish clear information regarding the means through which the data principals may exercise their rights and submit grievances.

As a result, the first step for a data principal seeking redress is to approach the data fiduciary itself. Only after exhausting this grievance redressal process can the matter be referred to the DPB.

- ***Practical Implications***

The requirement to first approach the data fiduciary is intended to promote efficient dispute resolution. It allows organizations an opportunity to address concerns before regulatory intervention becomes necessary and this may reduce the volume of complaints reaching the DPB.

At the same time, the requirement creates an additional procedural step for affected data principals as they are required to first seek relief from the very entity against whom the grievance is raised. While this may not present difficulties in routine cases, concerns are more acute where the complaint relates to a significant data breach, repeated non-compliance or a dispute regarding the data fiduciary's interpretation of its statutory obligations. In such cases, the requirement to first exhaust the data fiduciary's internal mechanism may delay access to regulatory remedies and increase the burden on data principals seeking redress.

LIMITED REMEDIES AVAILABLE TO DATA PRINCIPALS

The more significant challenge lies in the nature of the remedies available under the DPDP Act.

The DPDP Act does not confer upon data principals a statutory right to seek compensation for losses arising from unlawful processing or personal data breaches. This means that even where a data fiduciary is found to have violated the DPDP Act, the affected data principal does not automatically receive any monetary relief. This stands in contrast to the GDPR, where **Article 82** creates a direct and enforceable right to compensation, actionable against the data controller and data processor for both material and non-material harm arising from an infringement.

The position under the DPDP Act is reinforced by **Section 34**, which provides that all sums realised by way of penalties shall be credited to the Consolidated Fund of India, Accordingly, the enforcement framework is designed to penalise non-compliance rather than compensate the affected data principals.

The absence of a compensation mechanism represents a significant shift from the existing legal framework. **Section 43A** of the Information Technology Act, 2000 (**IT Act**) provides a statutory basis for seeking compensation in cases where a body corporate negligently fails to implement reasonable security practices and procedures, resulting in wrongful loss or wrongful gain. Section 43A of the IT Act is set to be repealed upon the DPDP Act coming into full force on May 13, 2027.

While the new framework introduces broader obligations and significantly higher penalties, it does not preserve the compensatory remedy that existed under the IT Act. The omission is particularly notable because the initial proposal for India's data protection framework did contemplate compensation rights for affected data principals. **Clause 64** of the **Personal Data Protection Bill, 2019** empowered the Data Protection Authority to award compensation to the data principal. However, this provision does not find a place in the final legislation.

Limited Internal Avenue

Section 31 of the DPDP Act introduces a limited avenue for direct relief through mediation. It provides that the DPB may direct parties to attempt mediation if it believes that a complaint is capable of resolution through that process.

The significance of mediation lies in its flexibility. Unlike the DPB's adjudicatory powers, mediation allows parties to negotiate outcomes that extend beyond regulatory penalties including corrective measures, commitments regarding future conduct, and financial settlements. In practice, mediation may provide the only avenue within the DPDP framework through which a data principal can potentially obtain direct monetary relief.

However, the utility of this mechanism is limited in practice. The DPDP Act prescribes no procedural framework for mediation. There are no timelines, no qualification requirements for mediators and no rules governing the enforceability of settlement agreements reached through this process. The effectiveness of the mechanism will therefore depend upon the requirements under the Mediation Act, 2023 as well as the DPB developing appropriate practices over time. The success of a mediation framework will also depend on the willingness of data fiduciaries to participate and the ability of the parties to reach a mutually acceptable outcome.

Section 31 introduces a degree of flexibility into the framework, but it does not substitute for a dedicated statutory compensation mechanism.

CAN DATA PRINCIPALS APPROACH COURTS UNDER THE DPDP ACT?

The absence of a compensation framework raises a broader question of whether data principals can seek remedies before courts. The answer remains uncertain.

Section 39 of the DPDP Act bars the jurisdiction of the civil courts in respect of matters that the DPB is empowered to determine. It also restricts courts from granting injunctions in relation to actions taken under the DPDP Act. This jurisdictional bar is not entirely new. Similar restrictions exist under **Section 61** of both the **IT Act** as well as the **Competition Act, 2002** which excluded the jurisdiction of civil courts in matters falling within the adjudicatory framework of those legislations. In light of **Section 39**, the extent to which individuals may pursue parallel claims before courts remain uncertain.

- ***Absence of a Private Right of Action:*** In contrast to the GDPR, which establishes a clear and enforceable right for data subjects to claim compensation from the responsible data controller or processor for material as well as non-material harm arising from an infringement, the DPDP Act does not confer upon data principals a corresponding direct private right of action against data fiduciaries.

  As a result, data principals cannot simply rely on the DPDP Act itself to seek damages before the court. Instead, they may need to rely on alternative legal frameworks to pursue compensation. This creates a degree of uncertainty that is likely to be resolved through future judicial decisions.

- ***Alternative Avenues for Redress:*** Although the DPDP Act does not provide a direct route to compensation, affected data principals may still explore remedies under other areas of law:

  - ***Tort Law:*** Traditional common law claims such as breach of confidence and negligence may be available in appropriate cases. In such proceedings, the obligations imposed by the DPDP Act may serve as evidence for standard of care expected from the data fiduciary. A claimant may argue that a failure to comply with statutory obligations supports a finding of negligence whereby breach of statutory duty is treated as evidence of negligence. This principle is well established in English common law jurisprudence, though its precise application in the context of privacy rights remains unexplored.

  - ***Consumer protection law:*** Data principals may also consider remedies under the Consumer Protection Act, 2019 (**CPA**). A failure to implement adequate security safeguards may potentially be characterized as a deficiency in service. However, a significant legal obstacle arises from the definition of 'consumer' under the CPA which requires that goods or services be acquired for consideration. Where digital services are provided without monetary consideration, service providers may challenge whether users qualify as consumers within the meaning of the statute.

- ***Constitutional remedies:*** Following the *Puttaswamy judgement,* the right to privacy now forms a part of the fundamental right to life and personal liberty guaranteed under **Article 21** of the **Constitution of India**. Consequently, serious failures by public authorities to safeguard personal data may be challenged as violations of constitutional rights of the data principals. In appropriate cases, constitutional courts may award compensation. However, such proceedings remain subject to limitations relating to maintainability and disputed questions of fact. In appropriate cases, constitutional courts may similarly award compensation for privacy violations by State actors. However, such proceedings remain subject to preliminary challenges relating to maintainability and disputed questions of fact.

INDEPENDENCE OF THE DPB

The effectiveness of the DPDP Act depends not only on the DPB's powers but also its ability to function as an independent and credible regulator.

The DPB occupies a pivotal position within the enforcement framework. It is responsible for adjudicating complaints, conducting inquiries, determining contraventions and imposing penalties. Given the breadth of these functions, the DPB's independence is critical to maintaining confidence in the data protection regime.

Section 18 and **Section 19** of the **DPDP Act** read with **Rule 17** of the **DPDP Rules** provide for the establishment and composition of the DPB. The legislation vests significant authority in the Central Government with respect to the composition and functioning of the DPB. The terms and conditions of service of the Chairperson and Members are also prescribed by the Central Government. This structural arrangement where the executive retains authority to frame the conditions under which the regulator operates is the source of the independence concern, as it leaves the DPB without the degree of statutory insulation commonly associated with autonomous regulators.

The issue assumes significance in cases where complaints may involve government departments and public sector entities. In these circumstances, the question of independence becomes particularly important. Stakeholders may question whether a regulator substantially controlled by the executive can effectively scrutinise entities that are themselves part of or closely connected to the Government.

At the same time, institutional independence of the DPB must be assessed not merely by statutory design but also by practice. The manner in which the DPB will exercise its powers, develops its procedures, and approaches enforcement priorities will play a significant role in shaping perceptions of its autonomy.

POTENTIAL AREAS OF FUTURE LITIGATION

The DPDP Act leaves several important questions unanswered, many of which are likely to be resolved through future litigation.

As the data protection regime of India becomes operational, courts may be called upon to delineate the relationship between the DPB's regulatory jurisdiction and the ability of the data principals to pursue private remedies outside the DPDP Act. The scope of the **Section 39** of the **DPDP Act** is likely to attract judicial scrutiny, particularly in cases where claimants seek damages for privacy-related harms while relying on violations of the DPDP Act as evidence for negligence or breach of duty.

The requirement that data principals first exhaust the grievance redressal mechanism of the data fiduciary before approaching the DPB may give rise to disputes concerning procedural fairness, access to remedies and circumstances in which such grievance mechanisms may be dispensed with.

Questions regarding the institutional independence of the DPB in cases involving a balance between the rights of the data principals and the interests of the government departments and public authorities are also likely to arise. In *Venkatesh Nayak v. Union of India (W.P. (C) No. 177/2026)*, currently pending before the Supreme Court of India, the petitioner has

contended that executive dominance over the appointment of the DPB compromises its independence as an adjudicatory body raising concerns about the DPB's impartiality in cases where the Government itself is the data fiduciary.

The outcome in these matters will significantly influence the effectiveness of India's data protection regime and shape the future trajectory of privacy and data protection litigation in India.

CONCLUSION

The DPDP Act significantly strengthens India's data protection framework and introduces a comprehensive system of rights, obligations and regulatory oversight. At the same time, the DPDP Act reflects a deliberate preference for regulatory enforcement over private remedies. Data principals must first pursue grievances before the data fiduciary, and even where violations are established, the DPDP Act does not provide a direct statutory right to compensation.

Alternative remedies may remain available under tort law, consumer protection law, and constitutional law. However, these remedies exist outside the DPDP framework and carry significant procedural and evidentiary uncertainties.

The role of the DPB is therefore critical. As the principal regulatory body under the DPDP Act, its effectiveness will depend not only on the powers conferred upon it but also on its perceived independence and ability to act impartially. As implementation progresses and courts begin interpreting the legislation, the balance between regulatory enforcement, individual remedies, and institutional independence will determine whether the DPDP Act delivers meaningful protection to data principals in practice.

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*

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