ARTICLE

Right Without Remedy: A Doctrinal Critique Of The Data Protection Board of India

Sreehari S[*]& Ananya Kurapati[**]

Abstract

The Digital Personal Data Protection Act, 2023 (DPDPA), establishes the Data Protection Board of India (DPB) as the primary adjudicating body for data privacy disputes. Unlike other major data protection jurisdictions with investigative, supervisory, and legislative authority, the DPB is a is a lean, penalty-focused body that operates under the executive branch's authority. This article examines three predominant issues of the DPB that undermine effective exercise of statutory rights to obtain meaningful redressal. Firstly, it evaluates the structure of the DPB, including its appointment, two-year tenure, its digitalised proceedings, and how appeals to TDSAT are delegated. These features are critically assessed in light of judicial independence and procedural fairness under Articles 14 and 21 of the Constitution. Second, it analyses the inadequacies of the evidentiary framework by identifying critical gaps in the burden of proof, particularly regarding consent managers and conflicting data minimization obligations that places unfair disadvantage on data fiduciaries. Third, it examines the DPB's remedial framework, establishing that removal of individual's right to compensation given under Section 43A of the Information Technology Act, 2000, the DPDPA leaves affected data principals with no avenue for personal relief beyond the imposition of penalties on the violator. Through doctrinal analysis, judicial precedents, and a comparative analysis with other jurisdiction models across the dimensions of institutional independence, burden of proof and individual compensation. This article demonstrates that India's enforcement model fails to provide effective redressal mechanism to aggrieved data principals, which creates a structural gap between the right to complain and the right to justice.

Keywords- Data Protection Board of India, DPDPA 2023, Institutional Independence, Burden of Proof, Remedial Framework

I. INTRODUCTION

History and jurisprudence have often acknowledged that a 'right' carefully crafted to champion justice often falls short due to a lack of an institutional framework for remedy. In Ashby v White, the House of Lords opined: "In consequence *of [this] Right or Privilege, the Possessors thereof must have a legal Remedy to assert and maintain it."*[268] There have been recurring cases where legal entitlement does not bear fruit; it is the allocation of procedural burden to structural adjudicatory bodies with a framework of remedies that makes a right genuinely operative and not merely declaratory.[269] In fields such as data protection, where information asymmetry exists,

[*] 3rd year B.com L.L.B (Hons.) Student, Institute of Law, Nirma University.
[**] 3rd year B.com L.L.B (Hons.) Student, Institute of Law, Nirma University
[268] Ashby v. White 92 ER 126 (1703).
[269] Lon L. Fuller, The Morality of Law 81–91 (rev. ed., Yale University Press 1969).

the effectiveness of statutes in these fields relies entirely on the redressal frameworks assigned to them.

Data protection frameworks around the globe do not just list down obligations, but they also create adjudicatory or supervisory institutions with investigative and adjudicatory powers vested in them.[270] By this, the enforcement framework would be constitutive of the right itself and not just a secondary feature of the regulative statute.

The parallel data protection enactment in India, the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the DPDP Act), adopts a different approach to the enforcement architecture. The DPDP Act created a streamlined adjudicatory body called the Data Protection Board of India (hereinafter referred to as the DPB) rather than the customary broad, independent body with investigative, supervisory, and legislative authority as seen in contemporary foreign laws.

The DPB is primarily responsible for investigating noncompliance, determining personal data breaches, and imposing monetary penalties for violations of law.

Therefore, it is defined not by ongoing regulatory supervision but by adjudicating noncompliance. His change in design differs from the models in which data protection authorities were considered to be independent regulators with a large oversight mandate. Under the General Data Protection Regulation (Hereinafter referred to as GDPR), for instance, the EU requires that member states create supervisory authorities that act with complete independence from the government in carrying out their responsibilities and exercising their powers.[271] These supervisory authorities have investigatory powers, corrective powers, and advisory powers, including a power to require compliance alongside a power to impose administrative fines.[272] In contrast, the DPDPA gives the Central Government very significant operational and appointment authority over the DPB, which limits its role to adjudicating and imposing penalties in the manner prescribed by laws, including subordinate legislation.

A lean, executive-based adjudicatory body emphasizes "enforcement-minimalism" because it aims for an efficient and centralized avenue for determining violations instead of creating multiple levels of a regulatory body. Although there may be effective enforcement, if a statutory right is being interpreted through an entity that has a punitive, rather than reparative role, the framework for how procedures and remedies are created will have added significance. In this sense, the type of institutional structure used by DPDPA should receive careful doctrinal consideration, not for reasons related to its policy considerations in a vacuum, but rather to understand how its institutional features relate to access to remedy under the Indian Administrative Law.

Individuals have the right under the DPDP Act to seek out the DPB in situations of non-compliance or breach of personal data.[273] However, the existence of a formal statutory forum does not guarantee an effective means of redress. Historically, administrative law has recognized that the true meaning of a right is mediated by institutional design; specifically, the allocation of burdens, the structure of remedies, and procedural safeguards will all combine to determine

[270] Council Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] arts. 51–59.
[271] GDPR art. 52(1).
[272] *Id* arts 58, 83.
[273] Digital Personal Data Protection Act, 2023, No. 22 of 2023 [hereinafter DPDPA] §§ 27–28.

whether a grievance mechanism offers true meaning or is merely an explicit declaration of rights.[274] If the enforcement architecture channels disputes to an entity that has a narrowly defined set of powers and procedures, the statutory rights may be influenced, if not restricted, by the structural design of that enforcement architecture.

Within the DPDP Act, there are three characteristics of this enforcement architecture that should be evaluated. First, the statute is almost completely silent on the allocation of evidentiary burdens in disputes where both the compliance records and the pertinent data are in the possession of the Data Fiduciary.[275] Secondly, the remedial framework is primarily penalty-driven; it permits the imposition of large monetary penalties payable to the State while failing to provide a clear compensatory jurisdiction for individual complainants.[276] Lastly, the Board must follow the rules of natural justice, but the Act and the rules do not have comprehensive rules for participatory safeguards like structured disclosures or defined hearing rights.[277] These gaps in the law are not just procedural but also affect how a complainant can succeed in getting relief from the Board.

Civil consequences for a person require fairness through procedures.[278] This is in line with the Constitution's articles 14 and 21, as fair treatment under these articles requires not only an accessible forum, but also that the rules of procedure and remedies of that forum are fair.[279] Consequently, the distinction between the right to complain and the right to obtain a remedy is structural and not just semantic. The Institutional question is whether or not the DPB's structure supports the statutory entitlement of individuals and provides significant redress or simply has individuals as the mechanism for regulatory sanction.

II. THE STATUTORY DESIGN OF THE DATA PROTECTION BOARD

a. COMPOSITION AND APPOINTMENT STRUCTURE

Section 18 of the DPDP Act, 2023, vests the Central Government with the power to constitute the DPB comprising a Chairperson and such number of Members as the Government may notify.[280] The qualities required are "ability, integrity, and standing," along with expertise in data governance, law, information and communications technology, or consumer protection.[281] Additionally, at least one member must have expertise in law. The appointment process is governed by a Search-cum-Selection Committee, chaired by the Cabinet Secretary.[282]

Disqualification of members is permissible on various grounds such as "insolvency, conviction of moral turpitude, incapacity to fulfil a member's duties, conflict of interest, or abuse of authority."[283] These must be preceded by providing an opportunity to be heard.[284]

---

[274] A.K. Kraipak v. Union of India (1969) 2 SCC 262.
[275] DPDPA §§ 8–10; cf. GDPR art. 5(2).
[276] DPDPA §§ 33–34.
[277] Id. § 28.
[278] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[279] Id.; A.K. Kraipak v. Union of India, supra note 7.
[280] DPDPA § 19(1).
[281] Id. § 19(3).
[282] Digital Personal Data Protection Rules, 2025, r. 17, G.S.R. 846(E), Gazette of India Extraordinary, Part II, Section 3(i) (Nov. 13, 2025).
[283] DPDPA § 21.
[284] Id. § 21(2).

Notwithstanding these procedural safeguards, the appointment structure raises concerns about Judicial Independence.[285] The Central Government has a degree of total control over the composition of the DPB's membership. This raise concerns over the Judicial Independence of the DPB and impartiality. In the ongoing Supreme Court case of *The Reporters' Collective and Nitin Sethi v. Union of India,* the petitioner contends that the significant concentration of appointment authority is a "complete executive domination" which violates the Constitution's separation of powers.[286]

The two-year tenure of the Chairperson and Members[287] further compounds the structural problems, such as institutional continuity and consistency of the DPB in its decision-making. The courts have always scrutinized tribunals functioning with short-term tenures due to various reasons. In the case of Rojer Mathew v. The South Indian Bank,[288] it was noted that without sufficient job security, there will be less interest from qualified individuals in accepting an appointment to a tribunal, thereby impacting the ability to provide effective and qualified approaches to institutional governance. More recently, in Madras Bar Association v. Union of India, the Supreme Court of India acknowledged that four-year appointment terms were constitutionally insufficient to provide the necessary level of security in providing an independent adjudicatory body and ordered that all members of the tribunal serve an appointment term of no less than five years.[289] The DPB's two-year appointment term clearly falls outside of the minimum requirements established by the Supreme Court for a constitutionally valid tribunal. Data protection adjudication involves technically complex inquiries that demand sustained institutional memory.[290] Frequent turnover would create a processing concern substantiated by the experience of TDSAT delays, which were referenced in Union of India v. Tata Communications.[291]

b. NATURE OF PROCEEDINGS

According to the DPDP Act, the DPB has been given quasi-judicial powers,[292] which allow them to perform the above functions, including receiving complaints, conducting inquiries, determining evidence, providing legally binding solutions, and imposing fines on cyber incidents as provided under the Act and the Code of Civil Procedure.[293] These roles are adjudicated by nature and cannot be interpreted simply as inspecting or supervising regulations.

---

[285] KS&K Advocates, Judicial Review and Appeals Under India's DPDP Act, 2023, https://ksandk.com/data-protection-and-data-privacy/judicial-review-and-appeals-under-indias-dpdp-act-2023/ (last visited Feb. 22, 2026).
[286] Deeptiman Tiwary, Why the New Digital Personal Data Protection Act Faces a Constitutional Challenge in the Supreme Court, Indian Express (2023), https://indianexpress.com/article/explained/explained-law/data-protection-act-challenge-supreme-court-10536413/ (last visited Feb. 22, 2026).
[287] DPDPA § 20.
[288] Rojer Mathew v. South Indian Bank Ltd. & Ors., Civil Appeal No. 8588 of 2019 (Nov. 13, 2019).
[289] Drishti IAS, SC Struck Down Key Provisions of the Tribunal Reforms Act, 2021, https://www.drishtiias.com/daily-updates/daily-news-analysis/sc-struck-down-key-provisions-of-the-tribunal-reforms-act-2021 (last visited Feb. 26, 2026).
[290] Medianama, India Notifies DPDP Rules 2025: DPBI Activation, https://www.medianama.com/2025/11/223-india-notifies-dpdp-rules-2025-dpbi-activation/ (last visited Feb. 22, 2026).
[291] Mahanagar Telephone Nigam Ltd. v. Tata Communication Ltd., Civil Appeal No. 1766 of 2019, (2019) 5 SCC 341.
[292] DPDPA § 27(1).
[293] Id. § 28.

Under section 28 of the act, the DPB is set to operate under the "Digital by Design" model.[294] This represents a historic first in Indian law history where a tribunal has operated completely through electronic means, beginning with receiving complaints and ending with issuing final orders.

This digital framework provides several substantive advantages in terms of procedural efficiencies. It enhances access for individuals located outside of a tribunal's jurisdiction, it eliminates the expense and inconvenience associated with attending a tribunal in person, and it has the potential to decrease the time required to complete a hearing compared to traditional tribunals.

However, these benefits must be assessed alongside their structural limitations. The exclusive reliance on digital infrastructure raises concerns regarding the exclusion of certain categories of data principals from effective participation in proceedings. Digital Awareness and the capacity to navigate quasi-judicial proceedings are two distinct competencies. Filing a formal complaint requires drafting submissions, uploading evidence, and responding to notices; these tasks require complex digital legal proficiency, which cannot be correlated with active internet usage.[295] Additionally, the DPB's ability to address intricate evidential concerns due to a lack of physical examination, which may be particularly required in high-stakes cases involving large-scale data breaches.

c. APPELLATE STRUCTURE

Section 29 of the DPDP Act designates the Telecom Disputes Settlement and Appellate Tribunal (Hereinafter referred to as TDSAT) as the appellate forum for challenges to orders of the DPB.[296]The appeals should be filed within 60 days from receipt of the order, and TDSAT is directed to dispose of such appeals within six months. This changed from the draft in 2022, which stated appeals would be heard by the High Court.[297]

The delegation of appeals to TDSAT raises two key issues. The first is one of institutional expertise. TDSAT was constituted under the Telecom Regulatory Authority of India Act in 1997 to adjudicate disputes, and its domain expertise is rooted in telecommunications, broadcasting, and related sectors.[298] Data protection law requires an understanding of the principles of informational privacy, consent, and the techno-legal issues arising from how data is processed, which is a special body of knowledge. The Supreme Court ruled in Union of India v. R.Gandhi that the credibility of a tribunal's decisions is directly related to the level of expertise among its members on the subject matter. The lack of a specific area of expertise (data protection) among members of TDSAT will diminish the ability of the appellate body to adequately review and evaluate the very complex and, in many cases, very fact-specific decisions of the DPB.

---

[294] Id.

[295] Internet & Mobile Ass'n of India & Kantar Insights, Internet in India 2023 (Mar. 4, 2024), https://www.iamai.in/research/internet-india-2023 (last visited Feb. 27, 2026).

[296] DPDPA § 28.

[297] PRS Legislative Research, Draft Digital Personal Data Protection Bill, 2022, https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022 (last visited Feb. 28, 2026).

[298] Telecom Disputes Settlement & Appellate Tribunal, Jurisdiction and Powers of TDSAT, https://tdsat.gov.in/admin/introduction/uploads/seminar_events/manjul%20bajpai%20chandigarh.pdf (last visited Feb. 28, 2026).

The second issue is of overburdening, causing a delay in the procedures. TADSAT deals with matters and appeals related to five areas of law. This has led to a significant backlog, with 3,448 pending cases between 2020 and 2025. The addition of the expectedly large number of appeals to TDSAT in relation to data will likely exceed the capacities of TDSAT and make the six-month timeframe to resolve a case unrealistic or unenforceable.

III. BURDEN OF PROOF AND EVIDENTIARY CONTROL

A foundational question in any adjudicatory framework is the allocation of the burden of proof, i.e., to determine which party has the obligation to provide evidence to support their position. With respect to data protection disputes due to the asymmetrical flow of information between data principals and data fiduciaries, the burden of proof lies with the Data Fiduciary. Section 6 (10) of the DPDP Act provides that when the Data Principal has given consent for the Data Fiduciary to use their data, but the Data Principal contends that such consent was not valid or was never given to the Data Fiduciary, then the Data Fiduciary must produce evidence of having provided proper notice of processing and obtained valid consent.[299] The evidence produced may include timestamped logs, screenshots, audit trails, etc.

While placing the burden of proof on the respondent (data fiduciary) is contrary to the General Burden of Proof Doctrine, this is consistent with global data protection laws. For example, under Article 7(1), the GDPR requires that the Data Controller demonstrate that the Data Subject has consented to Data Processing.[300] Additionally, the Data Controller is required to maintain proof of receipt of the Data Subject's consent for as long as the Data Processing is being performed.[301] Likewise, China's PIPL and Brazil's LGPD laws have adopted this controller accountability rule in their legislation.[302][303] While this ensures stronger accountability of data fiduciary and alignment with global standards, there are certain distinct gaps yet to be addressed by the law.

a. CONSENT MANAGER GAP

The DPDPA introduces the concept of a 'Consent Manager', a third-party agent who can hold or transfer consent records of personal data.[304] When a data principal stores their records of consent, such as a digital locker or their account on a consent manager's website. Consequently, the fiduciary is no longer in control of the record of consent that they have provided to the company.[305] The act does not carve out any exceptions to Section 6(10) to account for this scenario, nor does it clarify whether the evidentiary obligation shifts to the consent manager or whether it remains with the fiduciary. This creates an evidentiary vacuum where proof is the most consequential. This gap should be addressed by the DPB inevitably without any statutory guidance.

---

[299] DPDPA § 6(10).
[300] GDPR art. 7.
[301] Id. art. 7(1).
[302] Personal Information Protection Law of the People's Republic of China art. 9 (2021).
[303] Lei Geral de Proteção de Dados Pessoais [LGPD] [General Data Protection Law], Law No. 13,709, de 14 de agosto de 2018, art. 6(VI) (Braz.).
[304] DPDPA § 2(g).
[305] Digital Personal Data Protection Rules, 2025, r. 4, First Schedule, G.S.R. 846(E), Gazette of India Extraordinary, Part II, Section 3(i) (Nov. 13, 2025).

b. QUALITY AND DISGN OF CONSENT RECORDS

Another significant issue arises from the quality of consent records produced before the DPB. The mere existence of a consent record does not establish the consent as legally valid. This was observed in a case investigated against WhatsApp in 2021 regarding proper consent for sharing user information within the Meta company.[306] Although WhatsApp presented internal records to demonstrate that users accepted changes to the terms and conditions of their account, the Spanish Data Protection body found that the manner in which the user interface was designed effectively meant that users were assumed to have accepted the updated terms simply through continued use of the application. Accordingly, even though there were system logs showing users had agreed to share their data, the AEPD held that the documented "consent" was inadequate for legal purposes. Similarly, in the case against Google, where their interface design made it much easier for users to agree than to refuse, it harmed proving whether or not consent was truly 'freely given'.[307] In such situations, several procedural challenges would be created.

c. RETERNITION PERIOD CONFLICT AND ADVERSE INFERENCE

There is no clear indication in either the Act or the Rules on the duration for which data fiduciaries should keep consent records post-consent and whether the fiduciary must have consent records available only during the course of processing, or even after the data subject has withdrawn consent. Section 8(7) imposes a data minimisation obligation on fiduciaries, requiring them to limit retention of personal data once the purpose has been met.[308] Which means the fiduciary must delete the records once the consent has been withdrawn or upon completion of processing.

This clashes with the Section 6 (10) provision, creating unresolved tension between data minimisation mandates and evidentiary accountability. Additionally, pursuant to Section 111 of the Bharatiya Sakshya Adhiniyam, 2023, courts are permitted to make adverse inferences as a result of missing or non-produced evidence; thus, it is unclear whether such inferences would exist in the absence of the consent record. For instance, if a fiduciary deletes consent records in legitimate compliance with Section 8(7) and is subsequently required to produce them before the DPB, it faces the prospect of an adverse inference despite having acted in good faith.

Overall, these issues create not just a procedural inconvenience but impair data principals' ability to obtain any real relief from the DPB. This is a type of procedural inadequacy guaranteed by Indian administrative law and by Articles 14 and 21, which require correction.

IV. REMEDIAL MODEL

The DP DPB is responsible for enforcing the DPDP Act, 2023, through civil monetary penalties imposed by the authority, in accordance with the relevant section of the DPDPA. The DPB will impose a penalty after investigating the matter, in accordance with the prescribed amounts outlined in the Schedule under Section 33(1) of the DPDP Act.[309] The schedule lists various types of violations; however, the maximum penalty for breaches resulting from a data fiduciary's

[306] Agencia Española de Protección de Datos (AEPD), Resolución PS/00477/2021, WhatsApp Ireland Ltd. (2021).
[307] Commission Nationale de l'Informatique et des Libertés (CNIL), Délibération SAN-2019-001, Google LLC (Jan. 21, 2019), https://www.cnil.fr (last visited Feb. 27, 2026).
[308] DPDPA § 8(7).
[309] Id. § 33(1).

failure to take appropriate measures to protect the confidentiality or integrity of data is 250 crore rupees (over 100 crore rupees). The schedule also lists other penalties for data breaches and failures to comply with obligations regarding children's or sensitive data.[310]

In addition to the data fiduciary's wilful or negligent actions, the DPB must take into account several considerations in determining the appropriate penalty to impose for violations under the DPDPA, including: (1) the type of personal data involved in a loss/breach; (2) the frequency of the breach (i.e., repeat violation); and (3) whether the penalty is proportionate to the misconduct.[311] These criteria indicate that the law provides for penalties that serve to deter further violations rather than compensating victims of prior violations.

Section 34 of the DPDP Act is the most fundamental provision regarding the imposition of fines for violations of the DPDP Act and establishes that all fines imposed for violations of the DPDP Act will be deposited into the Consolidated Fund of India.[312] This provides an important legal ruling about where fines for violations (e.g., when the data principal's data is breached) will go – being that a fine will not be paid to the plaintiff – and indicates that violations of the DPDP Act should be treated as regulatory violations under the DPDPA, rather than as a civil injury for an individual plaintiff.

a. UNAVAILABILITY OF COMPENSATORY JURISDICTION

While the DPDP Act does not provide the DPB with any specific authority to award compensation to the data principals, Section 27 of the DPDP Act grants the DPB the ability to hold inquiries on alleged breaches once they receive a complaint or notice, and provide a remedy through the imposition of penalties or the direction of remedial actions.[313] Remedial actions are described primarily in regulatory terms (e.g., mitigating actions, directions for compliance) rather than restitution/compensation.

This deficiency is particularly noteworthy when contrasted with the previous regulatory scheme established by the IT Act 2000. Section 43A of the IT Act explicitly states that if a corporate entity (individual or company) fails to reasonably protect its data, it shall be subject to civil damages (compensatory payment) for any loss suffered by a victim of the data breach.[314] This provision gave adjudicative agencies the authority to provide monetary compensation to individuals who had suffered loss due to a data breach.

The DPDP Act repealed Section 43A[315]; however, the DPDP Act has not created a comparable civil remedy scheme. The structural omission is that the DPB removed the regulatory and civil redress facets of the original regime and replaced it with a penalty-based/economic-based enforcement system with no restoration to the victims.

The fundamental difference between penalty and remedy is fundamental to the doctrine — penalties serve as a means of defending public regulatory norms while remedies serve as a means of defending private injuries, and the distinction can also be understood with respect to their deterrent effect (penalties serve to deter future breaches, whereas remedies serve to put an injured

[310] Id. sch.
[311] Id. § 33(2).
[312] Id. § 34.
[313] Id. § 27.
[314] Information Technology Act, 2000, No. 21 of 2000, § 43A (as enacted, repealed 2023).
[315] DPDPA § 44(2).

party back in the position they'd have been had the breach not occurred). The DPDP Act clearly favours penalties over remedies.

b. NON-TRANSLATION OF PENALTIES ON CONSENT MANAGERS

Under section 6, consent managers have a duty to manage consent properly and may be penalised for failing to do so as prescribed in the Act.[316] Therefore, if a consent manager breaches their duties by mishandling personal data or failing to meet their statutory obligations, the DPB may impose monetary penalties under the powers granted in section 33 and the Schedule.[317]

However, even where a consent manager breaches their duties, the data principal does not have a statutory right to compensation. All penalties, regardless of amount, go into the Consolidated Fund under section 34[318], so the data principal's injury will remain unredressed from a legal perspective under the DPDP Act.

The above demonstrates one of the key points of this discussion: the enforcement of the DPDP Act is a vertical (state and regulated entity) process rather than a horizontal (the injured individual and the wrongdoer) restorative process, and the right to complain under section 27 does not equate to the right to recover financial damages.

c. COMPENSATION UNDER IT ACT

In State Bank of India v. Prashant Mahadeorao Buradkar, the Court illustrated the practical effect of this change. The crime of fraud occurred when the perpetrator obtained a duplicate SIM card and diverted funds from the victim's bank account. The adjudicating body exercised its powers under section 43A of the IT Act and ordered compensation to the victim.[319]

The ruling also highlights how earlier law had a restorative capacity. The adjudicating authority did not simply punish non-compliance with regulations; it ordered financial compensation to the victim. Under the DPDPA, a similar data breach now leads to either a regulatory review or a potential penalty against the violator; however, there is no statutory foundation for issuing compensation to the victim of data breaches. Therefore, the resolution for victims has gone from restitution to sanctions.

d. RESTORATION V DETERRENCE

DPDP Act's mechanism for providing remedies is based on the concept of deterrence through enforcement. The penalties imposed under the Schedule are extremely large (hundreds of crores) and therefore show that the DPDP Act was designed to provide companies with an incentive not to engage in improper activity through a monetary penalty.[320]

Deterrence is not the same idea as restitution. Administrative law literature has shown that the ability to access justice includes not only penalties, but also substantive remedies to those harmed. A recent case before the Supreme Court, Maneka Gandhi v. Union of India, discussed the necessity of procedural fairness pursuant to Article 21 and what the Court meant by "right,

---

[316] Id. § 6.
[317] Id. § 33.
[318] Id. § 34.
[319] State Bank of India v. Prashant Mahadeorao Buradkar, Cyber Appeal No. 6 of 2014 (Telecom Disputes Settlement & Appellate Tribunal, Sept. 12, 2024).
[320] DPDPA sch.

just and fair.[321]" If a system allows the filing of a complaint, but does not allow a remedy to those who have filed complaints, it is providing the opportunity for procedural participation, but ultimately does not provide any substantive opportunity for an individual to seek a remedy.
The DPDP Act provides for regulatory enforcement at the expense of restitution for individuals. Although an individual can file a complaint to seek enforcement action, they cannot rely on the enforcement process to recover their loss.

e. DOCTRINAL RAMIFICATION

DPDPA provides an avenue for filing grievances and has a thorough process for the imposition of sanctions by the regulator. However, the DPDP Act does not confer a right of redress in a compensatory sense to a data subject. Consequently, while violators such as consent managers face penalties for their actions, those penalties do not provide restitution to the data subject.
In summary, there are no remedies for affected data subjects. There is some regulatory deterrence, but no means of providing restorative justice. When a right does not have a corresponding remedy associated with it, it cannot be fulfilled. The distinction between enforcement and redress is therefore not merely an issue of language, but rather it is one of doctrine, as shown by the reference to Sections 27, 33, and 34 of the Act and the repeal of Section 43A of the Information Technology Act.

V. COMPARATIVE ANALYSIS OF DIFFERENT JURISDICTION

In this section, we'll analyze data protection statutes of other jurisdictions (namely European Union, the United Kingdom, Singapore and Brazil) to check (1) whether compensation to individuals exists, (2) where the burden of proof sits, and (3) the degree of institutional independence.

a. COMPENSATION TO INDIVIDUAL

The four regimes provide for a right to damages for people whose data has been processed improperly, but there are also significant differences. Under the GDPR in the EU, for example, anyone suffering "material or non-material" damage as a result of processing can claim compensation from the controller or processor.[322] In addition, controllers are jointly and severally liable, meaning they must compensate data subjects unless they can prove that the element of liability raised by the data subject was outside their control.[323] The UK continues to provide the same right to compensation through the UK GDPR and the Data Protection Act 2018, and also specifically recognises emotional distress as an example of "non-material" damage.[324] However, following Lloyd v Google LLC, there is a requirement that there must be evidence of harm for a claim to succeed and that a simple loss of control is not sufficient.[325]
Singapore's PDPA provides a private right of action for anyone who suffers "loss or damage directly" in accordance with section 48O.[326] The Reed v Bellingham case recently confirmed that emotional distress qualifies for compensation as well, and so has significantly broadened the

[321] Maneka Gandhi v. Union of India, supra note 11.
[322] GDPR art. 82(1).
[323] Id. art. 82(2)-(3).
[324] Data Protection Act 2018, c. 12, § 168 (UK).
[325] Lloyd v Google LLC [2021] UKSC 50, [74]–[79].
[326] Personal Data Protection Act 2012, No. 26 of 2012, § 48O (Sing.).

restrictive application of prior cases.[327] Article 42 of Brazil's LGPD imposes strict tort liability on controllers and processors to compensate for any material or moral damage caused to an individual as a result of processing that individual's data.[328] Compensation for damages will apply to both monetary and non-monetary losses, and responsibility can be held by multiple parties.[329]

The procedures for remediation under each regulatory framework influence how affected individuals may access justice. The EU and the UK both allow individuals to seek compensation via lawsuits and through payment by controllers and processors of fines imposed by data protection authorities, under Articles 82 and 83 of the GDPR and section 168 of the DPA 2018.[330] However, the availability of mechanisms for collective compensation is limited. In Singapore, individuals may commence lawsuits under section 48O as an option available to them.[331] The PDPC can also conduct investigations to determine whether an organization has violated its duties under the PDPA. In Brazil, individuals may sue under Article 42 of the LGPD, and the ANPD may impose administrative penalties on violators under Article 52 of the LGPD.[332]

b. BURDEN OF PROOF

The evidentiary burden of proof also varies significantly among jurisdictions. Under Article 82 of the GDPR, once an individual establishes that he/she sustained a loss and violated the law, the burden shifts to the data controller or processor to establish that he/she has not assumed responsibility for damages incurred by the individual.[333] The accountability principle described in Article 5 of the GDPR requires data controllers to demonstrate compliance with the law.[334] Under section 7 of the GDPR, the accountability principle requires the data controller to produce sufficient evidence to demonstrate that the individual gave his/her consent.[335]

The UK continues to have a statutory framework governing the accountability of data controllers and processors, through the incorporation of the GDPR into English law via the UK Data Protection Act 2018.[336] Compensation is still dependent on proof of loss or distress, as ruled in Lloyd v Google.[337]

The PDPA in Singapore does not include a statutory shift of the burden of proof clause. Thus, conduct and harm must be proven under section 48O.[338] Recently, tortious claims for emotional distress have been recognized as an available remedy in Singapore courts, but plaintiffs will be required to establish that the emotional distress suffered was the inconvenience suffered as a result of the organization's violation.[339]

---

[327] Reed v Bellingham [2022] SGCA 60, [72]–[75].
[328] LGPD art. 42.
[329] Id. art. 42(1).
[330] GDPR arts. 82–83; Data Protection Act 2018, supra note 57, § 168.
[331] Personal Data Protection Act 2012, supra note 59, §§ 48I–48J, 48O.
[332] LGPD art. 52.
[333] GDPR art. 82(3).
[334] Id. art. 5(2).
[335] Id. art. 7(1).
[336] Data Protection Act 2018, supra note 57, § 3.
[337] Lloyd v. Google LLC, supra note 58, [55]–[60].
[338] Personal Data Protection Act 2012, supra note 59, § 48O.
[339] Reed v. Bellingham, supra note 60, [89]–[92].

The Brazilian government now takes a more interventionist approach to privacy protection. The General Data Protection Law (LGPD) allows for courts to shift the evidentiary burden onto the data subject if there is sufficient evidence that the subject has a valid claim and that producing evidence would be an overly burdensome task for them.[340] Moreover, it is also the obligation of the data controller to provide evidence of the existence of valid consent by producing such evidence to the data subject at or before the first use of that data.[341]

c. INSTITUTIONAL INDEPENDENCE

International data protection authorities must implement and enforce regulations on Member States without any political influence.[342] According to GDPR, authorities must function independently, and at a minimum, must have a process to ensure independence from any outside interference.[343]

The United Kingdom has its own Information Commissioner; therefore, the ICO is an independent organization that performs its functions under the Data Protection Act 2018.[344]

In Singapore, the PDPC is a public body created by the Personal Data Protection Act, thus operating as part of the executive branch of government. The PDPC has the authority to investigate and penalize organisations, although it is similar.[345] In many respects, the Independent Commissioner was established under the GDPR.

The Autoridade Nacional de Proteção de Dados (ANPD) is a federal agency in Brazil officially launched in January 2020, created via combinative effect of the executive and legislative branches of government, as defined under Federal Law No. 13,853 enacted in July 2019 and entered into force later that year.[346]

Each country has established different levels of regulatory authorities and operational requirements, resulting in significant variances in terms of the level of regulatory authority established by each country. In both the EU and the UK, independence (from the executive) is a constitutional feature of enforcement; Singapore's model is still regulator-focused but has ties to the executive; and Brazil's model is in transition to independent regulatory authority. Each system's degree of independence will play an important role in shaping both enforcement intensity and the credibility of remedial protections provided.

VI. CONCLUSION

The DPDP Act, 2023, represents a significant legislative milestone in India's journey toward formalising data protection rights. However, the existence of a statutory remedy does not signify meaningful redressal. While DPB has the statutory foundation to become a genuine instrument of individual redress, the present framework is required to be reformed to achieve its full potential.

---

[340] LGPD art. 42(2).
[341] Id. art. 8(2).
[342] GDPR art. 52(1).
[343] Id. arts. 52–54.
[344] Data Protection Act 2018, supra note 57, §§ 114–116.
[345] Personal Data Protection Act 2012, supra note 59, § 3.
[346] Lei No. 13,853, de 8 de Julho de 2019 (Braz.).

The three central issues have been identified in this paper about the statutory structure and procedure of DPB. The institutional design of the DPB, such as its two-year term,[347] Its reliance on being appointed by the executive,[348] The fact that it is only an electronic-based tribunal, and that appeals are heard within a confused and overworked TDSAT, creates concerns about the independence,[349] expertise and accessibility that effective adjudication requires. The 2nd major weakness of the current regime is with the evidentiary framework. In theory, it is progressive by placing the burden of proof upon data fiduciaries.[350] However, it is fraught with ambiguities, particularly in relation to the role of consent managers, the legal adequacy of consent records, and the irreconcilable tension between the data minimisation requirements of section 8(7) and the evidentiary accountability imposed by Section 6(10)[351]. These are fundamental interpretive gaps; they are structural inconsistencies that will dictate whether a data principal can succeed before the DPB. The third main weakness in the current regime is based on deterrence rather than a reparative remedy. The repeal of section 43A of the IT Act (2000),[352] Without a like-for-like civil compensation arrangement, has resulted in a regime where there is punishment for regulatory violations but no compensation for individuals who suffered losses. All fines are payable to the Consolidated Fund of India, leaving any aggrieved data principal with no remedy. The comparison of regulatory mechanisms in India with the EU, UK, and Brazil shows how India can improve its system by reforming toward a stronger adjudicatory capacity. With the DPB set to become fully operational by May 13, 2027[353], there is a narrow but still available window for meaningful corrective action. Several practical reforms achievable without amending the entire act should be prioritized by the 3 constitutional pillars.

The current appointment mechanism has to be reformed to include meaningful participation from the judiciary or an independent collegium rather than giving sole power to the government. This is to ensure the DPB functions as a credible adjudicatory forum rather than an instrument of executive policy. Additionally, the length of tenure for which DPB members serve has to be revisited because their two-year terms contradict the constitutionally mandated minimum five-year term (determined by Madras Bar Association v. Union of India).[354] By extending DPB members' terms of office through subordinate legislation or amendment, there will be an extension of the length of time for which each member has served, thereby addressing both the Constitutional requirements and creating the institutional memory needed for the technically complex process of determining data protection.

The Central Government should develop rules under Section 6(10) that clarify evidentiary obligations in a consent manager context, indicating how long an organization must retain consent records for adjudicative focuses; establish that good-faith deletion will not carry negative

[347] DPDPA § 19.
[348] DPDPA § 18.
[349] DPDPA § 29.
[350] DPDPA § 6(10).
[351] Id.
[352] Information Technology Act, 2000, No. 21 of 2000, § 43A (as enacted, repealed 2023).
[353] Eesha Bagga Bhargava, India's New Data Protection Era Begins: A Practical Guide to the DPDP Act and DPDP Rules, 2025, Taxmann (2025), https://www.taxmann.com/research/company-and-sebi/top-story/105010000000027395/indias-new-data-protection-era-begins-a-practical-guide-to-the-dpdp-act-and-dpdp-rules-2025-experts-opinion (last visited Feb. 28, 2026).
[354] Madras Bar Association v. Union of India (2021) 7 SCC 369.

implications for an organization in compliance with Section 8 (7) and clarify the evidence standard will not be lower than that set forth by the agency to prevent contradictory statutory obligations from systematically undermining the data principal's ability to establish a case.

On the remedial side, the DPDP Act can restore a compensatory jurisdiction to the DPB, mirroring the civil damages framework previously provided by Section 43A of the IT Act. In any case, Section 40 rules should allow for the DPB to make a recommendation for compensation as part of its directions to remediate a violation, even though the amount of the compensation is ultimately determined by a civil proceeding. The current scenario wherein a complainant can establish a violation but is not entitled to any damages does not represent a viable legal principle and runs counter to the constitutional minimum requirement for access to meaningful justice outlined in Maneka Gandhi v. Union of India.[355]

Finally, as well as having a solely digital DPB, individuals who are filing a claim before the DPB and who do not possess the digital skills required to do so will need to be provided with assistance in filing their claims through legal aid, helpline support, and/or through access to intermediary representatives who will file the claims for them so that they are not excluded, without knowing, from the forum that was created to assist them.

[355] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.