ARTICLE

Digital Personal Data Protection Act, 2023: Compliance Architecture and Emerging Professional Implications

The primary objective of the DPDP Act, 2023 is disclosed in the long title of the Act. It clearly states that the Act seeks to enable the processing of digital personal data in a manner that recognises not only the right of individuals to protect their personal data but also the need to process such data for lawful purposes.

Dr. Sajoy P. B.
Associate Professor, Department of Commerce
Sacred Heart College, Autonomous, Kochi, Kerala
sajoypb@shcollege.ac.in

Dr. Ajoy P. B.
Advocate, High Court of Kerala
Ernakulam, Kerala
ajoypb@gmail.com

INTRODUCTION

The Central Government has, after much delay and debate, notified the timeline within which the Digital Personal Data Protection Act, 2023 (DPDP Act, 2023)[1] will be enforced. Considering the apprehensions raised by various sections of society including corporates, non-governmental organizations and civil rights activists, the Central Government has adopted an eighteen-month step-by-step rollout programme for enforcing the Act.

As a first step, the provisions relating to the Data Protection Board of India (DPBI) have been enforced with effect from 13.11.2025. By a separate notification, the said Board has been established with its Headquarters at the National Capital Region of India.[2] The total strength of the Board has been fixed at four members.[3] The next step involves the bringing into force those provisions of the Act relating to Consent Managers and their registration with the Board, with effect from 13.11.2026. Finally, the remaining provisions of the Act, including the new rights and liability regime, will come into force on 13.05.2027. Till then, the criminal liability regime already existing under the Information Technology Act, 2000 will continue.[4]

This one-and-a-half-year transitional period provides all stakeholders with sufficient time to adapt themselves to the new liability regime that will eventually come into force. This article provides a bird's-eye view of the new legal framework being set up under the DPDP Act, 2023.

CONCEPTUAL FRAMEWORK

The primary objective of the DPDP Act, 2023 is disclosed in the long title of the Act. It clearly states that the Act seeks to enable the processing of digital personal data in a manner that recognises not only the right of individuals to protect their personal data but also the need to process such data for lawful purposes. A definition has been provided in the Act for 'data'[5] and 'personal data'[6] with the intent of clearly defining the scope of the legislation. Every representation of information, facts, etc. that is shared or stored in cyberspace and is capable of being communicated, interpreted, or processed is defined as data. However, only such data about any individual that discloses some aspect of its identity is treated as personal data. Examples of personal data of an individual includes his/her name, age, image, gender, address, phone number, PAN card details, Aadhaar details, bank account details, credit card details, etc.

To achieve the objectives of the Act, four conceptual entities, namely: (a) Data Principal,[7] (b) Data Fiduciary,[8]

1. *See G.S.R. 843(E) [F. No. AA-11038/1/2025-CL & ES], dated 13.11.2025*
2. *See G.S.R. 844(E) [F. No. AA-11038/1/2025-CL & ES], dated 13.11.2025*
3. *See G.S.R. 845(E) [F. No. AA-11038/1/2025-CL & ES], dated 13.11.2025*
4. *See Section 43A of the Information Technology Act, 2000. The said provision will be repealed by virtue of Section 44(2)(a) of DPDP Act, 2023 when the new penalty-based liability regime comes into force on 13.05.2027*
5. *Section 2(h) of the DPDP Act, 2023*
6. *Section 2(t) of the DPDP Act, 2023*
7. *Section 2(j) of the DPDP Act, 2023*
8. *Section 2(i) of the DPDP Act, 2023*

(c) Data Processor[9] and (d) Consent Manager[10] have been created. Data Principal refers to an individual whose personal data is being processed whereas Data Fiduciary refers to any person who determines the purpose and means of processing the personal data of Data Principals. Data Processor refers to any person who is engaged by the Data Fiduciary for processing the personal data of Data Principals.[11] For example, suppose an individual 'A' purchases medicines from an online pharmacy 'B'. In addition to the medical prescription, 'A' may provide his credit card details to 'B' for making payments. 'A' may also provide his postal address to 'B' for delivering the medicines. 'B' may engage 'C' to process the personal data of customers like 'A'. Here, 'A' is the Data Principal, 'B' is the Data Fiduciary, and 'C' is the Data Processor.

A Data Principal may engage himself/herself in several transactions with different Data Fiduciaries. Since it is practically difficult for a Data Principal to keep an updated record of all personal data given by him/her to different Data Fiduciaries, the Act permits the Data Principal to take the assistance of any Consent Manager who is registered with the Data Protection Board of India.[12] The Consent Manager is essentially an online platform where a Data Principal can store his/her personal data. He/she uses the said platform for the purpose of giving/withdrawing consent to the processing of his/her personal data by various Data Fiduciaries onboarded onto the platform and subscribed by him/her for availing various services. Thus, the Consent Manager acts as an intermediary between the Data Principal and the Data Fiduciary.[13]

> Through the DPDP Act, 2023, Parliament has laid down a strong regulatory framework for efficient processing of digital personal data even while safeguarding the privacy rights of individuals.

The DPDP Act, 2023 imposes several obligations on a Data Fiduciary in relation to the personal data of a Data Principal which must be fulfilled before or at the time of processing the said data for business or other lawful purposes. The primary obligation is to obtain the consent of the Data Principal before processing his/her personal data. The consent obtained from the Data Principal must be free, specific, informed, unconditional, unambiguous and accompanied by a clear affirmative action. The DPDP Act and Rules require Data Fiduciaries to issue notices in simple language to the Data Principal while obtaining consent.[14] Also, the personal data can be processed only to the extent necessary for fulfilling the purpose for which consent was obtained.[15]

Further, the Data Fiduciary is under a statutory obligation to stop further processing of the personal data of a Data Principal once the Data Principal withdraws consent.[16] For the purpose of enabling easy withdrawal of consent, the original consent notice should contain an online communication link that can be utilised by the Data Principal for withdrawing the consent.[17]

The Act also requires a Data Fiduciary to provide a grievance redressal mechanism for enabling the Data Principal to redress any grievance.[18] Additionally, every Data Fiduciary is tasked with an obligation to promptly report every personal data breach to the Data Protection Board of India as well as to each affected Data Principal.[19]

Even though the Act prescribes a consent-based data processing regime, it also permits the Data Fiduciary to process the personal data of a Data Principal independent of his/her consent in certain limited circumstances like responding to medical emergencies, for complying with judicial orders, for taking measures during disasters or epidemics, for protecting intellectual property rights of employers, for protecting the sovereignty and integrity of India or security of the state, for complying with any obligation under law, etc.[20]

DATA PROTECTION BOARD OF INDIA (DPBI)

The Act empowers the Central Government to establish a Data Protection Board of India (DPBI) for ensuring effective implementation of the DPDP Act, 2023.[21] The Board consists of a chairperson and three members (all of them appointed for a term of two years) having expertise in law, dispute resolution, digital economy, administration, data governance, etc.[22] The primary function of the Board is to inquire into complaints made by a Data Principal in respect of any personal data breach or failure of the Data Fiduciary/ Consent Manager to observe statutory obligations and impose penalty as provided under the Act, after inquiry.[23] Its duties also include taking quick remedial responses to any intimation of personal data breach by any Data Fiduciary.[24]

The Board, in the performance of its functions, is vested with several powers of a Civil Court, including powers to issue interim orders.[25] The Board is also expected to follow the principles of natural justice while performing its adjudicatory functions.[26] The orders of the Board are subject to appeal before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) constituted under the Telecom Regulatory Authority of India Act, 1997.[27]

9. *Section 2(k) of the DPDP Act, 2023*
10. *Section 2(g) of the DPDP Act, 2023*
11. *Section 8(2) of the DPDP Act, 2023*
12. *Sections 6(7) to 6(9) of the DPDP Act, 2023*
13. *See First Schedule of the DPDP Rules, 2025*
14. *Sections 4, 5 and 6 of the DPDP Act, 2023*
15. *Section 6(1) of the DPDP Act, 2023*
16. *Sections 6(4) to 6(6) of the DPDP Act, 2023*
17. *See Section 6(3) of the DPDP Act, 2023 and Rule 3 of the DPDP Rules, 2025*
18. *Section 13 of the DPDP Act, 2023*
19. *Section 8(6) of the DPDP Act, 2023*
20. *Section 7(c) to 7(i) of the DPDP Act, 2023*
21. *Section 18 of the DPDP Act, 2023. DPBI has already been established. See supra note 2*
22. *Sections 19 & 20 of the DPDP Act, 2023*
23. *Section 27(2) of the DPDP Act, 2023*
24. *Section 27(1) of the DPDP Act, 2023*
25. *Section 28(10) of the DPDP Act, 2023*
26. *Section 28(6) of the DPDP Act, 2023*
27. *Section 29 of the DPDP Act, 2023*

LIABILITY REGIME

The DPDP Act, 2023 seeks to replace the existing criminal liability regime for data protection[28] with a penalty-based liability regime.[29] Under the new liability regime, if the Data Protection Board of India, on an inquiry conducted by it, determines that there has been a significant breach of the provisions of the Act by any person, then it is empowered to impose monetary penalties on that person, after hearing him.[30] While the Schedule to the Act specifies the maximum penalties that can be imposed for different breaches,[31] the actual quantum of penalty to be imposed has to be determined by the Board after taking into consideration several factors including the nature, gravity, and duration of the breach, the type and nature of the personal data affected by the breach, the repetitive nature of the breach, whether the person responsible for the breach has derived any benefit from the breach, whether effective and timely steps were taken to mitigate the effects of the breach and the likely impact of the monetary penalty on the person responsible for the breach.[32]

MISCELLANEOUS FEATURES

Apart from the broad features discussed above, the Act has incorporated several additional features. The Act requires the Board to explore the possibility of resolution of complaints by mediation or by any other alternate dispute resolution mechanism.[33] The Central Government has powers under the Act to strictly regulate the transfer of personal data by a Data Fiduciary to any other country or territory outside India.[34] Further, the Act empowers the Central Government to classify Data Fiduciaries as Significant Data Fiduciaries based on several factors such as the volume and sensitivity of personal data processed, risk to the rights of Data Principals and the legitimate concerns of the state relating to security, sovereignty, and integrity of India.[35] Once so classified, the Data Fiduciary will have to meet additional statutory obligations such as conducting periodic independent data audits, undertaking Data Protection Impact Assessment and appointing a Data Protection Officer based in India who will be responsible to the governing body of the Data Fiduciary.[36] The Act also allows the Central Government, on a reference made to it by the Board, to block access by the public to any information hosted by a Data Fiduciary under certain circumstances after hearing the Data Fiduciary.[37]

IMPACT ON THE PROFESSION OF COMPANY SECRETARY

Once the DPDP Act, 2023 becomes fully operational in May 2027, Company Secretaries will need to prepare additional compliance reports particularly for data-driven companies. Unless adequately trained, Company Secretaries will have to rely on the reports prepared by cybersecurity professionals and data auditors. Hence, there is an urgent need for capacity building in cybersecurity and data protection laws for Company Secretaries. This objective can be achieved in the short term by organising training programmes, seminars, workshops, refresher courses, etc. In the long term, the syllabus of the Company Secretary programme may have to be suitably modified to include topics relating to digital data protection and cybersecurity compliance.

CONCLUSION

Through the DPDP Act, 2023, Parliament has laid down a strong regulatory framework for efficient processing of digital personal data even while safeguarding the privacy rights of individuals. The Act is being enforced in a gradual and phased manner so as to give sufficient time to the Data Fiduciaries and Consent Managers to put in place the infrastructure necessary to comply with the provisions of the Act. When fully enforced, the DPDP Act, 2023 will go a long way to advance the objectives of Digital India.

28. *Section 44(2)(a) of the DPDP Act, 2023*
29. *Section 27(1)(b) of the DPDP Act, 2023*
30. *Section 33(1) of the DPDP Act, 2023*
31. *The maximum penalty imposed under the Act can be as high as ₹250 crores. See Schedule of the DPDP Act, 2023*
32. *Section 33(2) of DPDP Act, 2023*
33. *Section 31 of the DPDP Act, 2023*
34. *Section 16 of the DPDP Act, 2023*
35. *Section 10(1) of the DPDP Act, 2023*
36. *Section 10(2) of the DPDP Act, 2023*
37. *Section 37 of the DPDP Act, 2023*