Contours of Personal Data under the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 (**DPDP Act**) along with the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) regulates the processing of digital personal data[1] of data principals and casts obligations on data fiduciaries in respect of such data. Therefore, the data protection framework becomes applicable only if 'personal data' is being processed. The DPDP Act adopts a broad definition of personal data, leaving some ambiguity around its precise contours. In this context, this primer attempts to examine the scope of what may constitute personal data under the DPDP Act.

PERSONAL DATA UNDER THE DPDP ACT

What is data? The DPDP Act defines data as *"representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means."*[2] In simple terms, "data" refers to information that is represented or recorded in a way that allows it to be communicated, understood, or processed, either by a person or through automated processes (such as software) without continuous human involvement. This covers a wide range of information that can be processed and is in line with the definition of data under the Information Technology Act, 2000.[3]

What is personal data? It means any data about an individual who is **identifiable by** or **in relation** to such data.[4] Since personal data can only be of an individual, the DPDP Act does not apply to data of juridical persons such as companies, partnerships, or societies.[5]

The definition of personal data encompasses a broad range of data relating to an individual. Any data that can lead to **direct or indirect identification** of an individual can be considered as personal data.[6] Identifiers such as name, contact

---

[1] For this primer, in the context of the DPDP Act, "personal data" refers to "digital personal data".
[2] Section 2(h), DPDP Act.
[3] Section 2(o), Information Technology Act, 2000 defines "data" as *"data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."*
[4] Section 2(t), DPDP Act.
[5] The GDPR expressly excludes legal persons from the ambit of the regulation as well. Please see recital 14, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[6] Report on *"A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians"*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, available at
https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf, at pg. 29.

number, address, email address, and financial information are commonly understood to be personal data as they are reasonably unique to individuals, thus can lead to direct identification. Apart from those, even such data, which when combined with other pieces of information leads to identification may qualify as personal data.[7]

Whether such indirect identification is possible will depend on the means reasonably available to the data fiduciary and the nature of other data that may be combined with the original dataset.[8] Accordingly, apart from the commonly recognized identifiers, data stored in cookies on websites,[9] IP addresses may also constitute personal data where they enable identification.

Position in the European Union (EU). The EU's General Data Protection Regulation (**GDPR**) defines personal data as information relating to an identifiable natural person who can be identified, **directly or indirectly**, in reference to identifiers.[10] GDPR also recognizes that individuals may be associated with online identifiers provided by devices, applications, tools and protocols, such as dynamic IP addresses,[11] data stored in cookies which may leave traces that, when combined with other information, can be used to identify individuals or build profiles.[12] To that extent, such information would be treated as personal data.

NON-PERSONAL DATA

The application of the DPDP Act is limited to personal data, which implies that it does not extend to data that does not qualify as personal data. However, while the DPDP Act defines personal data broadly, it does not provide any explicit guidance on what would constitute as non-personal data.

Legislative background. A review of the legislative history of the DPDP Act indicates that the treatment of non-personal data has been a subject of some deliberation. The B.N. Srikrishna Committee left the question of regulating non-personal data open for future consideration,[13] while also empowering the central government to frame policies in this regard in the Personal Data Protection Bill, 2018.[14]

Subsequently, in 2021, the Joint Parliamentary Committee (**JPC**) observed that, given the scale of data collection and the difficulty in clearly distinguishing between personal and non-personal datasets, a unified framework governing both categories, albeit with differentiated protections, may be preferable.[15] The 2021 version of the Bill proposed by the JPC accordingly extended its scope to regulate processing of non-personal data as well, including anonymized data.[16] It defined non-personal data as any data other than personal data. However, the 2022 and 2023 iterations of the Bill, as well as the final DPDP Act, do not address non-personal data. Since the DPDP Act is silent with respect to treatment of non-personal data, and given the definition of personal data, it is clear that it does not regulate or apply to non-personal data.

Anonymized personal data. In addition, there is one more aspect over which the final DPDP Act differs from some of earlier iterations of the bills on personal data protection framework. Notably, 2018 and 2019 iterations of the bill explicitly

---

[7] *"White Paper of the Committee of Experts on a Data Protection Framework for India"*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, available at https://www.naavi.org/uploads_wp/new/srikrishna_white_paper.pdf, at pg. 36.

[8] *Supra* note 6.

[9] For a detailed discussion on cookies and the DPDP Act, please refer to out previous primer, available at https://elplaw.in/wp-content/uploads/2025/12/How-will-the-%E2%80%98cookies-crumble-under-Indias-new-data-protection-law.pdf

[10] Article 4(1), GDPR.

[11] The Court of Justice of the European Union (**CJEU**) in *Patrick Breyer v. Bundesrepublik Deutschland* (2016)*,* held that dynamic IP addresses could constitute personal data in cases the controller had legal means to obtain additional information enabling identification, available at https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=30991426

[12] Recital 30, GDPR.

[13] Pg. 13, *supra* note 6.

[14] Clause 105, The Personal Data Protection Bill, 2018, available at https://prsindia.org/files/bills_acts/bills_parliament/1970/Draft%20Personal%20Data%20Protection%20Bill,%202018%20Draft%20Text.pdf

[15] Report of the Joint Committee on the Personal Data Protection Bill, 2019, available at https://www.iltb.net/wp-content/uploads/2024/07/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf, recommendation no. 2, para. 1.15.8, at pgs. 25-26.

[16] Clause 2(d), Data Protection Bill, 2021, available at https://dpdpa.in/dpa_2021/act_only_new_%20dpa2021_ed.pdf

excluded anonymized data from its scope subject to certain conditions,[17] and also contemplated the prescription of anonymization standards. Anonymization refers to an irreversible process that transforms or converts personal data into a form in which a data principal cannot be identified.[18]

Further, in 2020, an expert committee on the non-personal data governance framework established by the Ministry of Electronics and Information Technology (**MeitY**) in its report (**2020 MeitY Report**) defined non-personal data as such data (i) which was never related to natural persons (such as weather), or (ii) which was initially personal data, but was subsequently **anonymized**.[19] Subsequently in 2022, a draft national data governance framework policy was also released by MeitY for consultation.[20] The draft policy, amongst others, sought to launch non-personal data based 'India datasets program' and address the methods and rules to ensure that non-personal data and anonymized data from both government and private entities are safely accessible by research and innovation eco-system. It is unclear what is the current status of the draft policy.

Put together, one could possibly draw following conclusions:

- The DPDP Act applies only to personal data and **does not** regulate processing of non-personal data; and

- Non-personal data (based on the 2020 MeitY Report) includes data unrelated to natural persons and data which was initially personal data but subsequently **anonymized**.

Would personal data include data that has been anonymized? The legislative history does not reflect a clear or consistent intent on the scope of personal data. While some iterations of the bill expressly excluded anonymized data from its scope, the final law (*i.e.,* the DPDP Act) is silent on this issue.

Despite this, it appears that anonymized data that meets certain standards is likely to fall outside the scope of personal data for two reasons: (i) the definition of personal data incorporates an identifiability test; and (ii) at least reports such as the 2020 MeitY Report do identify anonymized data as non-personal data. However, this position is contingent on whether the anonymization process followed by the data fiduciary is truly irreversible and cannot lead to identification of data principals when combined with other data sets in possession of the data fiduciary. In practice, businesses must be mindful of the possibility of re-identification, particularly where they possess the technical capability or additional datasets that could enable such reversal.

Position in the EU. It may be worth noting that the GDPR expressly excludes anonymized data from its scope, if the personal data is rendered anonymous in such a manner that an individual is no longer identifiable.[21]

WAY FORWARD

While there remains some ambiguity regarding the precise contours of personal data and the treatment of anonymized data, businesses are expected to implement fully compliant data processing systems within the prescribed timelines, *i.e.*, November 2027.

In the absence of detailed regulatory guidance, businesses should be conservative and interpret "personal data" broadly, in line with the intent of the DPDP Act. They would need to adopt a holistic approach when assessing datasets and evaluate whether a particular dataset, either on a standalone basis or in combination with other available data, can lead to the

---

[17] Clause 2(3), Personal Data Protection Bill, 2018; and Clause 2(b), Personal Data Protection Bill, 2019, available at https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf
[18] Clause 3(2), Personal Data Protection Bill, 2019.
[19] Report by the Committee of Experts on Non-Personal Data Governance Framework, available at https://ourgovdotin.wordpress.com/wp-content/uploads/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, para. 4.1 (iii), at pg. 13.
[20] Draft National Data Framework Governance Framework Policy, available at https://www.thehinducentre.com/resources/67557000-National-Data-Governance-Framework-Policy_compressed.pdf
[21] Recital 26, GDPR.

identification of a data principal. As a rule of thumb, if data can directly or indirectly identify an individual, it should be treated as personal data.

Further, while techniques that purport to convert personal data into non-personal data may fall outside the scope of the DPDP Act, careful assessment is required to determine whether such transformation is robust and irreversible in practice. In particular, businesses should evaluate whether they possess the technical means or supplementary data that could enable re-identification of data principals.

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 -raviskharnair@elp-in.com

Parthsarathi Jha, Partner - Email - parthjha@elp-in.com

Bhaavi Agrawal, Senior Associate- Email – bhaaviagrawal@elp-in.com