S&R

Data+

Personal and Non-Personal Data in Digital India: Before and After

This is the first note of a multipart series, focused on distinguishing between personal and non-personal data, including with respect to their separate regulatory, legal, and commercial implications. This note is divided into two sections. In Section I, we provide a brief summary of whether, and how, India's existing data protection framework addresses the definitions of, and the difference between, personal and non-personal data, respectively. In Section II, we provide an overview of India's legislative trajectory with respect to defining, and distinguishing between, the two.

Series Background

In the last few years, significant global progress has been made in terms of generating awareness about, and protecting, personal data. In particular, the ripple effects of the General Data Protection Regulation ("**GDPR**") of the European Union ("**EU**") have spread to, and influenced, the rest of the world – including India – especially with respect to the latter's ongoing efforts to overhaul its **existing data protection framework** (*Note 1, Section I*).

However, despite an apparent international convergence around key aspects, major gaps in understanding persist, especially when it comes to unpacking the contours of personal data with regard to its antithesis, *i.e.*, *non*-personal data ("**NPD**"). While, until recently, conditions in India, too, exemplified these gaps, certain **recent developments** (*Note 1, Section II*) hold promise for the future.

Today, analyzing the conceptual framework and regulatory trajectory of NPD has assumed additional importance – particularly for a country like India, poised as it is on the cusp of a **new digital governance architecture** (*Note 2*). Accordingly, it is time to examine the techno-legal challenges, sovereign priorities, and socioeconomic concerns related to NPD, even while discussing its opportunities and allied issues.

If 'non-personal data' is simply defined as data that is *not* personal (see the explanation to Clause 91(2) of the Personal Data Protection Bill, 2019, which was introduced in, and withdrawn from, Indian parliament in December 2019 and August 2022, respectively), we need to revisit the concept of personal data to check for what it is – and isn't. Accordingly, for the purpose of distinguishing personal data from NPD, a preliminary requirement is to trace its **conceptual paradigm** (*Note 3, Section I*) and various **categories** (*Note 3, Section II*). Further, its processing-related elements must be re-examined, including with reference to **notice, consent, and breach** (*Note 4*) – as well as in light of some extraordinary innovations proposed under Indian law relative to GDPR, such as in respect of **'deemed' consent** (*Note 5*), **sensitivity, volume, and harm** (*Note 6, Section I*), and relatedly, '**significant data fiduciaries**' (*Note 6, Section II*).

In that regard, the scope and limits of personal data (along with India-specific challenges) ought to be ascertained by comparing local cultural requirements, including those associated with its **meaning** (*Note*

7, Section I). Thus, a thorough definitional deconstruction, including with reference to existing and draft laws in both Europe and India, is useful to unearth a core aspect of personal data – one that most clearly distinguishes it from its non-personal equivalent: *i.e.*, **identifiability** (*Note 7, Section II*).

Nevertheless, while addressing identifiability, what must be viewed is the whole spectrum that lends itself for personal and non-personal data to transmute within, and inhabit, in their distinctive forms, including with the help of de-identification techniques such as **anonymization** (*Note 8*) and **pseudonymization** (*Note 9*). However, such distinctions within the personal/non-personal continuum have increasingly become blurry on account of the rising use of **mixed datasets** (*Note 10*) and de-anonymized data, the regulation of which has demanded urgent regulatory attention – including in **India** (*Note 11*).

While anonymization processes conducted on personal data are intended to yield non-personal outputs, the latter's **ambit** (*Note 12*) – better understood **now** (*Note 13, Section I*) than in previous eras – appears to be significantly more expansive than hitherto imagined, along with appurtenant **complications and opportunities** (*Note 13, Section II*). Accordingly, while India's plans to domesticate NPD through sovereign muscle for a better digital future has increasingly mirrored **Europe's trajectory in this regard** (*Note 14*), the former's ambitions now extend to becoming a cloud computing and data center hub, including through the establishment of '**data embassies**' (*Note 15*).

I. Personal and Non-Personal Data under India's Existing Data Protection Framework

Introduction

At present, India regulates the use of data under the Information Technology Act, 2000, as amended, including by the Information Technology (Amendment) Act, 2008 ("the **2008 Amendment**," and collectively, the "**IT Act**"), along with allied rules, such as the Information Technology (Certifying Authorities) Rules, 2000, as amended – the latter of which deals with digital signatures, including with respect to their creation, verification, standards, and certification, among other things.

Further, additional rules related to the IT Act include the following:

1. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (discussed further below) – which: (1) require entities holding sensitive personal information of users to maintain certain security standards, as well as (2) specify and prescribe security standards for personal information stored electronically.

2. Following the 2008 Amendment (especially with respect to providing an exemption to intermediaries from liability for any third-party information), the Information Technology (Intermediaries Guidelines) Rules, 2011 (the "**2011 Rules**") were framed – which provided due diligence requirements for intermediaries, prohibited content of a specific nature on the internet, and required intermediaries such as website hosts to block such content.

Subsequently, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "**2021 Rules**") were notified in February 2021, replacing the 2011 Rules. Key changes under the 2021 Rules included additional due diligence requirements for certain social media intermediaries, and a framework for regulating the content of online publishers with respect to news and current affairs, as well as curated audio-visual content. The 2021 Rules were further amended in 2022.

Earlier this year, India's Ministry of Electronics and Information Technology ("**MeitY**") published draft amendments to the revised 2021 Rules on its website with respect to due diligence by an intermediary under Rule 3, inviting feedback from the public. More recently, MeitY notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 (the "**2023 Amendment Rules**") – which amended the 2021 Rules further, and especially in terms of: (a) online gaming; (b) due diligence by intermediaries – including social media, significant social media, and online gaming intermediaries, respectively; as well as (c) grievance redressal. The 2023 Amendment Rules came into effect on April 6, 2023.

Other rules under the IT Act include the following (in addition to the ones mentioned above):

3. The Information Technology (Guidelines for Cyber Cafe) Rules, 2011 – which require cybercafés to: (1) register with a registration agency, (2) identify users and maintain a log of identity of such users, as well as (3) maintain records of their internet use.

4. The Information Technology (Electronic Service Delivery) Rules, 2011 – which allow the government to specify that certain services, such as applications, certificates, licenses, forms, etc., are required to be delivered electronically, and also provide a framework for the electronic delivery of such services.

Further, additional ancillary and/or sector-specific regulations also exist, such as the Information Technology (the Indian Computer Emergency Response Team and the Manner of Performing Functions and Duties) Rules, 2013; the directions and guidelines issued by the Indian Computer Emergency Response Team ("**CERT-In**"), including in respect of cybersecurity; the Consumer Protection Act, 2019; the Consumer Protection (E-Commerce) Rules, 2020; and rules published by various regulatory authorities such as the Reserve Bank of India ("**RBI**"), the Insurance Regulatory and Development Authority of India ("**IRDAI**"), and the Securities Exchange Board of India ("**SEBI**"), each of which governs different facets of data protection based on their respective jurisdictions.

DP Framework

More specifically, however, the data protection framework in India (the "**DP Framework**") stems from Section 43A of the IT Act (titled "*Compensation for failure to protect data*"), along with its subordinate rules, *viz.* the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI**").

Although Explanations (ii) and (iii) of section 43A of the IT Act define both 'reasonable security practices and procedures' and 'sensitive personal data or information,' such terms are described in fuller detail in SPDI under Rules 8 and 3, respectively. Further, provisions such as Rule 4 ("Body corporate to provide policy for privacy and disclosure of information"), Rule 5 ("Collection of information"), Rule 6 ("Disclosure of information"), and Rule 7 ("Transfer of information") of SPDI aim to address various discrete requirements of the DP Framework.

Personal and Non-Personal Data under the Existing DP Framework

While Section 43A of the IT Act, read with Rule 3 of SPDI, separately defines 'sensitive personal data or information,' the definition of 'data' under the IT Act does not appear to exclude non-personal data from its ambit.

Explanation (iii) of Section 43A of the IT Act defines 'sensitive personal data or information' as "such personal information as may be prescribed by the central government in consultation with such professional bodies or associations as it may deem fit." Rule 3 of SPDI further clarifies that sensitive personal data or information of a person means such personal information which consists of information relating to certain specified items, including passwords, financial information (such as details related to a bank account, credit/debit card, or other payment instrument), and biometric information.

Meanwhile, Section 2(1)(o) of the IT Act defines 'data' as "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."

Section 43A of the IT Act also refers to 'information in a computer resource.' However, neither of the definitions related to 'information' or 'computer resource' appears to contemplate personal data alone. For instance, Section 2(1)(v) of the IT Act defines 'information' to include data, message, text, images, sound, voice, codes, computer programs, software and databases, microfilm, or computer generated microfiche. Further, Section 2(1)(k) of the IT Act defines 'computer resource' as a computer, computer system, computer network, data, computer database, or software – where each of such constituent terms, other than the last two (*i.e.*, computer database and software, respectively), are separately defined in the IT Act in Section 2(1)(i), (l), (j), and (o), respectively.

Nevertheless, SPDI defines 'personal information' using language that appears to have inspired the eventual definition of 'personal data' under India's current draft of the Digital Personal Data Protection Bill, 2022 ("**DPDP**"), released by MeitY in November last year for public comments. Thus, Rule 2(1)(i) of SPDI defines 'personal information' as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." Meanwhile, Clause 2(13) of DPDP defines 'personal data' as "any data about an individual who is identifiable by or in relation to such data."

Similarly, the definition of 'data' under DPDP is more or less consistent with its equivalent under the IT Act – albeit more streamlined than before – adding components such as suitability of communication and interpretation, respectively, along with human or automated processing. Thus, Clause 2(4) of DPDP defines 'data' as "a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means." Interestingly, the definition of 'data' under DPDP, too, does not appear to preclude non-personal data as such.

II. India's Legislative Trajectory on Personal and Non-Personal Data

As discussed above, the existing DP Framework stems from Section 43A of the IT Act, including SPDI. However, in the absence of a standalone and/or dedicated domestic law on data protection, and in light of perceived inadequacies in the DP Framework – a white paper ("**White Paper**") on a revised paradigm was released in December 2017 by a government-constituted expert committee (the "**Expert Committee**").

Expert Committee and the White Paper

In the White Paper, the Expert Committee noted that data which is viewed as non-personal information can be combined with other datasets to create personally identifiable information, including via de-

anonymization techniques. Accordingly, it was possible for personal or non-personal data, when processed using 'big data' analytics, to be transformed into sensitive personal data.

In addition, the Expert Committee observed that research studies had concluded that it was difficult to distinguish between personal and non-personal data, and further, recognized the need to treat different types of personal data differently.

Pursuant to public comments to the White Paper and multi-city consultations, the Expert Committee submitted a report on a free and fair digital economy in July 2018 (the "**EC Report**") along with a draft of the Personal Data Protection Bill, 2018 ("**PDP 18**"). At that time, the EU had recently enacted GDPR, which came into force in May 2018, replacing the EU's erstwhile Data Protection Directive of 1995.

The EC Report

In the EC Report, the Expert Committee admitted that its deliberations had raised questions related to non-personal data, especially in connection with emerging activities involving data processing which hold considerable strategic and economic interest for the country.

PDP 18

Nevertheless, PDP 18 dealt with personal data only. Its Clause 2 was titled "*Application of the Act to processing of personal data*". Moreover, sub-clause (3) of Clause 2 clearly specified that PDP 18 would not apply to the processing of anonymized data either.

In addition, Clause 105 of PDP 18 was specifically titled "*No application to non-personal data*". The provision further specified that nothing contained in PDP 18 would affect the power of the central government to formulate appropriate policies for the digital economy as long as such policies did *not* govern personal data.

PDP 19

A year and a half after the EC Report was released, in December 2019, based on suggestions from the Expert Committee and various stakeholders, the Personal Data Protection Bill, 2019 ("**PDP 19**") was introduced. Like its predecessor, PDP 19 aimed to protect personal data (see Clause 2 of PDP 19), the meaning of which it expanded upon from PDP 18 (see Clause 3(29) of PDP 18) but defined somewhat similarly (*i.e.*, as data about or relating to a natural person who is directly or indirectly identifiable – see Clause 3(28) of PDP 19). However, while Clause 2(3) of PDP 18 had clearly stated that the law would not apply to the processing of anonymized data, Clause 2(B) of PDP 19 clarified that such non-application was subject to Clause 91. As such, the definitions of 'anonymization' and 'anonymized data' in PDP 19 remained the same as in PDP 18, except that the former specifically articulated the standard of 'irreversibility' (see Clause 3(2) of PDP 19).

Meanwhile, Clause 91(1) of PDP 19 mirrored Clause 105 of PDP 18 (as discussed above), and Clause 91(2) empowered the central government to direct any data fiduciary or data processor towards providing any anonymized personal data or other non-personal data for certain specified purposes – including for the purpose of better targeting of service delivery or formulation of evidence-based policies by the central government. Importantly, Clause 91(2) of PDP 19 contained a rudimentary definition of non-personal data (as 'data other than personal data') – albeit for the purpose of that provision alone.

However, various provisions in PDP 19 were inconsistent with contemporaneous data protection laws in key jurisdictions. For instance, by dint of its provisions on non-personal data, PDP 19 diverged from equivalent legislations of that period, including those in the EU, Australia, and Canada.

JC Report

Along with its parliamentary introduction, PDP 19 had been referred to a joint committee (the "**Joint Committee**"). After 78 sittings conducted over two years, the Joint Committee's report (the "**JC Report**") was presented before parliament in December 2021.

While PDP 19 had tentatively defined non-personal data as data other than personal data, the JC Report observed that it was impossible to clearly distinguish between the two (*i.e.,* between personal and non-personal data, respectively) – since data was collected, and indeed moved, *en masse* – so much so that data segregation into specific categories of 'personal' and 'non-personal' was impossible to achieve, including on account of data eclecticism at various levels of security.

Hence, the first recommendation in the JC Report was to ensure that PDP 19 dealt with both personal and non-personal data. It further recommended that PDP 19 ought to protect all kinds of data, and the regulatory authority should be empowered to regulate non-personal data as well, including in respect of breaches. Moreover, it was suggested that the short title of PDP 19 ought to be changed to the 'Data Protection Act, 2021' ("**Proposed DP Act**").

For the purpose of avoiding turf battles and regulatory confusion, the JC Report recommended a single administrative body. Accordingly, if such a body was poised to handle both personal and non-personal data, any further policy or legal framework on non-personal data was required to be made a part of PDP 19 (instead of being introduced as a separate legislation). In this regard, the JC Report suggested that as soon as the provisions to regulate non-personal data were finalized, there could be a separate regulatory framework on non-personal data within the Proposed DP Act.

Proposed DP Act

The Proposed DP Act (called the 'Data Protection Bill, 2021') – which represented an amalgam of revisions made to PDP 19 by the Joint Committee – was included within the JC Report (see p. 475 (handwritten p. 463) onwards). Consistent with the JC Report, the Proposed DP Act amended Clause 2 of PDP 19 to make the new law applicable to the processing of non-personal data as well (along with personal data), including in respect of anonymized personal data (see Clause 2(d) of the Proposed DC Act). Also, it added a definition of 'data breach' (see Clause 3(14) of the Proposed DC Act), which included breaches of non-personal data as well (see Clauses 3(28) and 3(29) of the Proposed DC Act).

Similar to Clause 105 of PDP 18 and Clause 91(1) of PDP 19, respectively, a separate provision in the Proposed DC Act specified that nothing contained in it would affect the power of the central government to formulate appropriate policies for the digital economy. However, unlike in previous versions, the Proposed DC Act specifically referred to policy-framing with respect to the handling of non-personal data (including with respect to anonymized personal data).

DG Committee

Despite the Joint Committee's eventual recommendation about including both personal and non-personal data within the same statute, on account of lingering uncertainties about the advisability of such a move – MeitY had constituted a committee of experts in September 2019 (*i.e.*, a few months before the Joint Committee was established) to deliberate on a framework for data governance (the "**DG Committee**"). In particular, the DG Committee was mandated to examine issues relating to, and make specific suggestions about regulating, non-personal data.

First DGC Report

A draft version of the DG Committee's first report was released in July 2020 (the "**First DGC Report**"). Among other things, the First DGC Report provided a definition of non-personal data and divided such data into three categories involving public, community, and private perspectives, respectively. It also proposed a separate legislation to regulate non-personal data, including through the establishment of a 'Non-Personal Data Authority' ("**NPDA**").

Revised DGC Report

Pursuant to stakeholder feedback with respect to the First DGC Report, the DG Committee proposed a revised version (the "**Revised DGC Report**") a few months later. In the Revised DGC Report, the DG Committee clarified the definition of non-personal data and re-examined the legal basis for asserting sovereign and community rights over non-personal data. However, the Revised DGC Report did retain certain key features of the First DGC Report, including those related to consent for anonymized data and an NPDA.

A more detailed analysis of the proposed data governance framework, as mentioned above, including with respect to non-personal data, will be provided in the next note of this series.

NDGFP

In May last year, MeitY had released a draft of the 'National Data Governance Framework Policy' for public consultation ("**NDGFP**"). The NDGFP aims to ensure that non-personal and anonymized data from both government and private entities are accessible by research and innovation ecosystems, including for the purpose of facilitating academic output and R&D initiatives by Indian start-ups.

In February this year, while presenting the Union Budget for FY 2023-24, Finance Minister Nirmala Sitharaman indicated that the NDGFP might be finalized soon, enabling access to anonymized data (see here and here, for example).

Proposed Digital India Bill

According to recent media reports, the government may frame rules for sharing non-personal data under a new law – including in respect of devices related to the 'Internet-of-Things' ("**IoT**"). In this regard, a draft bill (the "**Proposed Digital India Bill**") may be ready within a few months' time. It is possible that certain recommendations of the Revised DGC Report will be factored in with respect to the Proposed Digital India Bill, especially in connection with the sharing of non-personal data.

Current Status

PDP 19 was withdrawn in August 2022, including on account of the (large) scale of recommended changes made to it by the Joint Committee. A couple of months later, in November last year, the present draft of DPDP was released by MeitY for public comments. According to recent media reports, a revised draft of DPDP, pursuant to public feedback received in respect of the November draft, will be tabled before Parliament in July 2023.

In the next note of **Data+**, we will provide a summary of how India's proposed digital governance framework has sought to define, and distinguish between, personal and non-personal data, respectively, including through an analysis of past trends which have led to present developments.

*This insight has been authored by **Deborshi Barat** (Counsel); he can be reached at dbarat@snrlaw.in for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

S&R ASSOCIATES ADVOCATES

NEW DELHI
64 Okhla Industrial Estate
Phase III
New Delhi 110 020
Tel: +91 11 4069 8000

MUMBAI
One World Center, 1403 Tower 2 B
841 Senapati Bapat Marg, Lower Parel
Mumbai 400 013
Tel: +91 22 4302 8000