

How Much and How Bad? Significant Others in India's New Data Regime

Background

During the ongoing monsoon session of India's Lok Sabha, an as-yet unreleased Cabinet-[approved](#) version of the Digital Personal Data Protection Bill ("DPDP") is scheduled to be introduced by the Ministry of Electronics and Information Technology ("MeitY") in parliament [tomorrow](#). This revised draft may include important [changes](#) made to the last [iteration](#) (from November 2022), including pursuant to [public consultations](#) and [extensive feedback](#).

While the exact content of the 2023 bill remains officially unknown, a standing committee managed to adopt a [favorable report](#) on DPDP's revised version (despite strong opposition), tabling it across both houses of parliament yesterday and recommending an expeditious passage into law.

While DPDP has been largely modeled on the [General Data Protection Regulation](#) ("GDPR"), India's bespoke law may include a few key innovations compared to the EU's – such as those in respect of [children's data](#), [deemed consents](#) and [significant data fiduciaries](#) ("SDFs"), as previously discussed on [S&R Data+](#) (although [current reports](#) suggest that deemed consents have been done away with and/or substantially modified upon in the current draft, including [other changes](#) introduced in the latter with respect to appeals, exemptions, and cross-border data transfers).

Under Section 11, for instance, the central government ("CG") may notify any 'data fiduciary' as an SDF based on its assessment of prescribed factors – which include the [volume](#) of the personal data processed and the risk of [harm](#) to a 'data principal' (other than reasons of informational sensitivity, national/public interest, and additional factors).

While a 'data principal' is an individual with respect to whom certain personal data relates – companies, firms, associations of persons or bodies of individuals (even if they are unincorporated), the state itself, or any other (artificial) juristic person may be considered a 'data fiduciary' under DPDP – as long as they determine the purpose and means of processing data.

Pursuant to CG notification, special obligations may be imposed on SDFs under DPDP's Section 11, *over and above* those which all data fiduciaries need to comply with under Section 9, as discussed in an [earlier analysis](#). While our [last note](#) focused on sensitivity, we now address aspects of 'volume' and 'harm', respectively, in separate parts.

Part I: Volume

Introduction

In Europe, although GDPR does not have an exact equivalent for DPDP's SDFs, it does envisage situations when there are (or might be): (i) high numbers of individuals in each of multiple European countries who are likely to be substantially affected by processing operations; and (ii) clear requirements with respect to conducting a prior impact assessment in terms of protecting data.

With respect to the *volume* of data processed, GDPR talks about the necessity of a data protection impact assessment (“**DPIA**”). DPIAs should particularly apply to large-scale operations that aim to process a considerable amount of personal data at a regional, national, or supranational level. The justification for impact assessment stems from the fact that these operations could affect a large number of ‘data subjects’ (*i.e.*, the GDPR equivalent of DPDP’s ‘data principals’) and may also result in high risks on account of the underlying sensitivity of such data – especially when a new technology is used on a large scale, potentially compromising the rights and freedoms of data subjects.

Accordingly, GDPR suggests that a DPIA ought to be conducted when personal data is processed for taking decisions regarding specific individuals pursuant to:

1. a systematic and extensive evaluation of their personal aspects based on the profiling of such data; or
2. the processing of special categories of personal information, biometric data, information on criminal convictions and offences, or related security measures.

In addition, GDPR stipulates that a DPIA is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices, or for any other operations where the competent supervisory authority considers such processing as likely to result in a high risk to the rights and freedoms of data subjects.

Thus, despite *not* having an exact SDF requirement, GDPR does engage with the idea that a certain scale of data processing may significantly affect individual rights. In fact, GDPR’s Article 35(3)(a) clarifies that a DPIA will be particularly required (among other such situations) in the case of a systematic and extensive evaluation of personal aspects relating to natural persons (i) which is based on automated processing (including profiling); and (ii) on which decisions are based to produce legal effects in respect of (or which similarly and/or significantly affect) specific individuals.

The situation in India

Prior DPDP Iterations

In this segment, for the purpose of examining volume-related implications with respect to personal data processing, we compare DPDP with past versions of the law, such as the Personal Data Protection Bills of [2018](#) (“**PDP 18**”) and [2019](#) (“**PDP 19**”), respectively – as well as the [Data Protection Bill of 2021](#) (“**DP 21**,” and together with PDP 18 and PDP 19, “**Prior DPDP Iterations**”).

Children's data and volume

Earlier, like the [Children's Online Privacy Protection Act](#) (“**COPPA**”) in the United States (which imposes separate requirements on operators of websites or online services directed at children), Prior DPDP Iterations had provided for a separate class of data fiduciaries which remain involved in operations and services similar to what COPPA envisages, including in respect of processing large volumes of children's data. Accordingly, entities falling in this category, called 'guardian' data fiduciaries (“**GDFs**”), were proposed to be regulated via separate rules notified by the Data Protection Authority of India (“**DPA**”). While DPDP has done away with such GDF categorization, it has imposed additional obligations under Section 10 on *all* data fiduciaries that process children's data. DPDP has also done away with the DPA, replacing such authority with a 'Data Protection Board of India' instead (“**DPBI**”).

Social media and volume

PDP 19 had contained a special focus on regulating social media intermediaries (“**SMLs**”). To that end, PDP 19 had defined SMLs as intermediaries which primarily or solely enable online interaction between two or more users, thus allowing the latter to create, upload, share, disseminate, modify or access information using the former's services. However, certain intermediaries which primarily: (a) enable commercial or business oriented transactions; (b) provide access to the internet; or (c) operate in the nature of search engines, online encyclopedias, e-mail services, or online storage services, were not included within this definition.

PDP 19

Importantly, PDP 19 had specified that, over and above such factors which are considered by appropriate authorities for classifying 'general' data fiduciaries as SDFs, SMLs could also be notified as SDFs if: (a) such SMLs had users above a certain threshold, the applicable number of which the CG would later notify in consultation with the DPA; and (b) such SMLs were involved in actions that had, or were likely to have, a significant impact on electoral democracy, security of the state, public order, or the sovereignty and integrity of India. Further, different thresholds could be notified for different classes of SMLs.

DP 21

Similar to PDP 19, DP 21 had envisaged that social media 'platforms' (as opposed to 'intermediaries') (“**SMPs**”) which had a specified number of users, and whose actions were likely to have a significant impact on listed parameters relating to national/public interest, may be notified as SDFs. Like PDP 19, DP 21 had also envisaged different user thresholds for different classes of SMPs.

PDP 18 and DPDP

On the other hand, PDP 18 had contained no provisions on SMLs or SMPs. Similarly, DPDP, too, does not create a separate legal category for either SMLs or SMPs.

However, DPDP has introduced a *different* set of parameters (relative to those listed in Prior DPDP Iterations) for the CG to consider when it evaluates whether a data fiduciary ought to be notified as an SDF. Importantly, additional factors listed under DPDP include those earlier prescribed by PDP 19 for SMI assessments (for the purpose of SDF notification). Thus, elements of PDP 19's Clause 26(4) – such as 'significant impact on electoral democracy', 'security of the state', 'public order', or 'the sovereignty and integrity of India' – have been incorporated in DPDP under the provision on SDFs itself.

DPIAs

Prior DPDP Iterations

In the past, both PDP 18 and PDP 19 had contained requirements that were similar to those mentioned in GDPR with respect to DPIAs (e.g., see Clauses 33 and 27 of PDP 18 and PDP 19, respectively). Thus, if an SDF intended to process personal information in a way that involved (i) new technologies, (ii) large scale profiling, or (iii) the use of sensitive personal data or information ("**SPDI**") (e.g., genetic or biometric data), and/or (iv) if such processing carried a risk of 'significant harm' (see *discussion on 'harm' below, in Part II*), such SDF would be obliged to undertake a DPIA before processing such information.

Further, such Prior DPDP Iterations had each contained a minimum list of requirements that SDFs would need to comply with in respect of DPIAs, such as: (i) providing a detailed description of the proposed processing operation, along with statements about the purpose of processing and the nature of the underlying data; (ii) conducting an assessment of the harm that may be caused to those whose personal data is proposed to be processed; and (iii) undertaking measures to manage, minimize, mitigate or remove such risk of harm.

GDPR's influence

Importantly, GDPR contains a similar list of requirements. For instance, Article 35(7) of GDPR states that a DPIA is required to contain, at a minimum: (i) a systematic description of the envisaged processing operations, along with the purposes of processing – including the legitimate interest pursued by the 'controller' (the GDPR equivalent of a 'data fiduciary'); (ii) an assessment of the necessity and proportionality of the intended processing operation in relation to its purpose; (iii) an assessment of the risks to the rights and freedoms of data subjects; and (iv) the measures envisaged to address risks (including safeguards), along with corresponding security measures, to ensure the protection of personal data and for the purpose of demonstrating GDPR compliance – after having taken into account the rights and legitimate interests of data subjects and other persons concerned.

DPDP

SDFs under DPDP first need to comply with such *general* obligations that are applicable to *all* data fiduciaries under DPDP's Section 9, as discussed in our [previous note](#) on SDFs. Further, under Section 11, each SDF is required to undertake certain additional measures – such as conducting DPIAs and periodic audits. Unlike in Prior DPDP Iterations, however, DPDP does *not* spell out the required elements for conducting a DPIA – although it defines the term itself (to the extent of clarifying what a DPIA entails).

Thus, a DPIA has been defined as a process that comprises descriptions, purposes, assessments of harm, measures for managing the risks associated with such harm, and other prescribed matters with respect to processing personal data.

It is likely that if and when DPDP becomes law, separate regulations will be issued with detailed requirements related to several of DPDP's provisions – including those on DPIAs. Until then, GDPR can be viewed as an embodiment of global best practices in this regard. There is no obvious reason which suggests that DPDP – like the Prior DPDP Iterations – will *not* follow GDPR's tested template in the future.

Part II: Harm

Introduction

As earlier discussed, while GDPR does not have an exact equivalent for SDFs, it does envisage similar ideas of concern with respect to 'significance' – involving, in particular, situations when there are (or might be) legal or other major effects on individuals stemming from decisions that are solely based on automated processing and/or individual profiling.

In this regard, Section 2(1) of DPDP clarifies what 'automated' means: "any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data." In addition, DPDP, like GDPR, has extraterritorial application – to the extent that it applies to the processing of digital personal data *outside* Indian territory when such processing relates to: (i) 'profiling' individuals in India; or (ii) an activity of offering goods or services to people within Indian territory. According to DPDP, 'profiling' involves analyses or predictions of aspects concerning an individual's behavior, attributes or interests.

Almost every human activity today involves some species of data transaction. Accordingly, the internet has birthed new markets, including those engaged in the collection, organization, and processing of personal data, where such activities remain a critical component of the underlying business model. 'Big Data' offers specific methods and technologies for statistical data evaluation, which arise at the interface of business informatics and commercial data management – combining the fields of business intelligence, data warehousing and data mining (*i.e.*, the application of exploratory methods to a data inventory with the aim of discovering knowledge from such databases, and specifically for the purpose of pattern recognition). In this regard, issues of privacy and customer confidentiality have acquired added prominence on account of the rise of digital tracking and targeted advertising.

Prior DPDP Iterations

'Harm' under PDP 18/19

PDP 18 had defined the notion of harm broadly. For instance, Clause 3(21) of PDP 18 had included the following elements within the definition of harm: (i) bodily or mental injury; (ii) loss, distortion, or theft with respect to identity; (iii) financial loss or loss of property, (iv) loss of reputation or humiliation; (v) loss of employment; (vi) discriminatory treatment; (vii) blackmail or extortion; (viii) denial or withdrawal of a service, benefit, or good resulting from an evaluative decision about the data principal; (ix) restrictions

imposed or suffered, directly or indirectly, with respect to speech, movement, or any other action arising out of a fear of being observed or under surveillance; or (x) observation or surveillance which is not reasonably expected by a data principal.

PDP 19 had reproduced the same elements within its own definition of harm under Clause 3(20).

Significant harm

Further, 'significant harm' was separately defined in Prior DPDP Iterations – such as in Clause 3(37) of PDP 18, which had defined it as "harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm." Later, Clause 3(38) of PDP 19 had reproduced the same definition.

'Harm' under DP 21

DP 21, too, had contained a broad definition of 'harm', including bodily or mental injury, identity theft, financial loss, loss of reputation, and direct or indirect restrictions on speech or movement owing to a fear of surveillance. Additional elements in DP 21's definition included any denial or withdrawal of a service, benefit, or good resulting from an evaluative decision about the data principal, as well as psychological manipulation which impairs an individual's autonomy.

In this regard, DP 21 did not clarify the meaning of an 'evaluative decision' or 'psychological manipulation'. It is possible that an 'evaluative decision' under DP 21 included predictive decisions based on data-processing which typically determine whether a data principal should be provided with certain entitlements such as credit, employment, etc. However, the definition of 'harm' under DP 21 did not make a distinction between: (i) evaluative decisions which may be prejudicial to, or discriminatory against, a data principal (on the one hand); and (ii) evaluative decisions which are otherwise justifiable (on the other hand). Hence, it is possible that the mere act of denying a data principal certain goods, services, or benefits based on an evaluative decision could have been interpreted as 'harm' against such data principal under DP 21.

Further, unlike GDPR, the definition of 'harm' under DP 21 was extended to all species of evaluative decisions, without clarifying whether such decisions were required to involve natural persons only. Accordingly, such an expansive definition of 'harm,' as earlier formulated under DP 21, might have produced significant concern for data-based predictive decision-making practices and/or entities.

Harm under DPDP

Relative to Prior DPDP Iterations, DPDP has significantly reduced the scope of 'harm'. However, Section 2(10) of DPDP does retain the following elements: (a) bodily harm; (b) distortion or theft of identity; (c) harassment; or (d) prevention of lawful gain or the causing of significant loss.

However, what may be considered 'significant' with respect to a 'significant loss' has not been separately explained. Nevertheless, Section 2(11) of DPDP does define 'loss' as follows: (a) a loss in property, or an interruption in the supply of services – whether temporary or permanent; or (b) a loss of opportunity with respect to earning a remuneration, or earning a greater remuneration, or gaining a financial advantage other than by way of remuneration.

Accordingly, DPDP has done away with some erstwhile elements related to 'harm' (e.g., as contained in PDP 18 and PDP 19), including those related to discriminatory treatment, reputational loss, surveillance, restrictions on speech and movement, etc. – along with the removal of additional elements (e.g., as contained in DP 21) such as denials/withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal (as well as psychological manipulation which impairs an individual's autonomy).

Since the notion of 'sensitive' (or 'critical') personal data or information has not been defined in DPDP separately, certain related elements – such as that of 'significant harm' (as contemplated in Clauses 22(2)(a) and 15(1)(a) of PDP 18 and PDP 19, respectively) – have not been dealt with under DPDP either. For instance, PDP 19 had specified that the CG, in consultation with the DPA and the sectoral regulator, would notify such categories of personal data as SPDI based on, *inter alia*, the risk of *significant harm* that may be caused to a data principal by the processing of that data.

Conclusion

Other than DPDP itself, consistent with its aim to replace the dated Information Technology Act, 2000 (the "IT Act"), MeitY may make a draft bill ready for the proposed '[Digital India Act](#)' ("DIA") over the next [few months](#), focusing *inter alia* on [cybersecurity](#), prevention of [online harm](#), stricter penalties and 'future-readiness' – including through the responsible regulation of [emerging technologies](#).

In terms of protecting consumers from harm, the DIA may contain additional rules that balance regulation with encouragement – such as in respect of data captured by [invasive gadgets](#) like spy camera glasses and other wearable devices, but without compromising India's 'tech' ecosystem. Dedicated provisions to regulate new technologies may be introduced, including in respect of 'Know-Your-Customer' (KYC) requirements as a pre-condition to obtain approvals for sale.

According to recent [reports](#), the DIA will aim to facilitate an open internet, online safety and trust, a revised intermediary framework, and limited safe harbor. It may also introduce updated norms for the sharing of [non-personal data](#) – including in respect of technologies such as the Internet-of-Things, blockchain and Artificial Intelligence ("AI").

With respect to AI in particular, as discussed in our [separate note](#) on the subject, India's new data regime (comprising both DIA and DPDP) may apply to AI methodologies and machine learning ("ML") systems during various instances of digital data processing – including when systematic and extensive evaluations of personal aspects related to specific individuals are performed based on automated means, including through the use of profiling and decision-making technologies. After all, AI policymakers mainly focus on automated decision-making and ML systems (which are algorithmically controlled). Thus, significant regulatory challenges arise when advanced ML algorithms share important characteristics with human decision-making processes. For instance, there could be concerns about the potential liability of the underlying system, especially when data processing leads to harm. At the same time, and from the particular perspective of those affected by such automated decision-making processes, the increased opacity, newer capabilities and uncertainty associated with the use of AI may lead to diverse new challenges, both legal and regulatory.

Further, in terms of online safety, the DIA may introduce specific provisions for protecting users against unsafe content, online harm and new cybercrimes (such as '[doxxing](#)') – including by 'age gating' children from addictive technologies and online/digital platforms that seek to process large volumes of children's data.

In addition, moderating false information and/or curbing fake news, including with respect to content published on social media platforms, messaging services, websites, and other forums, might be focused on. In this regard, the DIA may introduce compliance requirements and/or specific measures, such as periodic risk assessments, algorithmic transparency and accountability, as well as mandatory disclosure. Concomitantly, the penalty framework for non-compliance, especially for cybercrimes and other serious offences, may become more stringent. A specialized adjudicatory mechanism for addressing online offences may also be introduced.

Furthermore, personal information that is anonymized later may be treated as the 'non-personal data' of the original individual. Accordingly, a data principal could act upon any subsequent harms arising from the re-identification of their data (for instance, if an applied pseudonymization technique is not robust enough) or arising on account of any other reason further to data processing.

The DIA may also [modify](#) the [safe harbor](#) principle under Section 79(1) of the IT Act with respect to intermediaries. Previously, the [Information Technology \(Amendment\) Act, 2008](#) ("the **2008 Amendment**") had introduced Section 79 to the IT Act under a substituted Chapter XII ('*Intermediaries not to be liable in certain cases*'). This provision sought to exempt intermediaries from liability for third-party information that was only hosted or otherwise made available. Thereafter, the [Information Technology \(Intermediaries Guidelines\) Rules, 2011](#) (the "**2011 Rules**") were framed to provide clear due diligence requirements for intermediaries. Further, the 2011 Rules prohibited content of a specific nature on the internet, and also required intermediaries (such as website hosts) to block such content.

Under the DIA, protection from liability for different kinds of intermediaries/platforms against content shared by users may be contingent upon intermediary compliance with prescribed obligations in respect of [hosting third-party information](#). At any rate, the the 2011 Rules were replaced by the [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules, 2021](#) (the "**2021 Rules**"), which included additional due diligence requirements for certain entities – including SMIs and significant SMIs – as well as a framework for regulating content with respect to online publishers of news, current affairs, and curated audio-visual content. The 2021 Rules were [further amended](#) in 2022 to extend such additional due diligence obligations on online gaming intermediaries (MeitY notified the 2023 Amendment Rules this year – which amended the 2021 Rules again in terms of: (a) online gaming; (b) due diligence by online gaming intermediaries; and (c) grievance redressal).

Even at present, pursuant to the 2008 Amendment, Section 43A of the IT Act requires companies, firms, sole proprietorships, and other associations of individuals engaged in commercial or professional activities to maintain 'reasonable security practices and procedures' ("**RSPPs**") if they possess, deal with or otherwise handle SPDI in a self-owned/controlled/operated computer resource.

SPDI has been expressly defined under the existing [Information Technology \(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information\) Rules, 2011](#) (the “**SPDI Rules**”). In particular, the SPDI Rules require entities that hold user-related SPDI to maintain certain security standards. The rules also prescribe the specific protocols necessary for storing personal information electronically, including with respect to SPDI.

*This insight has been authored by **Deborshi Barat** (Counsel); he can be reached at d Barat@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.*

© 2023 S&R Associates

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