COVINGTON

India Introduces Updated Draft of Personal Data Protection Bill

February 5, 2020

Data Privacy and Cybersecurity

On December 11, 2019, the Government of India introduced an updated draft of the Personal Data Protection Bill (the "Bill"), moving one step closer towards enacting a comprehensive privacy regime modelled on the European Union's General Data Protection Regulation ("GDPR").

The Bill released in December is the Government's second draft of legislation intended to address the Supreme Court of India's landmark decision in *K.S. Puttaswamy v. Union of India* (2017). In that decision, the Court held that privacy is a fundamental right and invited the Government to formulate "a regime for data protection." A Committee of Experts formed following the decision, headed by former Supreme Court Justice, B.N. Srikrishna, released the first draft Personal Data Protection Bill in July 2018.

The release of the Bill marks an important development in the enactment of comprehensive data protection laws worldwide. If the Bill is enacted, India will become the third largest economy (following the European Union and Japan) to implement comprehensive protections for personal data. As a popular destination for outsourcing, the Bill could have an outsized impact on companies around the world.

Although in many respects the Bill aligns closely with the GDPR, it also introduces novel obligations that exceed those required by the GDPR. Most significantly, the Bill's data localization provisions require "sensitive personal data" and "critical personal data" to be stored in India, subject only to narrow exclusions. The Bill also requires "significant data fiduciaries" to submit their processing facilities for audit, and grants the Government the authority to assign "trust scores" on the basis of audit results. In addition, the Government is empowered to compel organizations to produce anonymized and non-personal data for policy-making purposes. Provisions that more closely adhere to GDPR precedent also diverge in key areas, such as the legal bases for processing, individual rights, protections for children's data, and accountability obligations.

A Joint Parliamentary Committee, composed of parliamentarians from both the lower and upper houses of Parliament is expected to issue a report on the Bill the week of February 24th.

Below we summarize the key provisions of this most recent draft of the Bill. For a more detailed comparison of the Bill to the GDPR, click here.

Scope and Application

Structure and Terminology

The Bill's structure closely resembles that of the GDPR. Entities are accorded differing levels of responsibility based on their overall control of any given processing activity. As in the GDPR, entities that determine the purposes and means of processing -- termed "data fiduciaries" under the Bill -- have greater responsibility for compliance than data processors, which generally must follow the instructions of the former.

Although the Bill's use of the term "data fiduciary" may imply a responsibility to act in the best interests of "data principals" (or "data subjects," as they are known under the GDPR), except with respect to children's data, discussed below, these implicit responsibilities do not appear to be reflected in any specific additional requirements in the Bill. Indeed, the Bill's definition of a "data fiduciary" as a person or entity that "alone or in conjunction with others determines the purposes and means of processing personal data," conforms almost exactly to the GDPR's definition of a "controller."

Territorial Scope

The Bill applies to entities located both within and outside India. In particular, the Bill applies to:

- the processing of personal data that has been collected, disclosed, shared, or otherwise processed within the territory of India;
- the processing of personal data by Indian companies, Indian citizens, and any other persons or bodies incorporated under Indian law; and
- the processing of personal data by "data fiduciaries" not present within India if the processing is in connection with any business in, or systematic offering of goods or services to, data principals in India or with the profiling of data principals in the region.

This scope of application is potentially broader than that of the GDPR, as an entity may become subject to Indian law merely by processing personal data in India, such as through the use of a processor in the country, irrespective of the location of any concerned data principals. Importantly for India's outsourcing sector, however, the Bill permits the Central Government to exempt data processors (or classes of data processors) that are contracted by an overseas entity and process personal data relating only to individuals located outside of India.

Subject-Matter Scope

As in the GDPR, the Bill applies to the processing of personal data and includes extra protections for "sensitive personal data." However, the Bill's definitions of personal and sensitive personal data broaden its scope beyond that contemplated by the GDPR.

Personal Data: The Bill defines "personal data" as data "about or relating to a natural person who is directly or indirectly identifiable . . . ." However, unlike the GDPR, the Bill does not on its face take into account the "reasonable likelihood" that an individual will be identifiable. The Bill also expressly includes within the scope of personal data inferences drawn from personal data for the purpose of profiling. This leaves open the possibility that inferences could be considered personal data, even if they do not permit the identification of any individuals.

Sensitive Personal Data: The Bill's definition of sensitive personal data is broader than the analogous GDPR definition in two respects: (1) The Bill includes financial data within the scope

of sensitive personal data, imposing additional obligations on businesses that process billing or other financial information, and (2) the Bill authorizes the Government to define additional categories of sensitive data.

Wide Government Authority and Discretion: An important aspect of the Bill is the large number of provisions that are left to either the Central Government or the to-be-formed Data Protection Authority ("DPA") to define at a later date. For example, the Central Government has broad authority to exempt any government agency from any or all provisions, including collection and reporting requirements, if it determines that it is "necessary or expedient" in the interest of sovereignty, security, public order, and other public interests. Most controversially, the Bill authorizes the Government to compel the disclosure of information that does not constitute personal data — including anonymized personal data, a term to be defined by the DPA — "to enable better targeting or delivery of services or formulation of evidence-based policies." We highlight some of the areas where government or DPA intervention is permitted through each of the key issues we discuss below.

Key Substantive Requirements

Data Localization and International Data Transfers

The Bill restricts cross-border transfers of both sensitive personal data and "critical personal data," but does not impose limitations on outward transfers of personal data that do not fall into these categories.

Sensitive Personal Data: Sensitive personal data may not be transferred outside of India unless the data principal gives explicit consent and one of the following conditions is satisfied: (1) the transfer is made pursuant to a contract or intra-group scheme approved by the DPA; (2) the government has deemed a country or class of entities within a country to provide adequate protection; or (3) the DPA has specifically authorized the transfer. Even if the data fiduciary satisfies an exemption, the entity must retain a copy of the sensitive personal data in India.

Critical Personal Data: Under the Bill, critical personal data must be processed only in India, except under emergency circumstances or where the government has approved the transfer, taking into account India's security and strategic interests. The Bill gives the Government broad discretion to define "critical personal data" and does not specify limiting criteria.

Personal Data: The Bill does not contain restrictions on cross-border transfers of personal data that are not sensitive or critical personal data, a notable divergence from the GDPR.

Protections for Children

Additional Protections Apply to Children under the Age of 18: The Bill requires every data fiduciary to process personal data in a manner that is "in the best interests of the child." Children are defined as data principal under the age of 18, a significantly higher age threshold than what is provided by the GDPR and the U.S. Children's Online Privacy Protection Act.

Age Verification and Consent: Before processing a child's personal data, the data fiduciary must verify the individual's age and obtain parental or guardian consent. These requirements are more stringent than corresponding provisions in the GDPR, which require parental consent only for certain online services offered directly to children where the processing is based on consent.

Guardian Data Fiduciaries: The Bill authorizes the DPA to classify as a "guardian data fiduciary" any data fiduciary that operates an online service or commercial website directed at children, or processes large volumes of children's personal information, and prohibits these entities from profiling, tracking, behaviorally monitoring, or directing targeted advertising towards children.

Lawfulness of Processing

The Bill specifies that personal data may not be processed except for a "specific, clear, and lawful purpose." As in the GDPR, the Bill sets forth legal bases for processing personal data. These bases are: (1) consent, (2) legal obligation, (3) medical emergency involving a threat to life or severe threat to health, (4) providing medical treatment or health services, (5) protecting the safety of individuals during a disaster, (6) employment purposes, and (7) "reasonable purposes" as may be specified by regulations. The Bill does not, however, include some of the GDPR's key bases for processing, most notably contractual necessity (although, as discussed below, the "consent" basis may provide an alternative ground) and for a "legitimate interest."

Consent: Under the Bill, valid consent must be free, taking into account whether it complies with Section 14 of the Indian Contract Act, informed, specific, clear, and capable of being withdrawn. The Bill's basis for consent appears to be broader than that in the GDPR and may incorporate elements of the GDPR's "contractual necessity" ground. For example, Section 14 of the Indian Contract Act provides that consent is "free" when it is not caused by coercion, undue influence, fraud, misrepresentation, or mistake, which is less stringent than the GDPR's "without detriment" standard. The Bill also does not expressly require data fiduciaries to separately obtain consent for each processing purpose.

Reasonable Purposes: The Bill permits processing without consent for "reasonable purposes" as specified by the Data Protection Authority ("DPA"). In defining these reasonable purposes, the DPA must take into consideration a number of factors similar to the "legitimate interests" test under the GDPR, such as the data fiduciary's interests or any public interests, whether the data fiduciary can reasonably be expected to obtain consent for the processing, the effect of the processing on the rights of data principals, and the data principal's reasonable expectations given the context. Although the Bill specifies several purposes that the DPA may qualify as reasonable, such as fraud prevention, information security, mergers and acquisitions, and processing publicly available personal data, marketing and product development and improvement are not on the list. Critically, as the Bill merely permits, but does not require, the DPA to specify reasonable purposes, there is considerable uncertainty as to when data fiduciaries will be able to rely on this legal basis.

Sensitive Personal Data: The grounds for processing sensitive personal data in the Bill are identical to those for non-sensitive personal data, except in one significant respect. Where consent is required for processing sensitive personal data, the data fiduciary must obtain consent (1) explicitly and not inferred from other conduct, (2) separately from other processing, and (3) after informing the data principal of the purpose for processing that is likely to cause significant harm. In addition, sensitive data may not be used for employment purposes without consent.

Accountability Requirements

Like the GDPR, the Bill requires data fiduciaries to implement a series of internal measures, tuned to the risk of processing, to demonstrate accountability and compliance with the framework.

Significant Data Fiduciaries: The Bill permits the DPA to designate a class of data fiduciaries as "significant" based on criteria such as the volume of personal data processed, sensitivity of personal data processed, turnover of the data fiduciary, the risk of harm posed by processing, the use of new technologies for processing, and any other factor causing harm from such processing. Data fiduciaries that are designated as significant must comply with additional accountability requirements, as set out below.

Data Protection Impact Assessment: The Bill requires significant data fiduciaries to conduct a Data Protection Impact Assessment ("DPIA") before processing personal data if the processing involves (1) new technologies, (2) large-scale profiling or use of sensitive data, or (3) any other activities that carry a significant risk of harm, as may be specified by regulations. Notably, all DPIAs must be submitted to the DPA for review – a significant departure from GDPR.

Audit Requirements: Significant data fiduciaries must engage an independent auditor, selected from a list approved by the DPA, to conduct an annual audit of their processing activities. Data auditors may assign a "data trust score" to a data fiduciary based on their findings, which would need to be disclosed to data principals. The DPA may also direct data fiduciaries (that are not "significant") to conduct an audit if the DPA considers the data fiduciary's processing to be likely to cause harm.

Data Protection Officer and DPA Registration: Under the Bill, significant data fiduciaries must appoint a Data Protection Officer ("DPO") who is based in India and "represents" the data fiduciary under the Bill. Significant data fiduciaries must also register with the DPA.

Privacy by Design Policy: The Bill requires all data fiduciaries to prepare a "privacy by design" policy that details the "managerial, organizational, business practices and technical systems designed to anticipate, identify and avoid harm," among other elements.

Individual Rights

As with GDPR, the Bill grants data principals a broad array of rights, including rights of transparency, access, correction, and deletion. Notably, the Bill does not provide for a right not to be subject to automated decisions, as exists under the GDPR, although the Bill does prohibit the profiling of children.

Transparency: Under the Bill, data fiduciaries must provide a notice containing detailed disclosures, including the purposes for which the personal data is to be processed, the categories of personal data collected, the entities with whom personal data may be shared, and the procedures for redressing grievances.

Access: The Bill grants data principals the right to receive confirmation of whether their personal data is being processed, a summary of the processing activities undertaken, and a copy of the personal data processed by the data fiduciary. The data fiduciary must also provide "in one place" the identities of all other data fiduciaries with whom personal data has been shared.

Portability: The Bill gives data principals the right to receive personal data that is processed through automatic means in a structured, commonly-used, and machine-readable format. This right would also apply to profile information, even if the data may be inferred.

Correction: Under the Bill, data principals have the right to correct inaccurate or misleading personal data, complete incomplete personal data, and update out-of-date personal data. The

data fiduciary must take steps to communicate this updated information to all relevant entities or individuals to whom such personal data may have been disclosed, particularly where the information may affect the data principal's rights and interests.

Right to be Forgotten and Right to Erasure: Unlike the GDPR, the Bill distinguishes between the right to be forgotten and the right to erasure. Under the Bill, data principals have the right to request the deletion of personal data that is no longer necessary for the purpose for which it is processed. In addition to the right to erasure, the Bill grants individuals a right to be forgotten, which permits them to restrict or prevent the continued disclosure of personal data. The right to be forgotten applies where the data is no longer needed for the purposes for which it was processed, the data principal withdraws consent (where processing was based on consent), or the disclosure was unlawful. To enforce the right, individuals must apply to an "Adjudicating Officer" appointed by the DPA.

Data Processing Agreements and Security Requirements

Data fiduciaries and processors are subject to accountability requirements that broadly mirror those required by the GDPR.

Data Processor Agreements: All data fiduciaries' contracts with processors must specify that the processor will process personal data in accordance with the data fiduciary's instructions, personal data will be held in confidence, and sub-processors will not be appointed without approval.

Security and Breach Notifications: Data fiduciaries and data processors must implement necessary security safeguards, including methods to de-identify and encrypt data, as well as prevent unauthorized access to or destruction of personal information. The Bill requires data fiduciaries to notify the DPA of a breach "as soon as possible" if it is likely to cause harm to any data principal, but gives the DPA discretion to determine the timing of subsequent breach notifications. The DPA may also direct the data fiduciary to post a notification of the breach on the DPA's or business's website. No breach notification obligation applies directly to data processors (though presumably data fiduciaries may impose such an obligation by contract).

Social Media Intermediaries

The Bill imposes specific requirements on "social media intermediaries," which are defined as entities that "primarily or solely" enable online interaction between two or more users and enable these users to "create, upload, share, disseminate, modify or access" information using their services, excluding search engines, email services, internet access providers, and entities that enable commercial or business-oriented transactions. First, the Bill permits the Government to designate these intermediaries as significant data fiduciaries subject to the relevant accountability provisions discussed above. Second, social media intermediaries that are designated as significant data fiduciaries must allow users to voluntarily verify their accounts in a manner prescribed by the Government. Verified accounts must display a "demonstrable and visible mark of verification" that is visible to all users of the service.

Research and Innovation

Research Exemptions: The Bill broadly authorizes the DPA to exempt entities from *any* of the Bill's obligations for a research, archiving, or statistical purpose if compliance with the Bill would "disproportionately divert" resources from that purpose, the data has been anonymized in accordance with a code of practice promulgated by the DPA (and use of fully anonymized data

would not be possible), purpose could not be achieved with anonymized data, and the data will not be used to make decisions about a specific data principal or in a manner that poses a risk of significant harm. Importantly, as with other areas of the Bill, research exemptions are not operative automatically, but instead require the affirmative action of the DPA to apply.

Regulatory Sandbox: In addition, the Bill creates a mechanism by which data fiduciaries may be able to take advantage of a "regulatory sandbox" to test new technology with lower enforcement risks. To be eligible for participation, data fiduciaries must have their privacy by design policies certified by the DPA and published on both the data fiduciary's and the DPA's website.

Penalties

Criminal Liability: Any person who, knowingly or intentionally, re-identifies, or re-identifies and processes, personal data that has been de-identified by a data fiduciary or a data processor without that entity's consent may be punished by up to three years' imprisonment or fined up to approximately $3,000, or both. Persons subject to this provision are exempt from liability if they re-identify their own personal data or if the relevant data principal has explicitly given their consent. The Bill specifies that if the offense is committed by a company, every person in charge of or who was responsible to the company for the conduct of its business will be held liable unless the offense was committed without his knowledge or if he had exercised "all due diligence" to prevent the commission of the offense.

Administrative Fines: Data fiduciaries who violate the Bill's provisions may be subject to administrative fines of up to the higher of approximately $2 million USD or 4% of a group of entities' annual global revenue.

Injunctive Penalties: The Bill also authorizes the DPA to issue injunctive penalties, which includes the ability to block processing, restrict international transfers, and require the deletion of personal data.

Individual and Group Redress: Data principals who have been harmed by a data fiduciary's or processor's violation of the Bill may seek compensation from an administrative hearing before an Adjudicating Officer. The Bill provides that one or more data principals or an "identifiable class" of individuals may jointly bring a claim on their behalf.

* * *

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Gabe Maldoff*	+1 202 662 5537	gmaldoff@cov.com
Diana Lee*	+1 202 662 5684	dlee@cov.com

*District of Columbia bar application pending; supervised by principals of the firm.