July 30, 2018

THE PERSONAL DATA PROTECTION BILL, 2018: A SUMMARY

The report issued by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (**Report**)[1] and the draft of the Personal Data Protection Bill, 2018 (**Bill**)[2] is a significant development in the evolution of general data protection legislation in India. The normative foundation of the Bill is the judgement of the Supreme Court in *Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* (W.P. (Civil) No. 494 of 2012) (**Puttaswamy**) upholding the 'right to privacy' as a fundamental right under the Constitution of India. The Bill represents a potential sea change in the definition, treatment, and enforcement of the law surrounding personal data and its processing.

The summary provided below focuses on the key aspects of the Bill and the Report relevant to private Data Fiduciaries (*defined below*). The Bill also contains extensive provisions pertaining to the Processing (*defined below*) of Personal Data (*defined below*) by Central and State Governments, the treatment of Aadhaar information, the Right to Information Act, 2005 and a special regime for Significant Data Fiduciaries and Guardian Data Fiduciaries (*as defined in the Bill*). The aforementioned provisions are not the focus of this summary and will be examined separately.

Definitions and Jurisdiction

1. **Personal Data and Processing**: The Bill applies to the processing of all personal data, i.e. any data relating to a natural person (*referred to as the 'Data Principal'*[3]) who is directly or indirectly identifiable from such data, having regard to any feature of the identity of such natural person, or combination of such features with each other, or other information (**Personal Data**)[4]. While this definition will clearly cover identifiers such as names, its application to other identifiers like IP Addresses is less clear[5]. Processing (**Processing**) is defined broadly as the performance of operations on Personal Data and will include, *inter alia*, collection, storage, retrieval, usage, disclosure, transfer, structuring, alignment or combination, indexation, and erasure[6].

2. **Sensitive Personal Data**: The definition of Sensitive Personal Data (**SPD**)[7] retains[8] and clarifies[9] existing categories of sensitive data while adding new categories like official identifiers (Aadhaar numbers and other forms of statutory identification), genetic data, caste or tribe, religious and political beliefs or affiliations, and sex life. A nuanced distinction has been drawn between the new categories of SPD defined as intersex (*defined as a condition*) [10] and

[1] "*A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*" dated July 27, 2018 Available at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf
[2] Available at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf
[3] Section 3(14), Bill.
[4] Section 3(29), Bill.
[5] Paragraph BI (a), Chapter 3, Page 28 of the Report.
[6] Section 3(32), Bill.
[7] Section 3(35), Bill.
[8] Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 also included passwords and sexual orientation.
[9] It clarifies the definition of financial information, health information, and biometric data.
[10] Section 3(23), Bill

transgender status (*defined as a sense of gender*)[11]. Additional categories of SPD may be prescribed by the data protection authority (**DPA**) under the Bill[12]. The Bill will ***not*** apply to anonymized data[13], i.e. Personal Data which is irreversibly transformed such that a Data Principal cannot be identified from it[14]. This exclusion will not extend to mere de-identification, a potentially reversible process where identifiers have either been removed, masked, or replaced with unique codes[15].

3. **Extent:** The Bill is to govern all Processing of Personal Data:
   (a) within India[16];
   (b) by Indian persons (State, corporate, or natural)[17] whether in India or otherwise (horizontal application as laid down in *Puttaswamy*); and
   (c) by Data Fiduciaries or data processors outside India in connection with business in India, systematic activity of offering goods or services to Data Principals in India, or profiling of Data Principals in India[18]. Processing of data by Data Fiduciaries outside India which does not meet this standard will not be covered.

Further, the Bill will not regulate entities outside India that process information of Indian citizens outside India, as the Committee felt this will encroach on the jurisdiction of other States[19].

The Processing of Personal Data

4. **Fair and Reasonable Processing**: The Bill treats data controllers as Data Fiduciaries and imputes a fiduciary relationship with Data Principals[20]. Accordingly, they are required to uphold trust and loyalty[21] and process data in a ***fair and reasonable manner*** that respects the privacy of the Data Principal[22] and ensures a duty of care[23]. This requirement is novel and overarching. It will be interesting to see how far this is extended beyond the more specific requirements outlined elsewhere in the Bill.

5. **Purpose Limitation**: Personal Data can only be processed for the purpose which has been specified at the time of collection, and such purpose needs to be clear, specific, and lawful[24].

6. **Collection Limitation**: Collection of Personal Data is to be limited to data that is necessary for the purposes of Processing[25].

7. **Notice**: The Data Principal is required to give notice, before or at the time of collection, of the purpose for which Personal Data is being collected, categories of Data being collected, details of the Data Fiduciary including its trust score (*if applicable*), details pertaining to sharing and transferring of Personal Data, and rights of the Data Principal[26]. Such notice needs to be clear,

[11] Section 3(41), Bill
[12] Section 22, Bill.
[13] Section 2(3), Bill.
[14] Section 3(3), Bill.
[15] Section 3(16), Bill.
[16] Section 2(1)(a), Bill.
[17] Section 2(1)(b), Bill.
[18] Section 2(2), Bill.
[19] Paragraph A, Chapter 2, page 15 of the Report.
[20] Paragraph B(1), Chapter 4, Page 51 of the Report.
[21] Paragraph B(1), Chapter 4, Page 51 of the Report.
[22] Section 4, Bill.
[23] Paragraph B(1), Chapter 4, Page 51 of the Report.
[24] Section 5, Bill.
[25] Section 6, Bill.
[26] Section 8(1), Bill.

concise, easily comprehensible for a reasonable person, and in multiple languages where necessary and practicable[27]. Where Personal Data is being collected from another Data Fiduciary, notice must be provided to the Data Principal as soon as practicable[28]. The Committee has provided useful guidance on the format of privacy notices[29].

8. **Quality**: The Data Fiduciary is required to take steps to ensure that Personal Data processed is complete, accurate, and not misleading or outdated. Inaccuracies are required to be notified to third parties with whom such data has been shared by the Data Fiduciaries.[30]. One of the factors to consider while taking steps in this regard is to consider whether factual Personal Data is kept separately from Personal Data based on opinions or assessment[31].

9. **Storage Limitation**: Personal Data can only be stored for as long as is necessary to satisfy the purpose for which it is being processed or for the period required under applicable law. Data Fiduciaries are required to periodically review the Personal Data they possess, and purge it where not required[32].

10. **Accountability**: The Data Fiduciary is responsible for complying with the obligations under the Bill and demonstrating compliance[33]. While data processors have been recognized as separate entities, they are only required to comply with contractual restrictions[34].

Grounds for Processing of Personal Data and SPD

11. **Consent**: Personal Data can only be processed on the basis of consent which is free, informed, specific, clear, and capable of being withdrawn[35], given no later than the commencement of Processing[36]. To process SPD, in addition to the foregoing, consent needs to be explicit (i.e. informed having regard to the significant consequences for the Data Principal, clear without requiring reference to the context in which it was given, and specific i.e. allowing the Data Principal to provide separate consents for different purposes, use and categories of SPD)[37]. The Data Fiduciary cannot make the provision of goods and services, or the performance of a contract, contingent on the provision of any Personal Data which is not necessary for such performance[38]. However, in the event of withdrawal of consent, the Data Principal is liable for the legal consequences arising from such withdrawal[39].

    Unlike in the GDPR[40], contractual relationships have not been included as a ground for Processing. The ground has been omitted to protect the severability of consents under a contract and prevent Data Fiduciaries from bundling unrelated Data Processing activities in contracts[41].

[27] Section 8(2), Bill.
[28] Section 8, Bill.
[29] Annexure B, Report.
[30] Section 9, Bill.
[31] Section 9(2)(c), Bill.
[32] Section 10, Bill.
[33] Section 11, Bill.
[34] Section 37, Bill.
[35] Section 12(2), Bill.
[36] Section 12(1), Bill.
[37] Section 18(2), Bill.
[38] Section 12(3), Bill.
[39] Section 12(5), Bill.
[40] (EU) 2016/679 (General Data Protection Regulation).
[41] Paragraph B II (g), Chapter 3, page 41 of the Report.

Interestingly, the Bill also prohibits Data Fiduciaries from Processing categories of biometric data which are notified by the Central Government[42].

12. **Functions of the State**: SPD can be processed where necessary for any function of the Parliament or State Legislature, for exercise of any function of the State authorized under law, or for the provision of any service or benefit from the State[43]. Personal Data can be additionally processed for the issuance of certifications, licenses or permits for any action or activity of the Data Principal[44].

13. **Compliance with law or any order of any court or tribunal**: Personal Data, including SPD, can be processed if explicitly mandated under any law, or to comply with any order or judgment of a court or tribunal in India[45].

14. **Prompt Action**: Personal Data and SPD can be processed to (a) respond to medical emergency involving an individual, pursuant to an epidemic, or any other threat to public health; and (b) ensure safety of, or provide assistance or services to any individual, during any disaster, or any breakdown of public order[46].

15. **Employment**: Personal Data may be processed for recruitment, termination, provision of any service to, or benefit sought by, the employee Data Principal[47]. However, this ground can ***only*** be used if consent is not an appropriate ground in light of the employer-employee relationship, or would involve a disproportionate effort on the part of the Data Fiduciary[48].

16. **Reasonable Purposes**: Personal Data may be processed for other reasonable purposes to be notified by the DPA. Indicative purposes include prevention and detection of unlawful activity, whistle blowing, mergers and acquisitions, network and information security, credit scoring, debt recovery, and also Processing of publicly available Personal Data[49].

Children

17. Data Fiduciaries are required to implement appropriate mechanisms for age verification and parental consent before Processing Personal Data of Children (*persons below the age of 18 years*)[50] based on the volume and proportion of Children's Personal Data being processed, possibility of harm to Children, and such other factors as specified by the DPA[51].

18. Further, Data Fiduciaries operating commercial websites, online services targeted at children, or Processing large volumes of Children's Personal Data i.e. Guardian Data Fiduciaries[52], are barred from profiling, tracking, monitoring behavior, conducting targeted advertising, or undertaking any Processing which, may cause significant harm to Children[53]. However, if a

[42] Section 106, Bill.
[43] Section 19, Bill.
[44] Section 13, Bill.
[45] Sections 14 and 20, Bill.
[46] Sections 15 and 21, Bill.
[47] Section 16(1), Bill.
[48] Section 16(2), Bill.
[49] Section 17(2), Bill.
[50] Section 3(9), Bill.
[51] Section 23 (2) and (3), Bill.
[52] Section 23(4), Bill.
[53] Section 23(5), Bill.

Guardian Data Fiduciary is exclusively involved in providing counseling or child protection services, then they will be exempt from obtaining parental consent[54].

Data Principal Rights

19. **Rights**: The Bill provides several rights to Data Principal, including the right to access Personal Data[55] and details of its Processing, correct it[56], and port it[57]. The Bill proposes a limited version of the right to be forgotten[58], i.e. to restrict continuing disclosure of the Personal Data, only after obtaining an adjudication by an Adjudicating Officer.

20. **Exemptions**: There are certain general exceptions for exercise of the above rights[59]. For instance, a Data Fiduciary is not obligated to comply with any request which would harm the rights of other Data Principals[60].

21. **Privacy by Design:** The Bill requires that every Data Fiduciary is 'Privacy by Design' compliant[61]. This includes adopting periodic transparency measures such as by adopting notice obligations under Section 8 and by incorporating data trust scores[62].

22. **Breach Notification:** The Bill requires notification to the DPA of all Personal Data Breaches but only requires notification to Data Principals where required by the DPA[63]. This shifts the burden of deciding the materiality of breaches from the Data Fiduciaries to the DPA.

23. **Significant Data Fiduciaries:** The DPA may classify certain entities as Significant Data Fiduciaries on the basis of the volume and sensitivity of Personal Data Processed by it[64]. They are subject to enhanced obligations such as impact assessment, registration, audit, and appointment of a Data Protection Officer (**DPO**)[65]. Foreign Data Fiduciaries carrying out any Processing must appoint an India based DPO[66]. In any event, every Data Fiduciary must have a Grievance Redressal Officer[67].

24. **Local Copy:** The Bill requires Data Fiduciaries to keep one 'serving' copy of Personal Data in data centers in India[68].

25. **Critical Personal Data**: A new category i.e. critical Personal Data[69] can be stored only on Indian servers.

26. **Cross-Border Transfer:** Personal Data may be transferred out of India based on standard contractual clauses or inter-group arrangements compliant with DPA prescribed standards. Further, specified countries, sectors within a country, or international organizations, can be

[54] Section 23(7), Bill.
[55] Section 24, Bill.
[56] Section 25, Bill.
[57] Section 26, Bill.
[58] Section 27, Bill.
[59] Section 28, Bill.
[60] Section 28 (5), Bill.
[61] Section 29, Bill.
[62] Section 30, Bill.
[63] Section 32, Bill.
[64] Section 38, Bill.
[65] Section 36, Bill.
[66] *Id.*
[67] Section 39, Bill.
[68] Section 40, Bill.
[69] Section 40(2), Bill.

declared data equivalent by the Central Government upon the satisfaction of certain criteria. Interestingly, cross-border transfers appear to require consent from the Data Principal, in addition to the above requirements[70].

27. **Exemptions**: The Bill proposes certain exemptions to permit Processing for, *inter alia*, prevention, detection, investigation and prosecution of contravention of law, legal proceedings, statistical[71], journalistic[72], or personal[73] purposes. Importantly, it makes an exemption for Processing by small entities which engage in manual Processing[74].

Data Protection Authority

28. **DPA**: The Bill proposes the creation of an independent regulatory body responsible for its effective implementation, the DPA[75]. The duties of the DPA are wide ranging and include: (a) identifying additional categories of SPD and grounds for Processing Personal Data[76]; (b) mandating breach notifications to Data Principals[77]; (c) prescribing various codes of practice[78] including for notice, transparency, security standards[79], de-identification and anonymization[80], contractual clauses and inter-group schemes for cross-border transfer[81]; (d) identifying Significant Data Fiduciaries[82], Guardian Data Fiduciaries[83], and certifying Data Auditors[84]; (e) monitoring Data Fiduciaries and cross-border data flow[85]; and (f) advising Parliament and the Government[86].

29. **Powers**: Certain extensive powers shall vest with the DPA, which shall include: (a) calling for information[87]; (b) conducting inquiries[88]; (c) issuing codes of practice[89]; and (d) issuing directions to Data Fiduciaries or data processors[90]. These directions may range from restricting operations to prohibiting cross-border data flows[91]. The DPA is also conferred search and seizure powers[92] and powers of attachment of property to recover penalties[93].

Enforcement

The Bill prescribes extensive civil and criminal penalties.

30. **Civil Penalties and Damages**: Two key slabs of civil penalties are prescribed. The first (the higher of Rs. 5 Crores or 2% of total worldwide turnover) applies to breaches of notification,

[70] Section 41, Bill.
[71] Section 45, Bill.
[72] Section 47, Bill.
[73] Section 46, Bill.
[74] Section 48, Bill.
[75] Section 49, Bill.
[76] Section 22, and Section 60(2)(c), Bill.
[77] Sections 60(2)(d) and 32(5), Bill.
[78] Sections 60(2)(l) and 61(6), Bill.
[79] Section 61(6)(a), 61(6)(k), and 61(6)(l), Bill.
[80] Section 61(6)(m), Bill.
[81] Section 41 (1)(a), Bill.
[82] Section 60(2)(j), Bill.
[83] Section 23(4), Bill.
[84] Section 60(2)(i), Bill.
[85] Section 60(2)(k), Bill.
[86] Section 60(2)(q), Bill.
[87] Section 63, Bill.
[88] Section 64, Bill.
[89] Sections 60(2)(l) and 61, Bill.
[90] Sections 62, Bill.
[91] Section 65(1), Bill.
[92] Section 66, Bill.
[93] Section 78(2), Bill.

audit, and other compliance requirements[94]. The second (the higher of Rs. 15 Crores or 4% of total worldwide turnover) applies to more egregious violations including breaches in Processing of Personal Data or in making cross-border transfers[95]. One-time and continuing penalties of lesser amounts are prescribed for other breaches[96]. The Bill also provides for compensation to Data Principals[97]. This formulation, structured along the lines of the GDPR, may prove very onerous for smaller Data Fiduciaries.

31. **Authorities**: An Adjudicating Officer[98] is tasked with imposing penalties and orders of compensation[99]. Appeals from the Adjudicating Officer lie to an Appellate Tribunal[100], and a further appeal lies to the Supreme Court of India[101]. The jurisdiction of civil courts is excluded over matters that the tribunal is empowered to take up[102].

32. **Criminal Penalties**: Imprisonment (ranging from 3 to 5 years) is prescribed for persons who knowingly, intentionally, or recklessly obtain, disclose, transfer or sell Personal Data (or SPD) provided that such acts result in harm to a Data Principal[103]. Such harm is very broadly defined to include loss of employment/reputation, discriminatory treatment and/or restrictions on speech or movement[104]. A new offense has been proposed for knowingly reversing de-identification[105]. For corporate Data Fiduciaries, these consequences will extend to persons in charge of operations, or, where consent or neglect is attributable, directors, managers, secretaries or other officers[106].

33. **Amendment and Overriding Effect**: The Bill proposes the deletion of Section 43A (penalizing data controllers which cause wrongful loss or wrongful gain to any person), and Section 87 (which enables the existing rules on governing sensitive personal data), of the Information Technology Act, 2000[107]. Further, unless specified, the Bill will override laws inconsistent with its provisions[108].

34. **Phased Implementation**: By necessity, the Bill contemplates a phase-wise enactment. Once enacted by Parliament, certain sections *(relating to establishing the DPA and the power to make rules and regulations)* are proposed to come into effect immediately. Thereafter, the DPA is proposed to be set up in 3 months, grounds for Processing Personal Data notified and codes of practice issued in 12 months. The operative provisions of the Bill are only to come into effect 18 months from the date of enactment[109].

The Bill seeks to bring about a number of significant changes to the existing general data protection regime in India. Complying with it will mean that Indian Data Fiduciaries will be aligned with global best practices on Personal Data.

[94] Section 69(1), Bill.
[95] Section 69(2), Bill.
[96] Sections 70-73, Bill.
[97] Section 75, Bill.
[98] Section 3(2), Bill.
[99] Section 74(3), Bill.
[100] Section 79, Bill.
[101] Section 87, Bill.
[102] Section 89, Bill.
[103] Sections 90 and 91, Bill.
[104] Section 1 (21), Bill.
[105] Section 92(1), Bill.
[106] Section 95, Bill.
[107] Section 111 read with the First Schedule, Bill.
[108] Section 110, Bill.
[109] Section 97, Bill.

For Indian corporates, this will mean reassessing the nature and quantum of Personal Data they collect, store and process, re-evaluating their current practices surrounding consent and notice, and deciding on the treatment of their legacy data. The structured and phase-wise 18 month enactment schedule that the Bill envisages, may serve to mitigate some of these growing pains.

The Report also notes the dissenting opinions of certain members of the Committee. Their objections surround (a) the inclusion of data localization requirements and criminal offenses in the Bill; (b) the treatment of passwords and financial information as SPD; and (c) the provisions of the bill governing the Aadhaar framework.

Given the importance of the Bill and the framework it envisages, it will likely form the basis for much debate, and potentially some modification, before its enactment.

***

Cyril Shroff
Managing Partner
cyril.shroff@cyrilshroff.com

Arun Prabhu
Partner
arun.prabhu@cyrilshroff.com