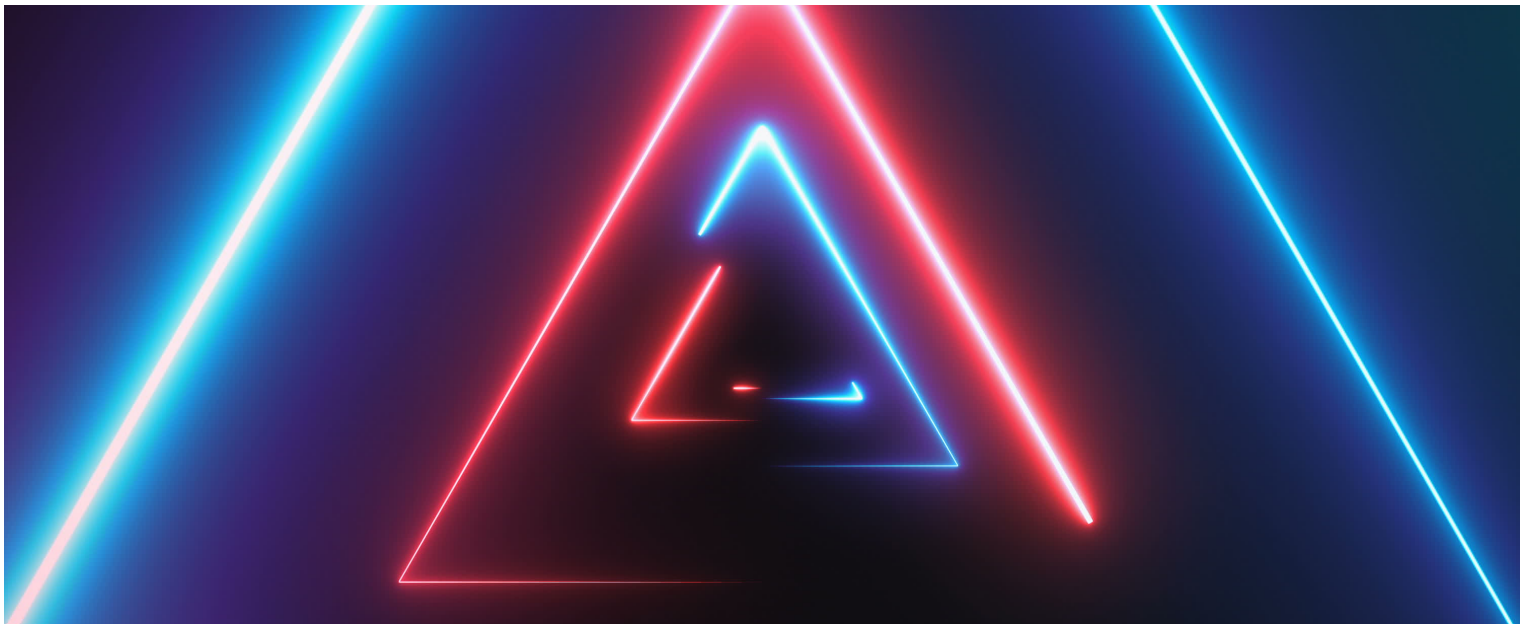
Dec 2018

India: Comparing the Personal Data Protection Bill 2018 with the GDPR

India's Ministry of Electronics and Information Technology ('Meity') published, on 27 July 2018, the Personal Data Protection Bill, 2018 ('the Bill'), comprising *inter alia* grounds for processing personal data and sensitive personal data, cross-border data transfers, and the establishment of a data protection authority ('DPA'). Whilst the Bill awaits enactment and may be subject to modifications, there are key provisions therein for organisations that will come under its scope to consider, particularly for those already grappling with General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') compliance. Arun Prabhu and Samraat Basu, of Cyril Amarchand Mangaldas, provide a comparison of the Bill and the GDPR, and identify key divergences in their approaches to the regulation of data privacy.



noLimit46/Essentials collection

The GDPR[1], which came into force in May 2018, governs over 500 million people[2], and is recognised by many as the most contemporary and comprehensive data protection regulation regime in the world.

India's Bill[3] was proposed by a Committee of Experts ('the Committee') appointed by MeitY[4] to operationalise the principles outlined by the Supreme Court of India in *Justice K.S. Puttaswamy (retd.) v. Union of India*[5]. If enacted, it will govern the personal data of over 1.3 billion people.

The GDPR's influence on the Bill is evident. Obvious similarities between the two regimes include their approaches to defining personal data, their articulation of the rights of data principals, recognition of data protection principles (such as purpose and storage limitation) and approach to enforcement.

A detailed and direct comparison between the Bill and the GDPR is, at this point, necessarily preliminary. The GDPR, with its roots in the Data Protection Directive (Directive 95/46/EC), a body of judicial findings such as *Google Spain*[6] and extensive additional guidance issued by the Article 29 Working Party[7], national data protection authorities and now, the European Data Protection Board[8], is a detailed and fleshed out legal regime whose impact is becoming increasingly clear.

In contrast, much of the material that will eventually make up the legal regime under the Bill remains to be evolved by the DPA to be appointed under it, as provided for by Section 60 of the Bill. For instance, 'critical personal data,' 'significant data fiduciaries' and 'guardian data fiduciaries' are yet to be defined, as are key standards for de-identification and anonymisation, notice, consent, storage of personal data and security safeguards.

While this may potentially lead to more divergence between the two regimes, the DPA may also choose to rely upon the GDPR and earlier EU jurisprudence in evolving India's regime, thereby allaying these concerns.

'Data controllers' versus 'data fiduciaries'

The Bill uses the term data fiduciaries[9] in place of data controllers[10], and data principals[11] in place of data subjects[12]. For the purpose of this article, and for ease of reference, we will continue to use the GDPR's definitions of data subject, data controller and data processor.

This change in terminology appears to be intended to highlight the 'fundamental expectation of trust' between the data principal and data fiduciary, and emphasise the latter's 'duty of care' to lawfully process personal data in a manner that is fair and reasonable[13].

While the requirement to, process personal data lawfully, fairly and transparently, ensure appropriate technical and organisation measures, and apply the data protection by design principle, is well recognised under Article 5(1) (a), GDPR; Recital 39 of the GDPR, the Committee has sought to impute an even a higher duty of care under the Bill. It remains to be seen what the real-life consequences of such a definition will be, given that the Bill goes on to define grounds and bases for processing in some detail[14].

One such consequence may be the manner of treatment of data processors under the two regimes. While the GDPR treats data processors as separate entities with clearly delineated rights and obligation[15], the Bill deals with them less clearly.

Consequently, the Bill does not specify a path for data controllers to devolve some of their obligations on to data processors. This may constrain the ability of the latter to offer specialised 'compliance as a service' solutions.

Personal data and sensitive personal information

Section 3(29) of the Bill defines personal data as data:

'about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.'

This definition is less clear than the GDPR's 'any information relating to an identified or identifiable natural person[16].' Furthermore, the GDPR also lists identifiers considered to be personal data, such as location data and online identifiers[17].

The Bill also differs from the GDPR (and many international data protection regimes) in that it explicitly lists 'financial information[18]' as sensitive personal data under Section 3(35) of the Bill. This may prove problematic in view of the extensive use (and aggregation across databases) of such data for fraud prevention, credit rating, anti-money laundering and related purposes.

In contrast, while financial data enjoys very real and substantial protection under the GDPR and sector-specific EU legislation which considers such data as sensitive (e.g., the second Payment Services Directive (Directive (EU) 2015/2366)[19], such protection avoids a requirement of explicit consent for the processing of financial data, thus avoiding some of the above potential consequences.

Grounds for processing

The Bill specifies the following grounds for processing of personal data under Sections 12 to 17 of the Bill:

- consent;
- functions of the State;
- compliance with law or any order of any court or tribunal;
- prompt action;
- employment; and
- reasonable purpose.

The inclusion of a separate head for 'functions of the State,' and the omission of well-used grounds under the GDPR, such as 'legitimate interest' and 'performance of a contract' may have some interesting consequences.

For instance, under the GDPR, given the nature of the relationship of employment, the use of freely given consent (otherwise a valid basis for processing[20]) to process employee data is generally discouraged. The employer usually relies on either 'legitimate interests[21]' or 'performance of a contract[22]' in order to comply with the GDPR.

Absent any of the above bases, the Bill specifies employment as a separate ground for processing, and thereafter restricts its use only to cases where processing on the basis of consent 'is not appropriate having regard to the employment relationship' or would involve 'disproportionate effort' due to the nature of the processing activities under Section 16 of the Bill.

The omission of 'performance of contract' as a ground of processing also has the potential to result in data controllers having to implement a very complex and layered consent regime.

Perhaps as a consequence, while the data controller is solely responsible for the consequences of consent withdrawal under the GDPR, the Bill makes the data subject responsible for the 'legal consequences' of withdrawing consent to process personal data, where such processing is 'necessary to fulfil a contract to which the data subject is a party,' under Section 12(5) of the Bill.

While the ambit of such 'legal consequences' is unclear, they could presumably extend to the consequences of partly performed contracts, claims for damages and costs for alternative forms of performance.

Reasonable purpose

Under the Bill, grounds of processing under the head of 'reasonable purpose' are required to be laid down by the DPA after considering factors such as the interest of the data controller, the effect on the rights of the data subject, any public interest in processing for that purpose, reasonable expectations of the data subject and the feasibility of obtaining consent under Section 17(1) of the Bill.

Suggested grounds inter alia include mergers and acquisitions, network and information security and recovery of debt, under Section 17(2) of the Bill.

Under Article 6(1) (f) of the GDPR, data controllers may process personal data on grounds of 'legitimate interest' upon assessing that such processing is justified by applying a three step test involving:

1. identification of the legitimate interest;
2. evidencing that the processing is necessary to achieve it; and
3. balancing of this interest against the individual's interests, fundamental rights and freedoms.

Right to be forgotten

Article 17 of the GDPR incorporates a more extensive right to be forgotten, and imposes a requirement on data controllers to erase any data pertaining to the data subject when such erasure is requested under an appropriate ground. Data controllers can, however, refuse to erase personal data relying on alternative legal bases, such as compliance with law or further to a legitimate business interest[23].

Section 27 of the Bill prescribes a much more limited version of this right, only available upon adjudication by an officer of the DPA that disclosure of personal data is:

- no longer necessary or has fulfilled the original purpose;
- based on consent which has since been withdrawn; or
- contrary to provisions of the Bill or any other law in force.

Breach notification

Article 33 of the GDPR requires data controllers to notify breaches in a two-step approach. Firstly, to the supervisory authority within 72 hours of becoming aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons, and secondly to the data subjects if a breach carries a 'high risk to the rights and freedoms of such data subjects,' with some exceptions applying.

The Bill has a more limited requirement regarding notification to data subjects of incidents of breach and vulnerabilities. While it requires data fiduciaries to file a report with the central DPA, it is the DPA itself that makes a call as to whether there is a necessity for the relevant data subjects to be notified[24]. In a similar vein, under Article 34 of the GDPR, where the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

Cross-border transfers of data, and data localisation

The two regimes also differ in their approach to cross-border transfers of personal data.

Under Section 40(1) of the Bill, any data controller engaging in a cross-border transfer of data is required to store a 'serving copy' of all personal data under its control on data systems within Indian borders, irrespective of the location in which such personal data is used or to which transferred.

This restriction has the potential to prove disproportionately burdensome to data fiduciaries. Apart from having to maintain data storage within India, companies may also end up having to reproduce their cloud data storage or processing infrastructure in India where they store or process personal data in a distributed manner.

Further, Section 40(2) of the Bill contains a blanket category of 'critical personal data,' which is prohibited from being transferred to any data system outside India. Sector-specific regulations issued by the Reserve Bank of India similarly restrict the transfer of all data related to payment systems outside India[25].

The GDPR requires all data controllers and processors not established in the EU to maintain a representative of the data controller/processor to be present within the EU unless they are exempted under Articles 27, 37, 38, and 39 of the GDPR. The Bill by contrast only requires 'significant data fiduciaries,' which carry out a larger scale of data processing, to maintain such an officer within India[26].

The GDPR contains a clear bifurcation in regulation of data transfers to countries which have obtained an adequacy decision and to those that have not[27]. Failing an adequacy decision[28], there are specific safeguards that need to be verified before data may be transferred to a country that is not deemed to be 'safe,' such as an enforceable instrument between the countries, standard contractual clauses or binding corporate rules[29]. The Bill, on the other hand, contains only a brief mention of the concept of adequacy of protection, specifying that the central Government must make a determination on adequacy before prescribing transfers to a particular country[30].

Other categories of data controller

Section 38 of the Bill defines various sub-categories of data controllers, including 'significant data fiduciaries' and 'guardian data fiduciaries' based on the volume, sensitivity, and risk associated with their data processing activities. More stringent restrictions are applicable to such entities to mitigate possible harm from violations[31].

While the GDPR does not have separate categories of controllers, it does contemplate exemptions from certain obligations for certain types of processors and controllers. For instance, record-keeping pursuant to Article 30(5) are waived for organisations that employ less than 250 persons unless the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data. Furthermore, under Article 35 of the GDPR a data protection impact assessment is required where processing, in particular relating to the use of new technologies, is likely to result in a high risk to the same rights and freedoms.

Penal regime

The GDPR contains a more comprehensive and structured approach to penalties on data controllers and processors. It specifies that within the bounds of prescribed penalties, the determination of the authority must be effective, proportionate, and dissuasive[32], a direction that has been done away with in the Bill. Further guidelines on penalties under Section 69 of the Bill are yet to be specified, but would be necessary, given the current structure with high base fines.

Another significant difference is the presence of criminal penalties in the Bill. Unauthorised access to, and processing of, personal data is punishable with imprisonment[33].

The GDPR, however, does not deal with criminal penalties, which are dealt with in provisions enacted by EU Member States.

A case for convergence

The cost of compliance with data protection regulations is significant. GDPR compliance costs were estimated at a gross figure of $7.8 billion for the world's 500 largest companies. In an increasingly global world relying on large data silos spanning multiple geographies, the cost of compliance with divergent, or even worse, contradictory legal regimes, can be prohibitive. This may well be a relevant factor for Meity to consider in evaluating the Bill and modifying it for its eventual enactment.

Arun Prabhu Partner
arun.prabhu@cyrilshroff.com
Samraat Basu Consultant
samraat.basu@cyrilshroff.com
Cyril Amarchand Mangaldas, Bengaluru, India

The authors would like to thank Patrice Vanderbeeken, who is a Partner at Pierstone Brussels, Noëllia Chitachi York, who is a Data Protection Specialist at Pierstone Brussels, and Dominik Vitek, who is an Associate at Pierstone Prague, for their valuable inputs during the course of finalisation of the article.

---

1. https://gdpr-info.eu
2. https://europa.eu/european-union/sites/europaeu/files/eu_in_slides_en.pdf
3. Available at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
4. http://meity.gov.in/writereaddata/files/Press_Brief_Data_Protection_1Aug17.pdf
5. *Justice K.S. Puttaswamy (retd.) v. Union of India Writ Petition* (Civil) no. 494 of 2012 dated 24 August, 2017.
6. *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*, Case C-131/12, Court of Justice of the European Union.
7. https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
8. http://edpb.europa.eu
9. Section 3(13) of the Bill; defined as any (group of) person(s) or legal entity(ies) who alone or with others determine the purpose and means for the processing of personal data.
10. Article 4(7) of the GDPR.
11. Section 3(14) of the Bill.
12. Article 4(1) of the GDPR.
13. A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice BN Srikrishna, at p7-10 (2018).
14. Sections 12 to 17 of the Bill.
15. Articles 4(8), 28, 29 of the GDPR.
16. Article 4(1) of the GDPR.
17. Ibid.
18. Which is in turn very broadly defined to include 'personal data relating to the individual's credit history and relationship with financial institutions.'
19. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
20. Article 6(1) (a) of the GDPR.
21. Article 6(1) (f) of the GDPR.

22. Article 6(1) (b) of the GDPR.
23. Article 17(3) of the GDPR.
24. Section 32 of the Bill.
25. https://www.rbi.org.in/SCRIPTs/NotificationUser.aspx?Id=11244
26. Sections 36, 38 of the Bill.
27. Articles 44, 45 of the GDPR.
28. Please note that adequacy decisions can also provide for exceptions or additional safeguards such as *inter alia* for sensitive data.
29. Article 46 of the GDPR.
30. Section 41 of the Bill.
31. Section 38(2), 38(3), of the Bill.
32. Article 83(1), 83(9) of the GDPR.
33. Sections 90 to 93, 95, 96 of the Bill.

RELATED CONTENT

OPINION

Finland: Data Protection Act enters into force after being "significantly delayed"

NEWS POST

Norway: Government launches consultation on ICT security and draft law transposing NIS Directive

NEWS POST

Netherlands: Government releases Brexit assessment tool

NEWS POST

South Africa: POPIA regulations come into effect

NEWS POST

UK: Government publishes draft regulations amending privacy framework