Parliamentary Report Keeps India's DP Bill Partly within GDPR Orbit

Graham Greenleaf

[2022] *UNSWLRS* 9
(2022) 175 *Privacy Laws & Business International Report* 1, 6-9

UNSW Law
UNSW Sydney NSW 2052 Australia

Parliamentary report keeps India's DP Bill partly within GDPR orbit

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney

(2022) 175 *Privacy Laws & Business International Report* 1, 6-9

The thirty-member Joint Parliamentary Committee (JPC) of India's two legislative chambers has presented its Report on *The Personal Data Protection Bill 2019*, two years after the Bill was referred to it in December 2019.[1] The delay was in part in due to covid. The Report is complex, containing a 40 page introduction to Indian's data privacy policies (in the JPC's view), 140 pages of a clause-by-clause examination of the Bill with recommendations for amendments, and 40 pages of dissenting reports from eight Committee members. The dissents primarily criticise the breadth of the grounds under which the government may exempt government agencies from the Bill. References to paragraph numbers, and to Recommendations ('Rec.') are to the JPC's Report.

This article examines the most important amendments proposed by the Report, rather than the aspects of the government's Bill to which no amendments have been proposed. The government's Bill has been analysed previously.[2] The JPC's proposed amendments will be considered by the government, which is likely to put forward an amended Bill taking them into account, before there is a final debate in the legislature. It is therefore likely to take months – or longer – before a Bill is enacted.

DPAI's reduced independence

The government Bill already allowed the government to give directions to the proposed Data Protection Authority of India (DPIA) 'on questions of policy', after giving the DPIA an opportunity to express its views. Although it received submissions that this provision should be scrapped, so that India could have an independent DPA, The JPC proposes the opposite, that the government should be able to give the DPAI binding directions 'under all cases and not just on questions of policy' (Rec. 86). Such directions are not required to be made public, so the potential for abuse is high.

The EU Commission's Decisions concerning Japan and Korea make it clear that the independence of a DPA is an essential ingredient of a positive adequacy finding under the GDPR. The Korea Decision[3] sets out the attributes of independence of the Korean DPA (PIPC) in considerable detail,[4] including that 'PIPA requires Commissioners to perform their duties independently, according to law and their conscience', and the Commission concludes that these and other provisions 'ensure that the PIPC acts with complete independence, free from external influence or instruction'.[5] The implications of a lack of independence go beyond the

[1] *Report of the Joint Committee on The Personal Data Protection Bill,* 2019 Seventeenth Lok Sabha, 16 December 2021

[2] Greenleaf, Graham, 'India's Data Privacy Bill: Progressive Principles, Uncertain Enforceability' (2020) 163 *Privacy Laws & Business International Report* 1, 6-9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572620>

[3] European Commission *Commission Implementing Decision of 17.12.2021*

[4] Ibid 2.4.1 'Independent oversight': paras (113)-(117).

[5] Ibid (115); but see discussion in FN 145 of an extraordinary over-riding provision, never used.

EU. DPA independence is necessary for a country to accede to Data Protection Convention 108+.[6] Membership of the Global Privacy Assembly (GPA), the international peak body of DPAs, also requires that 'The DPA functions as an autonomous and independent body', and one feature demonstrating this is that DPA members 'neither seek nor take instructions from anybody.'[7] It is clear therefore that, internationally, lack of independence denotes a second-class DPA. Over 130 countries have data privacy laws including DPAs, and the majority of those provide for their independence.

Extension of scope to all 'data', not only 'personal data'?

The most radical recommendation by the JPC is that the Bill should deal with 'both personal and non-personal data' [1.15.8]. Since 'non-personal data', read literally, could have nothing to do with people, but (say) concern the movement of shipping containers, or the bleaching of coral reefs, such a law could encompass controls over everything, and this makes little sense. However, the JPC refers to 'a single law and a single regulator to oversee all data that originates from any data principal [personal data subject] and is in the custody of any data fiduciary [personal data controller or processor]' [1.15.8.2]. They seem to want to include coverage of personal data that has been anonymised, or has been de-identified, or is otherwise seen as being in a 'grey area' between personal data and non-personal data [1.15.8.1].[8] The references to 'non-personal' data that they want inserted into the Bill could (I suggest) be read with that understanding in mind, as 'data that originates from any data principal'. However, this narrow reading is difficult to reconcile with the JPC's proposed definition: ' "non-personal data" means the data other than personal data' (Rec. 25). The JPC wants the data protection authority (DPAI) to be able to regulate this type of 'non-personal data'. [1.15.8.3], with provisions for such regulation to be inserted in this Bill once they are finalised [1.15.8.4] (Rec. 2).

How does the JPC recommend the Bill be amended to achieve this? It proposes that data breach notification rules apply to non-personal data (see below), a protective measure. The government Bill already provides that the government, in consultant with the DPAI, may 'direct any data fiduciary or processor to provide any personal data anonymised or other non-personal data to enable better targeting of services or formulation of evidence-based policies' (s. 91(2)). Such directions 'may be exempted from being placed before the Parliament' according to the Ministry advising the JPC (MeitY) [2.270]. Submissions pointed out that there were dangers in the re-identification of supposedly anonymised data, with no safeguards provided, and we could add that these dangers will multiply where uses are in secret. The JPC proposes that directions made under s. 91(2) should be included in the DPAI's Annual Report to Parliament (Rec. 88), but of course that may be long after abuse has occurred.

This expansion of scope to non-personal data is significant, particularly in relation to commercial uses of such anonymised or de-identified data. Both the recently revised data protection laws of both Japan and Korea attempt to also cover such data in their ambit. However, the proposed Indian version is a very vague set of proposals. A separate Parliamentary committee is also examining regulation of non-personal data.

---

[6] Convention 108+, art. 15(5): 'The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.'; see Greenleaf, G 'How Far Can Convention 108+ 'Globalise'?: Prospects for Asian Accessions' (2021) *Computer Law and Security Review* <https://ssrn.com/abstract=3530870>

[7] ICPPPC (now GPA) Working Group on the Future of the Conference *Interpretation of the Autonomy and Independence Criteria FINAL* [as amended post 2019 Annual Meeting] Tirana, Albania, November 2019

[8] '…a large volume of non-personal data is essentially derived from one of three sets of data – personal data, sensitive personal data, and critical personal data – which has either been anonymised or has been in some way converted into non-re-identifiable data' [1.15.8.1] JPC Report.

Special and additional regulation of social media platforms

In the government Bill 'significant data fiduciaries' (SDFs) are data fiduciaries designated (individually or as a class) by the DPAI, based on six criteria of 'significance', particularly the 'risk of harm' of their processing (s. 26(1)). SDFs have additional obligations not imposed on other fiduciaries.[9] There are special provisions for a 'social media intermediary' to be designated as a SDF (s. 26(4)).

The JPC proposes to go further. 'The foremost point of concern for the Committee was that the IT Act [the main current regulation] had designated social media platforms as "intermediaries"' [1.15.12.4] The JPC argues that some social media platforms are not [mere] intermediaries but are in fact publishers because they control factors such as allowing comments on their site, and they have a decisive role in which platform users access their content, including comments. They propose that 'all social media platforms, which do not act as intermediaries, should be treated as publishers and be held accountable for the content they host' [1.15.12.7]. This has major implications far beyond data privacy. Three other parts of the proposal involve facilities for user accounts to be verified (which should at least result in joint liability); for social media companies to be required to have a local office if they operate in India; and for something like a Press Council to be established to regulate both print and digital media (Rec. 6). In addition 'the processing of data relating to children or provision of services to them' has been added as one of the factors to be considered by the DPAI in deciding whether a fiduciary is a SDF (Rec. 47).

Related to these provisions is the recommendation that one of the factors to be considered in relation to penalties based on 'total worldwide turnover' should be the alignment of the Indian fiduciary and a 'group entity' in relation to processing and use of data (Rec. 71). India's *Information Technology Act* already imposes some regulation on intermediaries/platforms, so there is a danger of overlaps here.

The imposition of special obligations on 'platforms' (defined in various ways) is becoming globally popular, including in China's new law,[10] and proposed reforms in Australia.[11]

Data localisation and onward transfers

India's approach to limits on the export of personal data in the government Bill is very unusual, and the JPC's proposed amendments would make it more so.

The government Bill, in effect, divided personal data into four categories, with major differences in the treatment of sensitive and non-sensitive personal data (ss. 33-34). Three types of 'data localisation' result, summarised as:[12]

(1) *Local copy requirements*: A copy of all sensitive personal data must be stored in India', whether or not it is allowed to be exported.

[9] See Greenleaf (2020) for details.
[10] G. Greenleaf 'China's completed Personal Information Protection Law: Rights plus cyber-security' (2021) 173 *Privacy Laws & Business International Report*, 20-23 <https://papers.ssrn.com/abstract_id=3989775>
[11] G. Greenleaf and K. Kemp 'Australia's Online Privacy Bill targets social media giants' (2021) 174 *Privacy Laws & Business International Report,* 1, 5-9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4027702>
[12] For details, see G. Greenleaf 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards' *Submission to Joint Committee, Parliament of India* (12 February 2020) <https://ssrn.com/abstract=3539432>

(2) *Export requirements* allow sensitive personal data (SPD[13]) to be transferred outside India in three situations (all of which also require explicit consent of the data principal): (i) transfers pursuant to contract or inter-group scheme approved by the DPAI, with the exporter remaining liable; (ii) transfers to a country, class of entities etc which the government has found provides adequate protection (but 'adequate' remains undefined); or (iii) the DPAI has allowed transfers 'for any specific purpose'.

(3) *Export prohibitions are imposed on critical personal data* (CPD – to be defined by government), unless exempted for emergency medical purposes, or adequate and also has government approval in the particular case.

(4) *Non-sensitive personal data* has no restrictions on exports, no local storage requirements, unless deemed to be CPD under 3) above.

These complex provisions give the government and the DPAI a great deal of discretionary control, with few legislative constraints, particularly over the broad class of 'sensitive personal data'. The JPC's proposals would make these restrictions even more discretionary. Approval of contracts / intra-group schemes would also require the DPAI to consult the central government, and they could also not be approved 'if the object of such transfer is against public policy or state policy' (which would be given a broad definition) (Rec. 52, 53). The same government consent requirement would apply to any 'specific purpose' transfers approved by the DPAI (Rec. 54).

The result of the combined proposals is strange. 'Sensitive' personal data – which is defined broadly – is given protection which some would say constitutes excessive data localisation (local copies and discretionary export conditions), and the as-yet-undefined CPD is given even stronger protection. Personal data falling outside the 'sensitive' categories, however, is given no protection at all against data exports and onward transfers.

A more legally constrained approach would provide international business with more certainty.

The JPC also recommended that the Bill must be amended to provide that, where sensitive personal data is allowed to be exported, 'onward transfers' of such data to another country, or to a different entity/agency 'unless such sharing is approved by the Central Government' (Rec. 55). An onward transfer restriction is essential to the EU's requirements for 'adequacy', but it is not at all certain that merely delegating the power to approve onward transfers to India's central government will satisfy EU requirements.

From an EU perspective, the data localisation/export proposals appear to be simultaneously too strong and too weak (concerning non-sensitive personal data). The JPC's policy justification for data localisation [1.9] is brief but blunt: it will make data more accessible to government and law enforcement; 'employment generation' will result; India will have more international bargaining power; and citizens and residents will benefit from their data not going to other countries where they are unlikely to be able to pursue remedies for misuse. Data localisation is more than just an excuse for authoritarian governments to keep personal data within easy reach – though it can include that motivation. The EU and US have not previously had to deal with

[13] The Bill's definition of 'sensitive personal data' (s. 3(36)) is unusual because it includes 'financial data', which is largely limited to account identifiers, and data concerning relationships with financial institutions: s 3(18)). The definition excludes racial or ethnic origin (while including 'caste or tribe'), trade union membership, and criminal records. 'Biometric data' (s. 3(7)) and 'genetic data' (s. 3(19)) are both included and defined broadly. The government, after consulting the DPAI and any other relevant regulators, can by notification expand the categories of sensitive personal data (s. 15(1)). The JPC does not recommend changes to these definitions.

such localisation arguments in as powerful a 'friendly' country such as India. They will have to work out how to do so. A 'reject all localisation' approach will be futile.

Exemption of government agencies from the Act

A major exception to the scope of the government Bill arises from the government's powers to exempt, by executive order, 'any agency of the government' from any provisions of the Bill for any type of processing, on a very wide variety of grounds (s. 35). In contrast, the Srikrishna Bill limited such exemptions to grounds of State security, by Parliamentary legislation (not regulations), and only where necessary and proportionate to the objective to be achieved (s. 42 Srikrishna Bill). It has been argued that s. 35 would be inconsistent with India's constitutional right of privacy, because it fails the tests set out in *Puttaswamy #1* for legislative interferences with that right.[14]

The JPC's recommended amendments to section 35 are based on the four legitimating criteria for state interferences in privacy proposed in *Puttaswamy #1* ('action sanctioned by law'; 'necessary in a democratic society for a legitimate aim'; 'interference must be proportionate'; and 'procedural guarantees against abuse') and supported by the Srikrishna Report and Bill. They specifically recommend that the section be amended so that the expression 'such procedure' in section 35 which refers to procedures to be prescribed to be followed by exempted agencies, would be defined so that it 'refers to just, fair, reasonable and proportionate procedure'. They add that this requirement will apply notwithstanding any other legislation currently in force (Rec. 56). The JPC apparently believes that to define the exemption procedure as a 'just, fair, reasonable and proportionate procedure' will be sufficient to import all of the jurisprudence in the *Puttaswamy #1* judgment and the Srikrishna Report draft Bill. This is a vital question, because otherwise the Bill as it stands gives the government an almost entirely unchecked discretion to exempt any government activities from the Bill, simply by an order in writing, and may well be unconstitutional in light of *Puttaswamy #1*.

The JPC position is not tenable. As critics point out, it only refers to procedural safeguards, and does not require the government to demonstrate the necessity and proportionality of the substantive nature of the exemption, as required in *Puttaswamy* #1.[15] The dissenting opinions in the JPC Report are also very critical on this issue.

Adequacy decisions under the GDPR (Japan and Korea) have made it clear that the extent of government access to and use of personal data originating from the EU, and the procedures controlling such access and use, are 'make or break' issues in relation to a positive adequacy finding. The *Schrems I*[16] and *Schrems II*[17] judgments of the Court of Justice of the European Union (CJEU), taken together, set out demanding standards that must be met in relation to access by Indian government agencies, both in relation to transfers from the EU under an adequacy Decision (and attempts to obtain one), and under Standard Contractual Clauses (SCCs) in the absence of an adequacy Decision, as is often the case at present with data transfers from the EU to India.[18] Since *Schrems II* the Commission has released new SCCs,

---

[14] As discussed in detail in Dvara Research *Initial Comments … on the Personal Data Protection Bill'* 16 January 2020, pp. 10-13 <https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf >.

[15] Kazim Rizvi, The Dialogue (NGO), personal correspondence.

[16] *Maximillian Schrems v Data Protection Commr* Case C-362/14 [2015] (Grand Chamber)

[17] *Data Protection Commr v Facebook Ireland Ltd and Maximillian Schrems Case C-311/18* [2020]

[18] See C. Kuner 'The path to recognition of data protection in India' (2021) 33 *National Law School of India Review* 70 <https://papers.ssrn.com/abstract_id=3964672> which gives a comprehensive account of the EU's adequacy requirements and puts them in the context of India.

and the European Data Protection Board (EDPB) has made recommendations on supplementary measures to use with the SCCs,[19] both adding complexity to the valid use of SCCs. It is very unlikely that the few amending words recommended by the JPC would suffice to satisfy the EU's requirements post-*Schrems II*.

Weakened lawful grounds of processing requirements

The Bill currently provides that 'No personal data shall be processed by any person, except for any specific, clear and lawful purposes' (s. 4), but the JPC considered these words to be too vague, and proposes they be replaced with 'The processing of personal data by any person shall be subject to the provisions of this Act and the rules and regulations made thereunder.' (Rec. 28). The government's Bill had already considerably weakened the requirements for non-consensual processing in both the public and private sectors (ss. 11-15). With the replacement of s.4, it is questionable whether the four legitimating criteria for interferences with privacy specified in *Puttaswamy #1* (discussed above) are required by the Bill to be satisfied. This could cast doubt on the constitutionality of the whole Bill.

User rights expanded

The JPC proposes various amendments concerning user rights:

- Where a data principal is **deceased** the right to access should be exercisable by a nominated legal heir or representative, including (at least) the right to be forgotten (Rec. 39).
- The right of **data portability** should not be able to be denied on grounds of trade secrets but only because of technical non-feasibility, as defined in regulation (Rec. 40).
- The **right to be forgotten** should prevent more than just 'disclosure', so 'or processing' should be added at various points in section 20 (Rec. 41).
- Data fiduciaries should be **obliged to comply with requests to exercise rights**, except on grounds specified by regulations (Rec. 42), in addition to the exception allowing non-compliance if compliance would 'harm the rights of any other data principle'. To make sense, these requirements must be cumulative, and that is not clear.
- Regulations should be able to **exempt small to medium enterprises** from the requirement to have a Privacy by Design policy, and the regulation-making power should be clarified (Rec. 43). India is unusual in proposing a law that implements 'privacy by design' at all. However, proposed section 22 is very different from GDPR art. 25 in that it requires a policy, and that it be approved by the DPAI, but does not impose consequences on its non-implementation.
- The requirements on fiduciaries to maintain transparency in processing of personal data, as specified in regulations, should also include where applicable '**fairness of algorithm** or method used' (Rec. 44). Disclosure of algorithms used in decision-making is an unusual and advanced right.
- The **obligation to report personal data breaches to the DPAI should not be conditional** on any assessment of likelihood of harm to data principals. The form of such notice should be specified by regulations and must include details of the remedial actions being taken by the data fiduciary. Notice should be required within 72 hours of the data fiduciary becoming aware of the breach. The DPAI should be able to direct data fiduciaries to take remedial actions, in addition to deciding whether the breach must also be reported to data principals (Rec. 46). These are major improvements to the protection of data principals.

[19] Ibid, part IIB.

- In relation to **data breaches of non-personal data**, the DPAI should be able to 'take such necessary steps as may be prescribed' (Rec. 46), and the DPAI should be enabled take action in response to such breaches (Rec. 65). 'Non-personal data breach' is proposed to be defined as unauthorized processing 'that compromises the confidentiality, integrity or availability of such data' (Rec. 26). This is likely to be a very significant power in relation to data breaches concerning anonymized or de-identified data, and is a significant innovation. However, it is flawed in that it should not be limited to unauthorized processing: many data breaches are a result of authorized but faulty processing.

These are almost all valuable improvements to user rights.

Conclusions – Still a GDPR variant

The JPC's recommended amendments to the government Bill leave its structure unchanged in its essentials. The government Bill was based largely on the Srikrishna Bill. Whether the proposed amendments are accepted or not, the resulting India law is likely to end up heavily influenced by the GDPR, but with more detailed central regulation, a non-independent DPA, far more discretionary powers in the government and the DPAI, a broad power to exempt government agencies held by the central government, and further weakening of lawful grounds for processing. It will have innovations, whether considered desirable or not, such as an attempt to also regulate ill-defined 'non-personal data', a high level of data localisation and different obligations for different classes of 'data fiduciaries.'

If adopted *en bloc*, these variations would move India's Bill further away from many core elements of the EU's notion of 'adequacy', but none are so extreme as to overcome the numerous structural similarities and take the Bill outside the orbit of the GDPR, and a few are valuable.

Nevertheless, India's economic interests would benefit from a different change of direction. As Kuner puts it, India should aim 'to place itself in the international data protection mainstream'[20] by re-starting its attempts to obtain a positive adequacy decision from the EU, applying to accede to Convention 108+, and participating in OECD data protection discussions.[21]

Information: Beni Chugh and Srikara Prasad (Dvara Research) and Kazim Rizvi (The Dialogue) have provided valuable comments, but responsibility for all content remains with the author.

[20] Kener, op cit, p. 73.
[21] Kuner op cit, pgs. 89-91.