Submission on draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY)

Subject: Consultation on the Personal Data Protection Bill 2018

Dear Madam/Sir,

We have read with great interest the recent publication by your Ministry of the report and draft Personal Data Protection Bill (hereafter the "draft law") submitted by the Committee of Experts on Data Protection chaired by Justice B.N. Srikrishna[1].
As you know, we have followed the progress of data protection reform in India closely over the past year, and in January have participated to the consultation on the White Paper on Data Protection Framework for India. Given the significant data flows from the EU to India and the territorial scope of application of the draft law which will also cover foreign operators under certain conditions, the outcome of this reform process is of direct relevance to us.

We want to congratulate the Committee lead by Justice B.N. Srikrishna on the impressive result of its rigorous work. We would also like to commend the open and inclusive consultation process organised by the Indian authorities. The report and draft law confirm that privacy is an area where the EU and India share common values and interests.

Building on these shared values, to increase convergence between our systems could bring very significant benefits to our economies. This would in particular facilitate trade flows which increasingly rely on personal data transfers, while ensuring a high level of protection of the data exchanged between India and the EU.

The report and draft law proposed by the Committee lay the ground for an Indian data protection system characterised by the four key elements of a modern data protection regime: an overarching ("horizontal") law rather than sectoral rules; a core set of data protection principles; an empowerment of individuals with rights to control their data; and finally, the creation of an independent supervisory authority with effective powers to ensure the enforcement of those rules.

With the new law in place, India would be joining the growing trend of global convergence in this area. This is certainly true for the Asia-Pacific area, where countries like Japan, Korea or New Zealand have put in place data protection laws based on these principles, but also in many other regions of the world such as, for example, Latin America where Brazil passed its own law in August this year and Chile has recently announced the setting up of an independent data protection authority, while Argentina is currently reforming its privacy legislation. As a leading world economy and the world's largest democracy, India's endorsement of a high level of data protection would constitute a critical example at a moment where there is an increasing demand for international standards on privacy.

Importantly, if adopted, the law would certainly contribute to facilitating data flows between the EU and India, and could open the way for a possible adequacy dialogue.[1]

Based on our recent experience with reforming our data protection regime (including through a similar consultation process), and in full respect of India's sovereign decision-making process, we would like to offer the following general observations and comments on the draft law for your consideration:

- First, we note that in general, the draft law in a number of places leaves discretion to decide key matters in the hands of the Central Government or the Data Protection Authority rather than dealing with them in the draft itself. This could create some uncertainties which could perhaps be avoided by providing further clarifications in the version of the Bill to be submitted to the Indian Congress. Examples include: the power given to the Central Government to exempt certain data processors from the total or partial application of the law for the processing of personal data of individuals outside the territory of India[2]; the legal basis for data processing "under any law made by Parliament or any State legislature"[3] (without any further specification); the eligibility and qualification requirements to be met by data protection officers[4]; the specific obligations falling on the data processor (which, aside from Section 31 on security, are left to a possible clarification through codes of practice according to Section 61); or the "situation[s] of necessity" that might justify international data transfers[5] (and for which no guiding principles are provided). In sum, further clarifying such important points in the
law itself could be useful to increase legal certainty and legal predictability to the benefit of businesses and citizens alike.

- Second, we welcome the establishment, under the draft law, of the **Data Protection Authority for India**, a key element of any modern data protection law. Having such a body is important both for citizens by providing them with an 'accessible' point of contact to answer their queries and handle their complaints without having to go through lengthy and costly court proceedings. It is also good for business as an independent supervisory authority can ensure consistent enforcement across cases as well as, through guidelines, the uniform interpretation of the rules. Such guidance contributes to legal certainty and, at the same time, adaptability of the rules to evolving technological and economic conditions, which is what business needs.

To effectively play its role, it is essential that such Authority acts with complete **independence** and **impartiality** in performing its duties and exercising its powers, free from any external influence. While the draft law highlights this aspect for the Adjudicating Officers[1], we did not find a clear statement in this regard for the DPA as such. Similarly, the articles concerning the Appellate Tribunal could benefit from further clarifications as regards the qualifications, terms and conditions of appointments, grounds for removal, etc. of its members, as it is the case for the Data Protection Authority.

Moreover, any suggestion that the Authority could be influenced by the Central Government through "directitions" or any other decisions regarding, for example, human or financial resources, could undermine its legitimacy, effectiveness and authority. In this regard, the provision in the draft law according to which "[t]he Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order"[2] might raise questions. The Authority would indeed be "bound" by these "directitions on questions of policy"[3]. Moreover, as these "directitions" shall be "final"[4], they would according to the draft law not be subject to judicial review. The power given to the Central Government to issue binding instructions to the Authority based on such general considerations as the "integrity of India" or "public order" could put at risk the very independence of the Authority.

Also, the provision that prescribes that "the Central Government may, after due appropriation by Parliament by law in this behalf, make to the authority grants of such sums of money as it thinks fit for the purposes of this Act" could be interpreted as granting the Government broad discretion to determine the budgetary allocations to the Authority.[5] In this respect, might be useful to clarify that the Authority must have in any case the financial resources necessary to accomplish its mission effectively and in full independence.

Lastly, Section 100 of the draft law seems to suggest that neither individuals nor business operators would be able to challenge any action by the Authority as long as the latter has acted in "good faith". While independence from the Executive is crucial, this appears to eliminate an important element of judicial control over the conduct of the Authority.

- Third, the draft law in its **Chapter IX (Exemptions)** exempts specific types of data processing (in the interests of state security/criminal law enforcement, in order to pursue legal claims, for journalism) from large parts of the safeguards otherwise applicable. While this concerns legitimate objectives, one might wonder whether their pursuit really requires such broad exemptions from key provisions of the draft law.
Pursuant to the Bill, for instance, data processing operations in the field of law enforcement and national intelligence would not be required to comply with obligations concerning, inter alia, purpose limitation, collection limitation, lawful processing, notice, data quality, data storage limitation, or accountability, nor to be grounded in explicit legal bases outside of a general requirement to satisfy the requirements of legality, necessity and proportionality. Such processing operations by the State would not require data principals to be afforded access or other rights, nor must they comply with transparency and accountability measures, outside of the application of security safeguards.

A more balanced approach might be to provide for mechanisms and processes to reconcile these objectives with the right to data protection in individual cases. In our experience, high data protection standards and effective law enforcement and security operations are not mutually exclusive but can – and actually should – go hand in hand. Such standards contribute to legal certainty, by ensuring notably that evidence is collected lawfully and is thus protected from legal challenges when later used in court proceedings, and can enable law enforcement authorities and judicial authorities to cooperate more effectively and more rapidly with each other, including at international level. To limit any interference with the fundamental rights of the persons whose data is processed for law enforcement and national security reasons, providing at least some essential guarantees (e.g. need for a legal basis, independent oversight, effective remedies for individuals) could be useful. Also, the effectiveness of law enforcement or national security operation can be preserved by providing, for example, that the exercise of the rights of individuals can be restricted – or postponed – to the extent this is necessary and proportionate to avoid prejudicing ongoing investigations.

Fourth, the establishment of clear, flexible grounds for processing of personal data is at the heart of a modern data protection framework. In this respect, we welcome the inclusion of the "reasonable purposes" ground in Section 17, that appears to be largely similar to the GDPR’s "legitimate interests" provision and subject to a comparable balancing test. However, we read in Section 17(1.b) that "reasonable purpose" can also be interpreted as including cases where "the data fiduciary can reasonably be expected to obtain the consent of the data principal". We are wondering what is the exact meaning and scope of this clause, how does it intersect with Section 12 concerning processing of data on the basis of consent and whether they could be a risk that the requirements set forth in Section 12 could be in some way circumvented by this clause. Besides, we understand that "reasonable purpose" could also be used as a legal basis by any fiduciary, including the "State". If this would be a correct reading of this provision, it would very significantly extend the possibilities of processing of data by public authorities. We are thus wondering whether this legal basis should actually be available for processing by public authorities in the performance of their tasks or whether such authorities should not rather rely on legal bases such as the ones provided under Sections 13 and 14 that are better suited for the specific features and needs of these authorities (or whether a distinction should be made between, on the one hand, processing for reasonable purposes and, on the other hand, processing necessary for the performance of a task carried out in the public interest).

Fifth, the provisions of the draft law which require every data fiduciary to ensure the storage of at least one copy of personal data on a server or data centre located in India raise questions. This applies even more so to the provision in the draft law that permits the Central Government to stipulate that "critical personal data" (an undefined category) must be exclusively processed within India. These data localization requirements appear both unnecessary and potentially harmful as they would create unnecessary costs, difficulties and uncertainties that could hamper business and investments. This also applies to the exceptions in
Section 40(3) which provide no clear guidance as to when the Central Government might consider an exception "necessary" or in the "strategic interests of the State".

In our view, such localisation requirements are not necessary, be it from a data protection standpoint, as a matter of economic policy or from a law enforcement perspective:

As regards the protection of personal data, we firmly believe that modern data protection regimes should be designed to afford individuals a high level of protection while facilitating data flows in a way that maximises economic opportunity and consumer interests. As the EU data protection regime shows, a regime that is open to (and in fact facilitates) international transfers while ensuring a high level of protection is possible. Towards this end, our rules, which do not contain any data localization requirements, offer a variety of flexible tools, adapted to different business models and transfers situations, that range from adequacy to contractual instruments and from specific statutory transfer bases (so-called "derogations") to codes of conduct or certification mechanisms.

As a matter of economic policy, such an approach will create significant costs for companies – in particular, foreign ones – linked to setting up additional processing/storage facilities, duplicating such infrastructure etc. and is thus likely to have negative effects on trade and investment. If implemented, this kind of provision would also likely hinder data transfers and complicate the facilitation of commercial exchanges, including in the context of EU-India bilateral negotiations on a possible free trade agreement. We are also convinced that, contrary to what is sometimes suggested, India's striving tech industry does not need this type of forced-localization measures: India is already a top world leader in the data processing industry and has built one of the best digital ecosystems in the world without having recourse to forced localization measures. On the contrary, such measures might deter foreign investment as foreign clients and companies might prefer to switch the processing of their data to a country that does not impose these types of costly constraints. Very much like Ms. Rama Vedashree in her comments to the Srikrishna Committee's report, we believe that "mandating data localization may potentially become a trade barrier and the key markets for the industry could mandate similar barriers on the trade flows to India which could disrupt the IT-BPM industry"[1]. Besides, the existence of such requirements might lead to the multiplication of difficult conflicts of laws when other countries may impose similar but contradictory requirements concerning the same personal data.

Lastly, data localization is by no means the only way to ensure that law enforcement authorities are enabled to obtain (legitimate) access to electronic evidence. In this respect, the EU is facing similar challenges as India. However, rather than forcing the localization of personal data in the EU, it is currently preparing legislation that will allow the police and prosecutors to access electronic information, irrespective of whether it is stored in the EU or not. A similar approach has been adopted by the United States with the US CLOUD Act. Aside from these national legislative approaches, the ideal solution might actually be a multilateral arrangement allowing for mutual access to data. While it needs further strengthening, the Council of Europe's Budapest (Cybercrime) Convention, open to all countries around the globe, is such an instrument and it might be useful for India to consider joining the Convention (which is currently under revision).

• Sixth, we very much welcome the inclusion of core data principal rights such as the right to access and correction, and including "modern" rights such as that to data portability. At the same time, it appears that certain important rights are missing or possibly too restricted.

For instance, the draft law contains no right for individuals significantly affected by decisions
based solely on automated processing (e.g. rejection of an online credit, e-recruiting etc. application) to at least request and obtain an explanation of the logic of such decisions, to be able to challenge them and to obtain a human intervention to possibly revise them. Automated individual decision-making and profiling have great potential to speed up decisions, make them more informed and objective. At the same time, they can also pose risks for individuals, for instance if the underlying algorithms are “biased”.

Regarding the right of access, the draft law provides for a right to obtain "a brief summary of the personal data being processed"[1]. However, there is a question as to whether such a "brief summary" could ensure that the individual receives comprehensive information about the collection and use of his/her personal data by the data fiduciary (for example, how could a "brief summary" of someone's health data be of any use to an individual ?), and thus how helpful such summary will be. Instead, the law could be more specific and empower the data principal with a right to have access to all his/her data, including a copy of all data relating to him/her that are collected or processed.

Also, in order to ensure control of the individual over his/her personal data, it would be important to provide data principals with the "right to object" to processing, at least in situations where such processing takes place for “reasonable purposes” (Section 17). The exercise of this right would not be absolute and could be submitted to conditions to be specified in the law. For example, the exercise of the right could be excluded if the data fiduciary demonstrates compelling legitimate grounds that outweigh the interests of the data principal.

We also note that Section 27 titled the "Right to Be Forgotten" provides individuals with "the right to restrict or prevent continuing disclosure" in limited cases. It might be useful to go beyond this and to give individuals, under certain conditions, the right to have their personal data erased (in particular when the purpose of processing has been achieved or the processing is unlawful).

- Seventh, we note that under Section 38 the DPA shall, based on detailed criteria, assess whether certain data fiduciaries fall within the category of "significant data fiduciaries". This designation in turn determines the applicability of a number of data protection safeguards (e.g. DPO, data protection impact assessment, data audits, records). Given the large number of data fiduciaries, such an ex ante designation might put a heavy burden on the limited resources of the future DPA, which moreover might be slow in carrying out this cumbersome work. Also, the situation might be volatile, with businesses and their operations changing in nature and volume over time, thus requiring constant adjustment. Rather than relying on an ex-ante designation by the DPA, it could be advisable to adopt a risk-based approach – to be further specified in DPA guidelines where necessary – under which the responsibility for self-assessing is on the data fiduciaries, in line with the accountability principle.

Finally, also in light of the fact that we have in the past years gone through a similar process of consultation with stakeholders and reform of our data protection rules, we would like to express our readiness to share our experience and further discuss these issues with you, remotely or by coming to India in case this would be of interest.

We hope that these observations will be useful to you and wish you every success in this very important endeavour.
Yours sincerely,
Bruno Gencarelli

Head of Unit – International Data Flows and Protection
European Commission
Directorate-General for Justice & Consumers
Rue Montoyer 59 (office MO59 03/003),
B-1049 Brussels, Belgium
Tel. (32-2) 29 6.31.63
bruno.gencarelli@ec.europa.eu

[Footnote]:

2. See Remarks by President Jean-Claude Juncker at the joint press conference with President Donald Tusk and Prime Minister Narendra Modi on the occasion of the 14th EU-India Summit (available at: ).
3. See Section 104 of the draft Personal Data Protection Bill 2018.
4. See Sections 14 (a) and 20(a) of the draft Personal Data Protection Bill 2018.
5. See Section 36(3) of the draft Personal Data Protection Bill 2018 where it might be helpful to clarify certain attributes of the DPO directly in the law (e.g. autonomy, expertise in data protection, reporting link to the highest management level).
6. See Section 41(1)(c) of the draft Personal Data Protection Bill 2018.
7. Section 68 of the draft Personal Data Protection Bill 2018.
8. Section 98(1) of the draft Personal Data Protection Bill 2018.
9. Section 98(2) of the draft Personal Data Protection Bill 2018.
10. Section 98(4) of the draft Personal Data Protection Bill 2018.
11. Section 57 of the draft Personal Data Protection Bill 2018.
12. Sections 42 and 43 of the draft Personal Data Protection Bill 2018.
13. See also Srikrishna Committee Report, p. 150.
14. Section 3(13) of the draft Personal Data Protection Bill 2018.
15. Section 40(1) of the draft Personal Data Protection Bill 2018.
16. No definition of "critical personal data" (which must not be processed outside the Indian territory) is provided in the draft law but will have to developed by the Central Government at a later stage.
17. Section 40(2) of the draft Personal Data Protection Bill 2018.

www.eeas.europa.eu

Source URL: