PRIVACY INTERNATIONAL

Comments on the India Personal Data Protection Bill, 2018

October 2018

About us

This submission is made by Privacy International (PI).

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. Working internationally through an International Network of partners, Privacy International works, within its range of programmes, investigates how our personal data is generated and exploited and advocates for legal, policy and technological safeguards. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

To find out more about privacy and data protection in India , please refer to 'The State of Privacy in India' (last updated in January 2018).

Contacts

Ailidh Callander
Legal Officer, Privacy International
ailidh@privacyinternational.org

Alexandrine Pirlot de Corbion
Programme Lead, Privacy International
alex@privacyinternational.org

Overview

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 120 countries worldwide and instruments have been introduced by international and regional institutions such as the OECD,[1] and Council of Europe.[2]

We welcome the effort by the Government of India to reaffirm its commitment to upholding and respecting the right to privacy, and for noting the need to regulate the processing of personal data as being essential for the protection of privacy through the adoption of a data protection law.

The urgent need for this legislation has been reaffirmed in the Supreme Court decision regarding the Aadhaar Act, which stipulates the need for a robust data protection regime.[3]

However, the Personal Data Protection Bill proposed has a number of significant shortcomings. We recommend that to effectively protect privacy and to meet international standards in protecting personal data, that full consideration be given to the areas of concern and improvements outlined below under each Part of the Bill, and include:

1. Overreliance on consent and reasonable purposes

Core grounds for processing included within the Bill are consent and so called 'reasonable purposes', as explained in more detail in our brief both these grounds raise concerns and are open to abuse in their current form.

2. Individual Rights

Rights for individuals relating to their data are a vital part of a meaningful data protection framework. The rights that are included within the Bill, including the right to access and erasure need to be strengthened, including through limiting the time and cost of exercising these rights. The Bill also falls short by failing to include important rights, including the right to object, and rights in relation to profiling and automated decision-making.

3. Data localisation

The Bill includes mandatory data localisation requirements. However, it is unclear what the justification is for making data storage in India mandatory. The justifications for this provision noted in the report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna do not relate to the objective of the law which is to protect personal data. Mandatory data localisation will not provide adequate protection for people's data, i.e. storing the data in India will not necessarily make the data more secure, and secondly, such a requirement may have negative implications for people's rights and the security of their data with the risk that this provision is being used to access personal data for other purposes including surveillance as well as for commercial purposes.

[1] See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013, available at: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonald%20ata.htm

[2] See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 1981, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[3] https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

4. Wide exemptions

The exemptions to the Bill in Chapter IX are all overly wide and must be narrowed. In particular the exemption for Security of State are broad and undefined and thus open to abuse. All of the agencies mandated with the protecting the security of the state and with law enforcement powers must comply with the India's human rights obligations and any interference with human rights must meet the requirements of being in accordance with the law, necessary and proportionate for the pursuant of a legitimate aim – this includes in relation to the right to privacy and thus data protection

5. Role of the data protection authority

An independent and effective data protection authority to oversee the implementation and enforcement of the law is essential in ensuring that the law and the protections it provides translate into practice. Further clarity is required on the operation of the authority, including a timescale for its establishment.

6. Delegated Powers

The legislation has too many delegated powers, which remove the requirement for effective parliamentary scrutiny. These should be limited and the provisions added to the Bill.

7. Harmonisation and application to Aadhaar

The absence of a comprehensive data protection framework in India to date means that it is essential to review and harmonise existing law and practice with the new data protection law. This is not explicitly included within the Bill. Further commitment must be made to ensure that high data protection standards are met across the board, particularly in relation to Aadhaar which has far reaching implications for the privacy and security of people in India.

Detailed Comments

1. Short title and commencement and 2. Application of the Act

The territorial scope of application provided for in clause 1 (2), which states the Act would "*extend to the whole of India*", does not provide sufficient clarity on the scope of the law. This must be reviewed in conjunction with clause 2 to ensure the applicability of the law is clear and unambiguous.

Legislators have an obligation to protect the rights of those in their jurisdiction, including the right to privacy and data protection. Therefore, in order that individuals are not deprived of the protections they are entitled to, the law should be clear on how it applies, to whom and how it protects individuals in each of these scenarios:

- The data controller/data processor is established in India, even if processing takes place elsewhere;
- The controller or processor is not established within India, but is processing personal data of an individual in India; and
- The data is transferred to a third party outside India.

3. Definitions

'**anonymisation'** this term should not be qualified by being met by the 'standards specified by the Authority', rather it should meet the objective test of the individual not being identifiable.

'**de-identification'**
We welcome the Committee's conclusion that "de-identified data" is still to be treated as personal data. We note the reasoning behind the use of the term de-identification and that this it is intended to include pseudonymisation. We are concerned that in practice there may be confusion between de-identification and anonymisation, particularly given that pseudonymisation is used in other legal frameworks (e.g. GDPR and the recent Brazilian Data Protection Law). We consider that the definition of "de-identification" should explicitly highlight the difference, including stating explicitly, as in the Committee report, that de-identified data is still considered personal data. It would also be helpful if there were requirements to transparency of the de-identification and anonymisation processes as this can help ensure the security of such processes. Furthermore, please see our comments on the proposed offence in clause 92.

'harm'
Whilst we welcome the in-depth definition of what constitutes harm, we would recommend that 'distress' also be incorporated into the definition. A data principal should not have to demonstrate actual mental injury to demonstrate that they have been negatively impacted by a breach of this law.
'personal data'
We welcome that the definition of 'personal data' provided for in the Bill includes direct and indirect identifiability in scope. However, we would recommend it be reviewed to include examples such as online identifiers and location data.

'sensitive personal data'
We welcome the inclusion of a wide range of data to be qualified as sensitive personal data. In addition to those listed, we would also request that the definition for 'sensitive personal data' include:

- membership of a trade union;
- philosophical beliefs or other beliefs of a similar nature;
- the racial or ethnic origin of the individual;
- the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings;

Some consideration should be given as to whether there are any other categories specific to the Indian context that should be added. Considering the local context and realities are an important step in ensuring that relevant safeguards are provided for in legislation.

It is also important that higher protections extend to data which *reveals* sensitive personal data, through profiling and the use of proxy information (for example, using someone's purchase history to infer a health condition), it is possible for those processing data to infer, derive and predict sensitive personal data without actually having been explicitly provided with the sensitive personal data. We welcome the Committee's acknowledgement of the sensitivity of geo-location data and would urge inclusion of this within the categories of sensitive personal data.

CHAPTER II DATA PROTECTION OBLIGATIONS

We welcome the inclusion of this Chapter to outline the obligations associated with the processing of personal data.

However, the list provided in this Chapter fails to provide for widely-recognised data protection principles (even if they are provided for later in the Bill):

- **Transparency**: Personal data must be processed in a transparent manner. This principle is key to addressing practices such as the selling and/or transfer of personal data that is fraudulently obtained. Transparency is essential for ensuring that people's data is not used in ways they would not expect. Inclusion of this principle in this chapter would reaffirm commitments to transparency provided for in Chapter VII 'Transparency and Accountability Measures' under clauses 29 and 30 as well as the obligation of fair and reasonable processing in clause 4 and notice in clause 8.
- **Integrity and Confidentiality:** Personal data, at rest and in transit, as well as the infrastructure relied upon for processing, should be protected by security safeguards against risks such as unlawful or unauthorised access, use and disclosure, as well as loss, destruction, or damage of data. Inclusion of this principle in this chapter would complement the 'security safeguards' provided for in Chapter VII 'Transparency and Accountability Measures' under clause 31.

8. Notice

The timeframe provided for in this provision for the obligation to notify for data not collected from the data principal "*as soon as is reasonably practicable'* is too vague and it should be clearly defined.

Subclause 8(1)(e) needs to be reworded to make clear that it is also the "legal basis" for processing and not merely "basis" as it currently reads in the Bill.

We would request subclause 8(1)(h) include safeguards for the cross-border transfer of personal data.

Furthermore, this provision also fails to require the data fiduciary to notify the data principal about:

- the existence of profiling, including the legal basis, the significance and the envisaged consequence of such processing for the data principal;
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data principal.

We also have concerns regarding the exemption provided for in subclause 8(3) in relation to processing provided for in clause 15 and clause 21 (necessary for prompt action') in line with our arguments made in relation to those two clauses (see below).

CHAPTER III GROUNDS FOR PROCESSING OF PERSONAL DATA

The grounds for processing provided for in this chapter all rely heavily on three concepts. The first one provided for in clause 12 is consent, the second on which clauses 13-16 are founded is the concept of necessity and the third in clause 17 is reasonability.

In addition to the more detailed comments provided hereafter, we would like to raise our concerns in relations to these three concepts.

Firstly, on the reliance of consent, we would like to stress that consent is not always the most appropriate legal ground for processing. Consent is a core condition of data protection which allows the data principal to be in control of when their personal data is processed, and it relates to the exercise of fundamental rights of autonomy and self-determination. However, care should be taken that consent is not relied on as a means to disclaim liability for processing and it is vital that for consent to be meaningful it is accompanied by effective safeguards.
Increasingly our devices, networks and the infrastructure on why we rely is designed for data exploitation. This means that in some instances it is beyond the ability of individuals themselves to control the ways in which data about their lives is shared and processed. In those situations where there is a power imbalance between the individual and the data fiduciary (e.g. between employee and employer), this can jeopardise the validity of consent, as there is a high risk that the consent will not be free and there will be very little scope for the data principal withhold their consent, and therefore another legal ground must justify the processing of the personal data and then only what is necessary (e.g. performance of a contract or to fulfil employment law obligations).

In relations to the concepts of 'necessity' and 'reasonability' what remains concerning is that these terms are not defined in the law, and therefore leave room for much interpretation. Parallels can be drawn with the established concepts of necessity and proportionality in international human rights law. The Puttaswamy judgment details the Proportionality Test. In order for processing to be necessary the purpose for the processing must be achieved in the manner that least interferes with the rights of the individual. Clarity must be provided to ensure that the interests of the data principal are at the core of these concepts.

12. Processing of personal data on the basis of consent

Subclause 12 (5) provides for the situation where the data principal withdraws consent for the processing of any personal data necessary for the performance of a contract, then the legal effects shall be borne by the data principal. This mixes consent as a ground for processing personal data with contract and clarity should be provided if it is intended that the contract is a separate legal ground and the relationship with clause 12(3).

15. Processing of personal data necessary for prompt action

We note the aim behind this clause. However, subclauses 15 (a), (b) and (c) refer to "any individual" whose life or health is threatened, needs medical treatment or health services, and or whose safety must be ensured, but this terminology is very broad, and could be interpreted to justify all processing of personal data about any person even if they are not directly associated with the action taken in those instances.

16. Processing of personal data necessary for purposes related to employment

This ground for processing is overly broad and open to abuse, fuelling workplace surveillance and data based discrimination in the workplace. The processing of personal data of an employee should be governed by the employment contract and employment law. Inclusion of a ground for processing relating to contract, as noted above in relation to clause 12, together with the ground for processing in compliance with the law in clause 14 should thus be sufficient and clause 16 deleted.

17. Processing of data for reasonable purposes

This ground for processing is overly broad. In the way it is currently worded it would allow the processing of personal data for a broad range of purposes simply based on the data fiduciary's assessment of the processing being necessary. This provision fails to ensure consideration of the rights of data principals and is open to abuse.

In particular, we are concerned by the following:

- Subclause (17)(1)(a): It is unclear what is meant by "interest" of data fiduciary. Could this also include the commercial interests of a company or the political interests of a political party? The current wording is open to abuse.
- Subclause (17)(1)(c): It is unclear what is meant by "public interest". The term is not defined in the Bill and the Bill does not refer to the definition of "public interest" which could be provided for in other laws in India. The current wording is open to abuse. Also, "public interest" needs to be assessed in relations to the interests, rights or freedoms of the individual.
- Subclause (17)(2): The list provided for in this subclause is overly broad. We do not believe that the Data Protection Authority should have the discretion to define reasonable purposes related to the activities listed in this subclause. Any legal grounds for processing should be defined clearly in the law. The current list of reasonable purposes needs further review and definition and a number of the proposed reasonable purposes should be removed, in particular credit scoring and in terms of sub clause (g), it should be clear that just because data is a matter of public record does not mean that it can be lawfully processed without having to comply with the obligations provided for in the Bill.

This provision requires thorough revision.

19. Processing of sensitive data for certain functions of the State

This provision is overly wide, permitting the use of sensitive personal data for the provision of any 'service' or 'benefit' and does not include sufficient safeguards.

21. Processing of certain categories of sensitive personal data for prompt action

Subclauses 21 (b) and (c) refer to "any individual" in need of medical treatment or health services, and or whose safety must be ensured, but this terminology is very broad, and could be interpreted to justify all processing of personal data about any person even if they are not directly associated with the action taken in those instances. We already noted similar shortcomings in Sub-clause 15, and our concerns are heightened given subclause 21 is about the processing of sensitive personal data which must be subject to higher safeguards.

22. Further categories of sensitive personal data

Subclause 22(1) provides very wide delegated powers to the Authority to specify further grounds of processing of sensitive personal data. We recommend that the Bill is amended to limit such broad powers awarded to the Authority, and to ensure that any deviations from the Act which would increase the circumstances in which sensitive personal data is processed, be subject to an open, inclusive and transparent legislative process.

Furthermore, we are concerned by the high threshold of the risk which must be demonstrated being "of significant harm". This threshold must be reviewed.

CHAPTER V – PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

23. Processing of personal data and sensitive data of children

Clarity is sought as to what constitutes "appropriate mechanisms for age verification" referred to in subclause 23(2).

We are also concerned by the high harm threshold provided for in subclause 23(5) of "significant harm". This threshold must be reviewed.

CHAPTER VI – DATA PRINCIPAL RIGHTS

24. Right to Confirmation and Access

Providing "a brief summary" is not sufficient, a data principal should be provided with at least the following information:

- information as to the identity of the data fiduciary (and contact details);
- the purposes of the processing,
- the legal basis for processing;
- the categories of personal data;
- the recipients of the personal data;
- whether the data fiduciary intends to transfer personal data to a third country and the level of protection provided;
- the period for which the personal data will be stored;
- the existence of the rights of the data principal;
- the right to lodge a complaint with the data protection authority;
- the existence of profiling, including the legal basis, the significance and the envisaged consequence of such processing for the data principal;
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data principal;
- the source of the personal data (if not obtained from the data principal);
- whether providing the data is obligatory or voluntary; and
- the consequences of failing to provide the data.

As noted above in relation to the right to notice in clause 8, a specific timescale must be provided within which data fiduciaries comply with a request to exercise this right (and other rights in the Bill). We note the Committee's comments regarding placing the timescale in delegated legislation but respectfully disagree. The time period should be explicitly provided on the face of the legislation, for example, in the EU General Data Protection Regulation it is 1 month and in the Argentinian Data Protection Law it is 10 days. As noted in the Committee Report the Right to Information Act in India sets at 30 days the timeframe to respond to requests, this is a reasonable time frame and should be included in the Bill.

Subclause 24(2) should also ensure that as well as having access to the data an individual should be provided with a copy of it. Furthermore, particular measures must taken when the data principal is illiterate or faces other challenges in understanding the information they are provided with, especially if it is provided to them in a language that is not their mother tongue.

26. Right to Data Portability

We would like to challenge the exemption provided for under subclause 25(2)(c) to protect trade secrets and in case it is not technically feasible. Further conditions must be included in the law when calling on these exemptions to ensure they are not abused or misused. We do not believe that trade secret can be relied upon to prevent individuals from exercising their right to data portability. As for technical feasibility, the burden should be on the fiduciary to demonstrate that they have adopted all reasonable technical measures currently available to facilitate the exercise of the right to data portability.

27. Right to be Forgotten

It is unclear *who* will have to decide on the form and manner in which this right shall be exercised. Clarity is needed on this element of in subclause 27(4). We understand from the Committee's Report that this will be the adjudication wing of the data protection authority. This is a complex task in practice and we consider further consideration should be given to the authority's role and the resources that they will require in order to effectively exercise such a function. The rights of freedom of expression and information should also be included in the considerations of the Adjudicating Officer under subclause 27(3). Furthermore, it is not clear that this right, actually provides for a right to erasure/ deletion (similar to that in Article 17 of GDPR) – rather it is limited to restriction of processing or preventing further disclosure. If a data fiduciary has no legal basis for processing e.g. one of the conditions under subclause 27(1) are met then an individual should have the right to request that their data is deleted. This should not be limited to 'personal information on the internet' as the Committee's Report suggest but be a comprehensive right.

28. General conditions for the exercise of rights in this Chapter

A central component of any data protection law is the provision of the rights of individuals and so it is essential that these rights be accessible to all without discrimination. With this in mind, we would like clarity on what other alternatives for enjoying theses rights will be put in place should the data principal not be able to submit their request in writing in cases that they may be illiterate, or they may not be able to write in the language asked (if the documentation is requested in a language that they cannot write in), or they may lack of familiarity with procedure, they may also have a disability which prevents them from doing so. Alternatives must be established to handle these various reasons why a data principal may not be able to submit their request in writing.

Furthermore, this subclause needs to provide clarity on the timeframe by which the data fiduciary must manage such requests from data principals. As noted above in relation to the right of access, the number of days in which the data fiduciary must respond to requests to exercise these rights should be explicit on the face of the legislation.

Clause 28 (2) notes that the data fiduciary may charge a reasonable fee to be paid by the data principal if they submit a request to exercise the rights they are provided for in this law. Individuals should bear no cost in exercising this right.

The term "reasonable time period" provided for in Subclause 28 (3) is too vague, and also it should not be to the discretion of the Authority to decide that timeframe. The law should already provide a timeframe within which the data fiduciary must comply with the requests under this Chapter.

Whilst there could be some legitimate reasoning behind the inclusion of the exemption provided for in clause 28(5) around harm to other data principals, this exemption is not clear enough as to how this is to be implemented. Some conditions must be provided for in this subclause in relation to this exemption to avoid any abuse which may negatively impact the data principal seeking to exercising their rights and also to ensure that the rights of other data principals are considered in a meaningful manner.

We also recommend that using a specified format be optional to allow some discretion to data fiduciaries and to avoid this being used as a way to frustrate and delay data principal's exercising their rights.

Rights in relation to automated decision-making and profiling

We note the Committee's comments on page 74 and 75 of the Report against including specific rights in relation to automated decision-making and profiling in the Bill. Other jurisdictions are increasingly recognising the importance of such rights and one key example is in the GDPR, which the Committee considers in its report. Whilst the framing of these rights in the GDPR is not perfect the provisions do go beyond simply involving a step of human review as suggested in the report but also include, for example, limitations (a prohibition) on certain types of solely automated decision-making, as well as the requirement for safeguards. In our response to the White Paper we provided some suggestions on how the Indian Bill can include the prohibition of certain automated decisions and rights in relation to profiling in ways that improve the solutions provided in GDPR. For example, these rights should be treated separately and not conflated as is done in GDPR; there should be clarity in the wording used to ensure that there is clarity on when the provisions apply; as well as safeguards such as the right to an explanation of a decision, the availability of human involvement and the right to redress.[4]

This Bill is an opportunity to lead in rights relating to automated decision-making and profiling rather than just exclude such rights all together from the Bill. Accountability and privacy by design do not replace the need for individuals to have strong and enforceable rights in this regard and the assertion that 'individuals are always at liberty to go to courts' made in the Report disregards the numerous barriers faced by people in accessing justice through the Courts.

CHAPTER VII 'TRANSPARENCY AND ACCOUNTABILITY MEASURES'

29. Privacy by Design

We welcome the inclusion of this obligation, but it is not complete nor sufficient. In addition to being "by design", privacy should also be "by default, e.g. without any manual input from the end user. Such a measure is essential given the cumbersome, complex and highly technical nature of many privacy and data protection policies. The burden should not be on the individual: an individual should not be expected to have the knowledge and expertise to understand the complexity of the services, systems and devices they use. They should enjoy the highest level of protection by default.

[4] See for example, Privacy International's suggestions to contribute to the development of the EU Article 29 Working Party Guidance on automated decision-making and profiling, available at: https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

Subclause 29(d) refers to “commercially accepted or certified standards”. It is unclear what this means in practice (including the level of oversight) and further clarity needs to be provided in this clause.

30. Transparency

We welcome the commitment to ensuring transparency of processing activities. We would however like to seek clarification if this provision is different to the obligation to give notice under subclause 8 to the data principal. Is this subclause meant to be a more general obligation of transparency to the public as opposed to the individual? As noted above, transparency should be embedded as a core principle in the law.
We would also like to seek clarity on subclause 30 (c) which refers to processing “in exceptional situations” and “exceptional purposes of processing” which create a risk of significant harm. These two terms “in exceptional situations” and “exceptional purposes of processing” are not defined elsewhere in the law, and clarity is needed as to what these refer to. Otherwise there is a high risk that these provisions are open to abuse.

Furthermore, an additional subclause should be added to require disclosure of data breaches.

32. Personal Data Breach

We would also challenge the threshold of “harm” occurring for the data fiduciary to have to notify the Authority provided for in subclause 32 (1). Even if no harm occurs, or no harm seems to have occurred, the data fiduciary should have an obligation to notify the Authority. A harm may only be visible at a later stage, and thus there needs to be a record that a breach had occurred. Furthermore, mandatory data breach notifications act as an incentive to improve and maintain data security.

The law should be clear on a specific timescale for notification to the Authority, it should not be left to the discretion of the Authority as provided for in subclause 32 (3). In other jurisdictions, a specific timeframe is provided in number of hours after becoming aware of a breach, for example 72 hours.

We would also strongly recommend that the data fiduciary should have the obligation to notify the data principal directly, and the decision should not depend on the Authority as currently provided for in subclause 32 (5). We are concerned that following this process would cause undue delay to a data principal being notified of a breach of their personal data had occurred and thus delay mitigation measures that could otherwise be taken.

The obligations of data processors in relation to data breaches should also be clear.

33. Data Protection Impact Assessment

We welcome the inclusion of this obligation on data fiduciaries to undertake Data Protection Impact Assessments. We would however request that theses assessments are not only mandatory for the processing “involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data … which carries a risk of significant harm to data principals” as provided for subclause 33 (1) but that the threshold be removed and DPIAs be mandatory in these scenarios and others where there is a high risk to the rights of individuals.

We would also request a clarification as to who the term “data auditor” refers to in subclause 33(2) as this term is not defined in the law, although we understand from the report that they are to be independent external auditors empanelled by the DPA.

Provision should also be made in the Bill to make DPAs publicly available.

34. Recording keeping

It is unclear what "important operations" means in subclause 34(1)(a). Clarity needs to be provided on what this term means as discretion should not be left to the data fiduciary to determine what "important operations" constitute.

It is unclear as to whether subclause 34(3) is intended to stress that this obligation applies to all data fiduciaries as well as the entities listed in this subclause, "Notwithstanding anything contained in this Act, this clause shall apply to the Central or State Government, departments of the Central and State Government, and any agency instrumentality or authority which is "the State" under Article 12 of the Constitution", or whether the obligation applies only to those listed in this subclause. Clarity should be provided on this.

35. Data Audit

We welcome the obligation to conduct audits of processing activities of data fiduciaries. Again, clarity should be provided on who is the data auditor and consideration given to the resource implications. Provision should also be provided for making as much of the audit public as possible.

36. Data Protection Officer

We would like to note that any decision to assign other functions to the Data Protection Officer than those provided for in the law, should consider that none of those other functions lead to any conflict of interest.

In relation to this point, we would also stress the need for Data Protection Officer to be independent in their functions and have guaranteed protection against reprisals.

37. Processing by entities other than the data fiduciary

This provision is very brief and fails to provide sufficient requirements as to what the contract between a data fiduciary and a data processor. Further requirements are needed to ensure that the data fiduciary only engages, appoints or involves a data processor which can guarantee it can and will implement appropriate technical and organisational measures to ensure compliance with the law by demonstrating those measures are in place as well as compliance. This clause should provide more detail on the requirements which this may entail, and which should be included in the contract between the data fiduciary and the data processor. Data processors should be in no doubt as to their obligations under the Bill, and it is important that their explicit responsibility is clear, such as in clause 31 regarding security.

38. Classification of data fiduciaries as significant data fiduciaries

We are concerned by the discretion given to the Authority under this subclause to determine what constitutes a significant data fiduciary. This should be provided for in the law so as to avoid confusion and misinterpretation. The law should consider qualifying the different criteria listed under subclause 38(1) (a)-(f), i.e. what volume of processing, what turnover, etc.

39. Grievance Redressal

We challenge the need for a data principal to have do demonstrate “harm” to be able to have their grievances addressed by the data fiduciary, especially given the high threshold of what constitutes “harm” as defined by this Bill.

CHAPTER VIII TRANSFER OF PERSONAL DATA OUTSIDE DATA

40. Restrictions on Cross-Border Transfer of Personal Data

In relation to the obligation under subclause 40 (1) regarding the storage of data on a server or in a data centre located in India. Data localisation per se does not protect the safety of personal data. If other jurisdictions offer an adequate level of protection, there is no justification based on safety of personal data for preventing their transfer or imposing the storage of the personal data in a particular country. Further, Privacy International noted that in other jurisdictions the imposition of data localisation has been introduced as a way to facilitate unlawful surveillance and limiting the capacity of individuals to protect the confidentiality of their communications.

Furthermore, it is unclear what “critical personal data” means in subclause 40(2). This term is not defined elsewhere in the bill. Clarity needs to be provided on what this term means.

The grounds for exemption provided for in subclause 40(4) are too broad and require further clarification. Firstly, too much discretion is given to the Central Government to decide that “certain categories of personal data” can be exempted from having to be stored data in India”. Secondly, it is unclear what those “certain categories of personal data” could be. Thirdly, the exemption for “grounds of necessity or strategic interests of the State” is too vague and must be clearly defined and limited.

We would also like to seek clarity on the exemption of this subclause not applying to sensitive personal data as provided for under subclause 40 (4) will work in practice.

41. Conditions for Cross-Border Transfer of Personal Data

It is unclear if “other than those categories of sensitive personal data” referred to subclause 41 (1) refers to term “critical personal data” noted in subclause 40 (2) but which is not defined. Clarity is required on what this term means.

Clarity is needed as to who will draft the “standard contractual clauses” referred to in subclause 41 (1)(a).

Subclause 41(1) (b) refers to a test permissibility but it is unclear what that will be. Does this refer to a requirement for adequacy?

The requirement to get consent from the data principal as requested in subclause 41 (1)(e) is confusing and needs to be clarified.

CHAPTER IX EXEMPTIONS

42. Security of the State

Given that agencies responsible for the security of the state are currently not covered by the law, we welcome the recognition of the need to bring to bring these agencies under the law. However, the exemptions provided for in subclause 42 (2) for the processing of personal data in the interests of the security of the State must be revised as they are currently too broad. All of the agencies mandated with the protecting the security of the state must comply with the India's human rights obligations and any interference with human rights must meet the requirements of being in accordance with the law, necessary and proportionate for the pursuant of a legitimate aim – this includes in relation to the right to privacy and thus data protection.

Wide conditions for processing and broad exemptions provided for in section 42 do not meet these standards. This section must be revised and narrowed to ensure compliance with human rights and data protection standards in particular upholding the rights of individuals and subjecting these agencies to independent oversight and accountability mechanisms. We support the Committee's recommendation that the Central Government should expeditiously bring in a law for the oversight of intelligence gathering activities.

43. Prevention, detection, investigation and prosecution of contraventions of law

The exemptions provided for in subclause 43 (2) for the processing of personal data in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law must be revised as they are currently too broad.

At minimum the activities associated with these exemptions should be must be governed by separate legislation to ensure that any processing of personal data is necessary and proportionate to the aim pursued.

Law enforcement agencies should still be subject to principles of transparency, accountability and integrity and confidentiality (i.e. security). Furthermore, if rights are to be suspended during an investigation, such as the right to information and to object, but these must be restored as soon as possible once they no longer risk undermining the investigation.

44. Processing for the purpose of legal proceedings

The exemptions provided for in subclause 44 (1) and 44 (2) for the processing of personal data the purpose of legal proceedings must be revised as they are currently too broad – there is no justification put forward to have an exemption to so many of the data protection obligations.

45. Research, archiving or statistical purposes

In order to avoid abuse and wide interpretation of this ground:

- There is a need for clarity on what the research, archiving or statistical purposes are. Further detail should be included within the law and/or guidance be developed to define this further.
- Such a ground must not exempt a data fiduciary or processor from all of their obligations, and they should provide for appropriate safeguards for the processing of personal data for these purposes.
- Safeguards could include ensuring that the data will not be used to take decisions about the individuals and that the processing is prohibited if it would cause harm.
- A data principal should still have rights over their data including the right to be informed and the right to object that their data be processed for these purposes.

We would suggest including non-governmental organisations working for the public interest within research exemption provided for in this clause.

We would call for the broad discretion provided to the Authority to specific exemptions from Clause 4, clause 31 and clause 33 to be revised. Any exemptions must be clearly provided for in the Bill at the onset.

We are also concerned by the high harm threshold provided for in subclause 45(2) of "significant harm". This threshold must be reviewed.

46. Personal or domestic purposes

This clause exempts certain clauses of the Bill to apply for personal or domestic purposes. However, this clause needs to be revised to ensure that all processing for personal or domestic purposes should not be included within the scope of the bill. This requires clarifying what constitutes "professional or commercial activity" by a natural person which would not be sufficient for them to be data fiduciaries as per the definition provided for in the law but would still require them to comply with some elements of the law.

47. Journalistic purposes

In relations to exemption for journalistic purposes, the necessary measures must be considered to reconcile the right to protection of personal data with the right to freedom of expression and information.
In addition to what is already provided we would suggest that this clause be expanded to include other legitimate exercises of freedom of expression, such as research and investigative activities carried out by independent non-governmental organisations.

48. Manual processing by small entities

We would like to seek clarity on what is mean by "means other than automated means", does this refer to paper records?

CHAPTER X DATA PROTECTION AUTHORITY OF INDIA

49. Establishment and incorporation of Authority

This clause does not provide a timeframe by which the Authority should be established. This should be provided in the law.

We would like to seek clarity of how the offices at other places in India will operate versus the head office. Is the intention to establish a decentralised governance structure?

This clause must stipulate that the data protection authority remains independent, in order to effectively and adequately fulfil its mission of enforcing the data protection framework. The Authority should be free from external influence, and refrain from actions incompatible with the duties of the authority.

51. Terms and conditions of appointment

This clause should provide for a timeframe for the establishment of the authority and appointment of its head/members.

52. Removal of members

We are concerned by the broad discretion given to the Central Government to remove from office the chairperson or any members from the Authority. This threatens the independence of the Authority and its ability to undertake its mandate free from external influence.

We would also request that an opportunity to appeal be given to the chairperson or any members from the Authority who may be removed from office.

53. Grants by Central Government

We are concerned that the dependence on the Central Government to decide as they see fit the funding necessary by the Authority fails to provide necessary process to ensure that the Authority is given sufficient resources to fulfil its mandate.

60. Powers and Functions of the Authority

As noted in our comments to these specific clauses, the broad discretions given to the Authority under clause 17, 22, and 33 of this bill are of concern and must be reviewed. The specification currently at the discretion of the Authority to define must be defined on the face of the Bill.

This clause must also include the power of the Authority to impose sanctions and fees to complement Chapter XI.

61. Codes of Practice

In relation to subclause 61(10), it is not enough that the codes of practice be made available to the public. Consideration must be given on the need to provide the codes of practice in a variety of languages (if the documentation is drafted in a language that they cannot understand) as well as how to make this information available to individuals who may be illiterate, or they may lack of familiarity with procedure, they may also have a disability which prevents them from accessing the Internet.

62. Powers of Authority to issue directions

This clause is a vague and does not provide sufficient clarity on what this power would entail and on what would the authority issue directions.

65. Action to be taken by Authority pursuant to an inquiry.

This clause must also include the power of the Authority to impose sanctions and fees to complement Chapter XI.

66. Search and seizure

We are also concerned with the possible involvement of the as noted in subclause 66(2). We would strongly suggest that instead of involving law enforcement, the Authority be given enhanced investigatory and enforcement powers. The Authority must also be provided with the resources necessary to carry out such investigations and enforcement action.

CHAPTER XI PENALITIES AND REMEDIES

69. Penalties

It is important to ensure that this clause also applies to data processors and not only data fiduciaries.

The fines as provided for in this clause can be easily absorbed by most corporates leveraging data technologies in the country and should therefore be raised significantly in line with emerging practice worldwide.

75. Compensation

Reaffirming our comment on the definition of 'harm' (see above), we would stress the need for the term 'harm' to include distress.

This clause should also include provisions for collective redress. The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organisations processing personal information, which would benefit all those affected. Provision should therefore be made in the process to allow individuals to be represented by qualified representatives and for certain qualified bodies, such as non-profit groups working in the field of data protection, to make complaints and seek remedies.

CHAPTER XII – APPELLATE TRIBUNAL

79. Establishment of the Appellate Tribunal

Clarity is necessary to explain the relationship between the Authority and the Appellate Tribunal.

88. Right to legal representation

We would like to seek clarity as to who constitutes a "legal practitioners or any of its officers".

89. Civil court not to have jurisdiction

This clause limits the avenues to access remedy. We would like to seek clarity as to what would occur if a data principal is not able to access the Appellate Tribunal, for example because of lack of physical proximity? Furthermore, violation of the Bill should not be limited to criminal sanctions which in certain scenarios will be inappropriate.

CHAPTER XIII OFFENCES

90. Obtaining, transferring or selling of personal data contrary to the Act

We are challenging the need for a data principal to demonstrate "significant harm" if their personal data has been obtained, transferred or sold in violation of the provisions in the Bill. This threshold is too high. Even if no harm occurs, a person must have avenues for redress and there must be relevant sanctions, which should not necessarily be criminal.

92. Re-identification and processing of de-identification personal data

We would suggest that consideration be given to 'public interest' in relation to the processing of de-identified personal data with the aim of protecting security researchers who are exploring and researching the vulnerabilities and weaknesses of 'anonymisation' and de-identification techniques with the aim of alerting data fiduciaries, improving them and/or developing Privacy-Enhancing Technologies (PET). This type of research is crucial and must be protected and facilitated by the law.

94. Power to investigate offences.

Clarity is necessary to explain the relationship between the Authority and the police officers which may be granted powers to investigate any offence under the law.

CHAPTER XV MISCELLANEOUS

98. Power of Central Government to issue directions in certain circumstances

The discretionary powers awarded to the Central government in this clause are too broad and vague. This clause must be reviewed to ensure that the powers granted to the Central Government do not permit it to bypass effective parliamentary scrutiny. This threatens the independence of the Data Protection Authority.

103. Power to remove difficulties

As it currently reads it seems to permit that if compliance is too difficult to implement the Central Government could decide to amend the law. This is also open to abuse and wide interpretation. Any changes and/or evolutions in the obligations and safeguards provided in this law must be subject to an open, inclusive and transparent legislative process.

104. Power to exempt certain data processors.

The discretionary powers awarded to the Central government in this clause are too broad and vague. This clause as it stands is open to abuse and wide interpretation. The scope of the law and who it applies to must be provided in this law must be subject to an open, inclusive and transparent legislative process.

105. No application to non-personal data

This clause needs to be reviewed as it lacks clarity as to what "do not govern" personal data means.

Furthermore, to complement our comments on definition on personal data provided for in the bill, we would like to raise the need to address the evolution of what constituted personal data which may be undermined by this clause over time. There is a need for an evolved and expansive definition

'personal data'. In the era of data linkability, and de-anonymisation of data sets, and with the development of artificial intelligence, there are also concerns that other forms of data can *become* personal data, as they can lead to an individual being uniquely identified and identifiable. The signature of movements and device identifiers, including behaviour using the device, can be linkable between non-sensitive and sensitive transactions. The legislation should consider that personal data can be revealed from other data, it can be derived, inferred and predicted.

106. Bar on processing certain forms of biometric data

It is unclear what "certain forms of biometric data" refers to as it is not defined in the bill.
Furthermore, clarity is required as to when and how a Central Government will notify data fiduciaries about the prohibition to processing certain forms of biometric data.

107. Power to make rules

The discretionary powers awarded to the Central government in this clause are too broad and vague. This clause must be reviewed to ensure that the powers granted to the Central Government do not permit it to bypass effective parliamentary scrutiny.

Clarity is necessary to explain the role and powers of the Authority in relations to this clause which awards the Central Government quite numerous (30 in total) and substantial delegated powers.

108. Power to make regulations

This clause must be reviewed to ensure that the powers granted to the Authority do not permit it to bypass effective parliamentary scrutiny.