PRIVACY INTERNATIONAL

Privacy International's Response To The White Paper Of The Committee Of Experts On A Data Protection Framework For India

January 2018

About Privacy International

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. It is based in London and, within its range of programmes, investigates how our personal data is generated and exploited and how it can be protected through legal and technological frameworks. Privacy International has focused on the General Data Protection Regulation (GDPR) and its passage through the EU institutions since 2009. Over the last two decades, it has engaged in the drafting of data protection laws across the world including, but not only, Kenya, Uganda, Indonesia, the Philippines, Brazil, Myanmar, Thailand, Senegal, Mexico, and legal reform on Paraguay, Chile, Colombia, South Africa, Morocco as well as promoting the need for data protection in countries like Pakistan and India. 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.

Contacts

Alexandrine Pirlot de Corbion
Advocacy Officer
alex@privacyinternational.org

Ailidh Callander
Legal Officer
ailidh@privacyinternational.org

Table of Contents

INTRODUCTION 5

PART II - SCOPE AND EXEMPTIONS 6

Chapter 1: Territorial and Personal Scope 6

Chapter 2: Other Issues of Scope 6

Chapter 3: What is personal data? 7

Chapter 4: Sensitive personal data 8

Chapter 5: What is processing? 9

Chapter 6: Entities to be defined in the law: Data Controller and Processor 10

Chapter 7: Exemptions for Household purposes, journalism and literary purposes and research 10

Chapter 8: Cross- Border Flow of Data 12

Chapter 10: Allied Laws 15

PART III - GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS 16

Chapter 1: Consent 16

Chapter 3: Notice 17

Chapter 4: Other Grounds of Processing 18

Chapter 5: Purpose Specification and Use Limitation 19

Chapter 6: Processing of Sensitive Personal Data 19

Chapter 7: Storage Limitation and Data Quality 20

Chapter 8: Individual Participation Rights - 1 21

Chapter 9: Individual Participation Rights - 2 23

PART IV - REGULATION AND ENFORCEMENT 26

Chapter 1: Enforcement Models 26

Chapter 2: Accountability and Enforcement Tools 26

A. Codes of Practice 26

B. Personal Data Breach Notification 26

C. Categorisation of Data Controllers 26
D. Data Protection Authority 26
Chapter 3: Adjudication Process 31
Chapter 4: Remedies 31
A. Penalties 31
B. Compensation 31
PART V - KEY PRINCIPLES OF A DATA PROTECTION LAW 34

INTRODUCTION

Privacy International welcomes the aim of the White Paper published by the Committee of Experts constituted by the government of India under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna to solicit public comments on what shape a data protection law must take. This initiative is an important next step following the recognition of the fundamental right to privacy as read in Article 21 (Right to life and liberty), and Part III (Chapter on Fundamental Rights) of the Constitution in the matter of K S Puttaswamy and others v. Union of India.

Privacy International believes that the initiation of this process offers a significant opportunity for India to draft and adopt a data protection law which would provide the most advanced safeguards for regulating the processing of personal data as well as adopting innovative measures to enforce it.

The responses provided by Privacy International to the White Paper of the Committee of Experts on a Data Protection Framework for India through this open consultation are based on our experiences of working on privacy for over 25 years, our expertise on international principles and standards applicable to the protection of personal data, and our leadership and research on modern technologies and data processing.

We trust that this initial consultation will provide the foundational feedback India is seeking to support its process to develop a data protection framework for India. Our responses reflect on the Provisional Views and questions presented in the White Paper. With the aim of providing clear responses, Privacy International is submitting general comments on certain chapters of the White Paper which includes direct responses to some of the questions and reflections on the Provisions Views. We used this opportunity to welcome some of the thinking of the Committee as well as to highlight areas of concerns, emphasise issues we identified as needing further deliberation and raise issues which we assessed were missing and should be considered.

Privacy International is looking forward to the next steps and hopes the India government will make it possible for stakeholders like us to share their expertise further down line, and in particular during the legislative process which will see India draft a data protection bill. Privacy International remains available to engage further in this process and provide additional feedback which may be sought by the government of India.

PART II - SCOPE AND EXEMPTIONS

Chapter 1: Territorial and Personal Scope

General Comments/ Views on this Chapter:

In order to provide its residents with access to the highest data protection safeguards and the enjoyment of their fundamental rights, Privacy International supports the idea of India adopting an extended jurisdictional scope to apply to any entities established in India or processing personal data of individuals who are in India.

Therefore, the law should apply to:
- processing of personal data by entities, data controllers or processors, established in India, regardless of whether the processing takes place in India or not.
- processing of personal data of individuals who are in India by entities, controllers or processors not established in India, where the processing relates to i) offering goods or services to data subjects in India or ii) monitoring their behaviour within India.

Chapter 2: Other Issues of Scope

General Comments/ Views on this Chapter:

The law should apply to natural persons only. Data protection is about safeguarding our fundamental right to privacy, which is enshrined in international and regional laws and conventions. Legal persons can enjoy other legal protections, such as intellectual property, trade secrets, or specific contractual arrangements to preserve their interests.

The law should apply to processing of personal data by both public and private entities. Whilst there may be exceptions which are provided for within the law for certain types of processing of personal data by public institutions, it is an unacceptable practice that they are completely exempt from protecting the personal data of data subjects, or for those exceptions to be excessively wide or vague.

Any exemption awarded to public entities should meet the test of proportionality and necessity and be clearly set out within the data protection law, with proper checks and balances. If necessary, further guidelines should be developed by the independent supervisory/ data protection authority to explain these to prevent any ambiguity.

The law should include a provision outlining the entry into force and application of the law with clear deadlines. If a transitory provision is introduced to address the issue of retrospective application, it should be clearly defined in scope and time. This information is essential to ensuring a smooth transition process as well as to ensure that the enforcement of the law starts in a consistent manner for all entities subject to the law to comply with their new duties and responsibilities, and for individuals to be informed as to when the law starts being applicable and enforceable.

Chapter 3: What is personal data?

General Comments/ Views on this Chapter:

The two statements provided for consideration in the White Paper are in line with the interpretation of personal data in many jurisdictions and as upheld by regional and international data protection standards.

Nevertheless, Privacy International strongly supports the expansion of the definition of 'personal data' so as to interpret it to include any information which can be used to identify an individual. For example, profiling, tracking and monitoring do not need a specific name/address or other direct identifier, but they can still be used to identify individuals and affect how they are treated. Indirect identification is a key aspect to be included in the definition of personal data.

In the era of data linkability, and de-anonymisation of data sets, and with the development of artificial intelligence, we are also concerned that other forms of data can become personal data as they would lead to an individual being uniquely identified and identifiable. The signature of our movements and our device identifiers, including our behaviour using the device, can be linkable between non-sensitive and sensitive transactions.

This signature then becomes a problematic unique identifier, just as a biometric, linking a device to an individual to a health record.

An inclusive, "future-proof" definition of personal data would guarantee a level of protection already afforded to individuals in other jurisdictions. In this regard, Privacy International would like to bring to the Committee's attention to the definition included in Article 4(1) of the GDPR:

"personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular

by reference to an identification number, location data, online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity."

We would recommend that India address this issue of indirectly identifiable data in the law and if necessary adopt measures requiring the independent competent authority to develop guidance and keep this issue under review.

Chapter 4: Sensitive personal data

General Comments/ Views on this Chapter:

The debate on sensitive personal data has advanced greatly. We strongly encourage India to consider the different categories listed below and integrate them within the definition of sensitive personal data to ensure they are subject to a higher standard of protection.

At the very least, the law should adopt these standards to include:

(i) racial or ethnic origin
(ii) political opinions
(iii) religious or philosophical beliefs
(iv) trade union membership
(v) genetic data
(vi) biometric data
(vii) data concerning health
(viii) data concerning a natural person's sex life or sexual orientation
(ix) criminal convictions and offences

We welcome the inclusion of 'genetic data' being listed in the Provisional Views as 'sensitive personal data' but to complement this addition, we would recommend that biometric data be considered as such too. Biometric data requires additional protections because of the unique ability of biometric technologies to track individuals across systems, the uniqueness of this information, and the sensitivity of the information held within and derived from biometrics.

We welcome and support the consideration in the Provisional Views [4.3 (1)] to treat caste information as sensitive personal data. Along the same lines, we would suggest that India consider any other identifiers which could be deemed to be sensitive personal data in the context of India.

We are concerned by the suggestion in Provisional Views [4.3 (3)] that political or philosophical beliefs should be subject to an assessment as to whether the data subject has an expectation of privacy for these two categories of data. By default, all of the above should be treated as sensitive personal data regardless of the expectation of privacy of the data subject. Failure to do so could result in harm to the data subject, including unlawful discrimination and exclusion.

With data linkability, de-anonymisation of data sets, and profiling practices, we are greatly concerned that even information that is not initially sensitive could quickly become sensitive and that sensitive data can be derived, inferred and predicted from seemingly non-personal data or non-sensitive personal data. Therefore, Privacy International recommends the Committee to clarify that any data processing that leads (or may lead) to the identification of individuals' characteristics such as those listed as sensitive data should be subject to the highest safeguards.

Chapter 5: What is processing?

General Comments/ Views on this Chapter:

The definition proposed is in line with the definition of 'processing' provided for in many jurisdictions as well as regional and international data protection standards.

The definition of 'processing' should be broad and inclusive rather than exhaustive. This would encourage India to think innovatively and progressively to respond to current and future technological advancements in this definition. With this in mind, we would like to put forward the idea of specifically integrating the 'generation' of data as an activity which must be regulated and overseen, and for which individuals must be awarded protection.

This suggestion is based on Privacy International's analysis that the problems with what we have called 'Data Exploitation' often begins with excessive generation, since generation is the precondition for further processing. This excessive generation of data by the systems and services we use, together with other root causes such as lack of awareness, transparency and accountability lead to the core problem of power imbalances in a data driven world. This addition to the definition of 'processing' would complement the 'use limitation principle' and concept of 'data minimisation'.

Chapter 6: Entities to be defined in the law: Data Controller and Processor

General Comments/ Views on this Chapter:

As accountability and enforcement are key to the success of the protection of personal data, the law should clearly identify the parties responsible for complying with the law as well as their obligations and duties to ensure compliance and protection of the rights of individuals, and what measures they should take should they fail to do so, and/or the rights of individuals that are at risk or/and infringed such as notifying individuals and providing them redress.

Entities that have control over personal data and/or process personal data, often known as data controllers and processors respectively, should have obligations set out in the law which require them to inform the independent supervisory authority that they are processing personal data, and to abide by the principles outlined in the law to ensure the protection of the rights of individuals.

Privacy International recommends that the data protection law in India includes obligations not only for data controllers but also for data processors. Data controllers and processors are responsible for ensuring that they take all necessary measures to ensure compliance with the law. The law should clearly define data controllers and processors and provide clear responsibilities, obligations and liability for both. The law should also address the relationship between controllers and processors and specify clear requirements as to what is expected (see for example Article 33 of GDPR). Controllers and processors should also be subject to record keeping obligations, security obligations and data breach notification requirements.

Chapter 7: Exemptions for Household purposes, journalism and literary purposes and research

General Comments/ Views on this Chapter:

The four categories of exemption listed in this section i) Domestic/Household processing, ii) Journalistic/Artistic/Literary Purpose, iii) Research/Historical/Statistical Purpose and iv) Investigation and Detection of Crime, National Security, are common categories of exemptions in data protection laws in other jurisdictions and are provided for in regional and international data protection standards.

However, the scope of the exemptions varies and should be carefully considered to ensure that

they do not undermine the safeguards provided for in the law by being over expansive, broad and vague.

In particular, we would like to highlight the following:

Domestic/Household processing: Along with limiting scope of the law to 'natural persons' it is widely accepted that processing for domestic or household purposes is exempt from application. Some jurisdictions include further criteria to this exemption. For example, the GDPR also requires that it be "with no connection to a professional or commercial activity" (Rec. 18). In an online world, where the lines between professional and personal are increasingly blurred, consideration should be given to how this exemption is defined and explained to data subjects.

Journalistic/Artistic/Literary Purpose: This exemption is often narrowly construed and interpreted in other jurisdictions (see draft bills proposed in Argentina and Brazil). A narrow "journalistic exceptions" risks leaving out other legitimate exercise of freedom of expression, including investigations carried out by independent non-governmental organisations or by individuals that do not qualify as "journalists" under national law. Privacy International recommends that the exemption includes journalistic, artistic/literary expression, or other freedom of expression or human rights purposes.

Research/Historical/Statistical Purpose: Exemptions for these purposes should only be applied when strictly necessary and not be seen as a blanket exemption. The activities subject to the exemption need to be clearly defined, for example, is research limited to academic research or does it include commercial research? There should be sufficient safeguards in place to protect the rights of data subjects. Furthermore, whilst rarely noted within this provision as an exemption, Privacy International would suggest that this exemption apply under certain conditions to research carried out by independent non-governmental, non-for-profit organisations. Data protection standards should be applied as far as possible and detailed consideration should be given to any limitation on the rights of data subjects and the relevant data controllers should consider and mitigate any prejudice to the rights and freedoms of the data subjects. A data subject should be given the right to object that their data be processed for this purpose.

Investigation and Detection of Crime, National Security: Privacy International agrees that is better and more appropriate to develop specific exemptions than providing blanket exemptions for (i) information collected for the purpose of investigation of a crime, and apprehension or prosecution of offenders; and (ii) information collected for the purpose of

maintaining national security and public order. Privacy International recommends that the processing of personal data by law enforcement and intelligence agencies is subject to the same essential data protection rules as the rest of the public and private sectors. This is particularly so in relation to the data protection principles and the rights of data subjects, as well as provisions regulating transfer of personal data to third countries. In particular, Privacy International recommends that the Indian data protection law does not provide for the issuing of blanket national security certificates or any other mechanisms that allow for a wide exemption to the data protection principles and which lack transparency and effective oversight.

Privacy International agrees that the two safeguards provided for in the Provisional Views 5) and 6) are necessary to provide some minimal safeguards against misuse of these exemptions:

5) The exemptions must be defined in a manner to ensure that processing of data under the exemptions is done only for the stated purpose. Further, it must be demonstrable that the data was necessary for the stated purpose.
6) In order to ensure that the exemptions are reasonable and not granted arbitrarily, an effective review mechanism must be devised.

On a general note, Privacy International would like to bring attention that the title of this chapter did not directly refer to the exemptions for the purpose of investigating of a crime, and apprehending or prosecuting offenders and the purpose of maintaining national security and public order. We would strongly insist that this exemption be clearly addressed from the onset in this chapter or be treated within its own chapter to provide it the attention it requires given the risks that may emerge from a wide, over-arching exemption on this basis.

Chapter 8: Cross- Border Flow of Data

General Comments/ Views on this Chapter:

There are various models adopted to regulate and manage the transfer of data across borders. Some jurisdictions such as Mexico resort to a privacy notice to be agreed which will provide for whether or not the individual agrees for their data to be transferred and the recipient of the data will have to comply with the same obligations as the original data controllers.

Another mechanism for regulating and overseeing international data transfers is for an

assessment of adequacy to be undertaken for the expected recipient of the data. This is the model adopted in the EU and Argentina, for example.

Any sharing and transfer of personal data to entities in other countries can only be allowed if the recipient of the data provides a level of protection of personal data that is at minimum equivalent to the level established in the national law of the sender. The assessment can be conducted by an independent competent authority, such as the independent supervisory body established by the law. The assessment of the level of protection of personal data afforded in the third country should at least include explicitly:

- rule of law, respectful of human rights including national legislation in force in areas such as public security, law enforcement and intelligence agencies; as well as the laws, policies and practices regulating access to personal data by public authorities and private entities; and regulatory/professional rules;
- existence and effective functioning of independent supervisory authorities to ensure compliance with the law;
- the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

This assessment should be reviewed regularly and so this provision should provide for a periodic review mechanism of the decision-making process.

If an adequacy assessment cannot be undertaken, the controller or processor should take measures to compensate for the lack of data protection to ensure that the appropriate safeguards exist and are enforceable to protect the data subject.

For example, whilst Section 12 of Argentina's Data Protection Law 2000 No. 25.326 prohibits transfers to countries that do not provide adequate levels of protection, the adoption of a Regulation in 2016 introduces two model contracts for international data transfers to countries that do not provide adequate levels of protection with one applying for transfers by data controllers to data controllers, while the other must be used for transfers to data processors rendering services.

In South Africa, the law provides for a set of conditions which must be complied with by the 'responsible party', the sending party, to transfer personal information about a data subject to

a third party in a foreign country. These include (i) the data subject must consent to such a transfer; (ii) the transfer is necessary for the performance of a contract; and (iii) the transfer is for the benefit of the data subject and it is not practicable for the 'responsible party' to obtain the consent of the data subject for that transfer.

Irrespective of the exceptions deployed, these need to be highly regulated and will require further guidance to ensure that they are not potentially broadly interpreted and are compliant with human rights standards. These exceptions must be narrowly interpreted to ensure that such agreements do not result in the weakening the data protection offered in the law.

In particular in relation to the cross-border transfer of personal data by intelligence agencies and law enforcement, Privacy International recommends that the overarching principle is that any transfer of personal data to third country is afforded the same level of safeguards as other transfers of personal data. This is particularly necessary given that intelligence sharing arrangements between agencies in different countries are typically confidential and not subject to public scrutiny, often taking the form of secret memoranda of understanding directly between the relevant ministries or agencies. Non-transparent, unfettered and unaccountable intelligence sharing threatens the foundations of the human rights legal framework and the rule of law.

Regardless of the purpose, there is no rationale to justify transfers by intelligence agencies having lower safeguards than those applicable to law enforcement's transfers. In reviewing India's compliance with its international human right obligations, the report of the UN Universal Periodic Review Working Group included a recommendation for India to:

5.145. Bring all legislation concerning communication surveillance in line with international human rights standards and especially recommends that all communication surveillance requires a test of necessity and proportionality (Liechtenstein);

5.146. Take the necessary steps to ensure that all operations of intelligence agencies are monitored by an independent oversight mechanism (Liechtenstein);

Privacy International believes that the data protection law offers a significant opportunity for India to implement these recommendations.

Chapter 10: Allied Laws

General Comments/ Views on this Chapter:

A general data protection framework, such as that which will be provided by the Indian data protection law, does not preclude the adoption or application of sectoral laws regulating particular sectors.

However, Privacy International recommends that the data protection law makes it clear that its scope is to protect the fundamental rights of individuals, such as the right to personal data protection, and therefore any laws (current or future) which contradict such protection, e.g. by limiting those fundamental rights, should be considered null and void. This would not preclude the application of any laws that provide higher safeguards.

PART III - GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

Chapter 1: Consent

General Comments/ Views on this Chapter:

Consent is a core condition of data protection which allows the data subject 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.

Consent must be freely given, informed and specific to the processing in question. The manner in which consent is obtained must be carefully considered, individuals should be informed in a clear, accessible and intelligible way about the processing and what they are consenting to. Consents should be 'unbundled' or separated and not presented as a take it or leave it (overall consent) option. For consent to be freely given, individuals should be able to withdraw consent in the future.

Reliance on consent should not negate the obligation on data controllers to comply with the data protection principles including transparency, fairness, purpose limitation and data minimisation. Even where relying on consent, data controllers should carefully consider (for example through a data protection impact assessment) any prejudice to the rights of individuals as a result of the processing and take steps to mitigate these.

The provisional views expressed in the white paper in Section 1.4 (3) indicate that "the standards for implied consent may need to be evolved in order to ensure that adequate information is provided to the individual giving her consent". Privacy International is concerned by the high risks of abuse in relying on 'implied consent'. We recommend that for consent to be a valid legal basis for processing, it must be explicit and unambiguous i.e. demonstrated by a clear indication of the individual's wishes.

A further consideration to be taken into account is how to manage consent where there is an imbalance of power in a relationship, which can jeopardise the validity of consent. For this reason, consent is one ground of processing, in that where processing is necessary, for example for, compliance with a legal obligation or for the performance of a contract, it would be disingenuous to seek consent if it is necessary for the purpose of processing that the processing

go ahead anyway. An important part of 'free consent' is the ability to withdraw consent and in situations where this is incompatible with the purpose of the processing, another basis of processing (other than consent) will be needed. All other conditions for processing should be clearly defined, narrow in scope and subject to the requirement of 'necessity', in that the processing should cause minimum interference to the rights of the data subject and there should be adequate safeguards in place.

Chapter 3: Notice

General Comments/ Views on this Chapter:

Notice is key to fair and transparent processing. As such notice should be a requirement for public and private data controllers and should be provided to the data subject both when the data is collected from the data subject and from a third party. Privacy or data protection impact assessments can be an important tool for evaluating the effectiveness of notices, and regulatory guidance on privacy notices should be provided. Enforcement and redress mechanisms must also be available to ensure that data controllers take their notice obligations seriously.

The form of notices will be context specific however data protection law should contain prescriptive provisions as to what information, as a minimum, a privacy notice should contain, and requirements as to the form such as concise, transparent, intelligible, easily accessible and using clear and plain language.

The law should specify what information a notice should contain, as a minimum. At the time the personal data is obtained (whether directly from the data subject or a third party), the data subject should be informed of:

- The identity and contact details of the controller
- The purposes of the processing
- The legal basis for processing
- The recipients of the personal data, where they are located and what safeguards will be in place
- The period for which the personal data will be stored
- The existence of the data subject's rights
- The right to lodge a complaint with the data protection authority

- The existence of automated decision-making and/or profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- The source/ origin of the personal data.

Chapter 4: Other Grounds of Processing

General Comments/ Views on this Chapter:

There may be specific limited scenarios where consent is not the most appropriate legal basis for processing. These other lawful grounds for processing should be specifically defined and include relevant safeguards. Other grounds for processing should include a requirement that the processing is necessary and proportionate, in the sense that the purpose of processing could not be achieved in another way that interferes less with the rights of the data subject. If the Indian data protection law includes the conditions of necessary for the performance of a contract and necessary for compliance with a legal obligation, care should be taken that it is made clear to the data subject what the contractual requirement is, and why and what the relevant legal obligation is. Contractual terms should be otherwise regulated to protect consumers from unfair terms and any law permitting the processing of personal data (and thus an interference with the right to privacy/ data protection) should meet the tests of lawfulness, proportionality and necessity.

A public interest ground should be clearly defined to avoid being abused. For example, it should be possible to list the specific public interest grounds (e.g. administration of justice) and ensure that such a list is clear and exhaustive.

If there is to be a condition which permits processing of data in emergency situations, this should be carefully thought through and defined. All grounds for processing should be subject to other safeguards to protect the rights and interests of the data subject, including fairness, transparency and a data protection impact assessment which clearly takes into account any prejudice or adverse effect on individuals.

The 'legitimate interest' condition included for example in Article 6.2 (f) of the GDPR (with an exclusion for public authorities carrying out their public tasks), can provide a significant loophole for abusive or excessive processing, in particular if it allows for processing for 'any' interest, including those of a third party. Privacy International believes that this should not constitute a legal ground for processing. At the very least, detailed guidance and oversight must be

provided to ensure that where it is relied upon, individuals' rights can always override processing for legitimate interest. As well as being limited to processing that is 'necessary', if there is any doubt in the balancing exercise that there is prejudice to the individual, then the presumption should be that the processing should not go ahead. Furthermore, it is imperative that data controllers provide clear notice to the individuals of the specific legitimate interest they are relying on (i.e. they cannot simply rely on generic or vague legitimate interest) and allow for assessment of prejudice to individuals on a case by case basis, including offering an opt-out mechanism.

Chapter 5: Purpose Specification and Use Limitation

General Comments/ Views on this Chapter:

Purpose specification and use limitation are key principles of data protection. Technological developments (and the mass generation, collection and analysis of data which accompany them) mean that these principles are ever more important. The purpose of the processing and the proposed use of it must be clearly defined and explained to the data subject. If the data is to be used for a purpose other than the original purpose, then the data subject should be adequately informed of this and a legal condition for processing identified. This may necessitate obtaining further consent. It is particularly important that sensitive personal data is not processed for purposes other than those originally specified. Personal data should only be retained for the period of time that it is required for the purpose for which it is collected and stored. This will strengthen and clarify the obligation to delete data at the end of processing which should be included in another provision such as the data quality principle. Guidance on how to implement these principles in practice should also be provided.

Chapter 6: Processing of Sensitive Personal Data

General Comments/ Views on this Chapter:

The law should recognise that certain categories of personal data are so intimate to a person as to require a higher level of protection. The types of data that constitute sensitive personal data are discussed in more detail above in response to Chapter 4.

As a minimum the following protections should be included: a prohibition on processing sensitive (or special category) personal data unless a specific narrow exemption applies; limits

on the use of sensitive personal data for automated-decision-making; safeguards for international transfers; and record-keeping and data protection impact assessment obligations. The exemptions for processing sensitive personal data need to be clearly defined and narrowly construed. Consent, for example, should be explicit (rather than implied), although Privacy International's position is that consent should always be explicit. The sensitivity of the data should also be considered in enforcement and redress mechanisms. If these protections can be strengthened through sectoral regulation (for example in the financial or health sector) then this is to be encouraged.

Chapter 7: Storage Limitation and Data Quality

General Comments/ Views on this Chapter:

Storage limitation

Storage limitation or data minimisation is a key concept of data protection, both from an individual rights and information security perspective. The law should clearly stipulate that data should not be kept for longer than necessary for the purpose for which it was originally obtained. Any exceptions to this must be very limited and clearly defined. Just because the data controller might come across another use of the data during the passage of time does not justify blanket indefinite retention. How long it is necessary to store data will be context-specific, however, this should be guided by other legislative obligations, regulatory guidance and industry practice. So that individuals are fairly informed about the processing of their data, they must be informed as to how long their data will be retained. Therefore it is imperative that the legislation incentivises data controllers to implement the data minimisation principle by minimising the collection of personal data and not storing it longer than necessary.

Data controllers should establish retention schedules specifying the retention periods for all the data that they hold and keep these under regular review. This is separate to deleting personal data on the request of the data subject, which must also be provided for in the legislation. After the necessary time period personal data should be securely deleted. If data is to be stored beyond the retention period in an anonymised (and not pseudonymised) form, the privacy implications and any consequences for the data subjects must be carefully considered.

Data quality

Data quality or accuracy is also a key concept of data protection, both from an individual rights perspective and that of the data controller. The onus should be on the data controller to ensure data is accurate, complete and up to date. Data controllers should keep the personal data they process under regular review and every reasonable step must be taken to ensure that inaccurate personal data is rectified or erased without delay.

Chapter 8: Individual Participation Rights - 1

(Confirmation, Access and Rectification)

General Comments/ Views on this Chapter:

The 'individual participation principle' is a key principle of data protection which encompasses many rights, such as the right to information on how the data is being processed, the right to access the data and the right to rectification of inaccurate data. All these rights must be incorporated into a data protection law for India. These rights are reflected in various international and regional standards and form part of the acquis of the scope of the right to privacy and data protection.

The UN Human Rights Committee, in interpreting the scope of obligations of states parties to the International Covenant on Civil and Political Rights (of which India is a party since 1979), noted, back in 1989, that:

> "In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination." (Human Rights Committee, General Comment No 16 on Article 17 of ICCPR.)

Right of confirmation and access (and the right to information)

The rights of confirmation and access to personal data are core to data protection and protecting the right to privacy. The right to confirmation and the right of access is also the right that other individual rights relating to data protection hinge on. You will generally need to know what and how your data is being processed in order to decide whether to exercise your right to object, rectify, restrict, portability or erasure.

A key part of the right of access is understanding how personal data is processed. Therefore, the right of access should specify the information that a data subject is entitled to (some of which they should have been provided to at the beginning of the processing as a part of their right to information). This information includes the purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data has been or will be disclosed, the envisaged period for which the personal data will be stored, the existence of individual rights in relation to personal data, the right to lodge a complaint with a data protection authority, and the existence of automated decision-making and/or profiling and meaningful information about the logic involved. Where the personal data have not been collected directly from the data subject, they should be provided with information about the source of the data. This information should be accompanied by a copy of the personal data. There should not be a disproportionate effort exemption; this is an ambiguous term and can lead to abuse of the right of access. If a data controller takes the decision to process personal data then they should have the corresponding right to provide access, regardless of the effort involved.

It is not sufficient to merely provide for a right of access; the law should provide further minimum requirements in relation to the process of obtaining personal data. These include requirements on:

- Timeframe: This should be within a reasonable specified time (for example 30 days).
- Cost: There should be no cost in exercising this right (while some legislation allow the charging of reasonable costs, that is not the case under GDPR and this approach should be adopted in India, where many still live in poverty and where even a relatively small cost may be an significant financial burden to the exercise of individual's rights.)
- Format: The information provided to the data subject should be in a form that is readily intelligible to them and does not require them to have any particular expertise or knowledge to comprehend the information they are provided with.

- Appeal: If the request is denied, the data subject has a right to be given reasons why, and to be able to challenge such denial. Furthermore, if their challenge is successful they must have the right to have the data erased, rectified, completed or amended.
- Clarity: Any restrictions of the right of access should be clearly and narrowly defined in law. If data is withheld from an access request on the basis of any such exemption, this should be explained to the data subject.

Right to rectification

The right to rectification should include having inaccurate data rectified and also rights for individuals to pursue redress with the regulators and courts to rectify, block, erase or destroy inaccurate data.

Chapter 9: Individual Participation Rights - 2

(Right to object to processing, right to restrict processing, right to not be subject to automated decision-making and the right to data portability)

General Comments/ Views on this Chapter:

The right to object to processing in general, the right to object to processing for direct marketing, the right to restrict processing, the right not to be subject to automated decision-making and the right to data portability are all important and should be enshrined in a comprehensive data protection law for India.

Right to object

The right to object to the processing of personal data is a key part of data protection and must be included in a data protection law for India. We disagree with the provisional view that a general right to object to processing may not prove to be suitable for India.

The White Paper highlights the need for a practically enforceable and effective right in relation to automated decisions. It is important to be clear on what is meant by automated decisions and that the law also covers profiling. Privacy International recommends that the law should include both a right to object to profiling (see for example in Article 21 of GDPR) and a separate prohibition on being subject to certain automated decisions (see for example Article 22 of

GDPR). There must be clarity about the definitions and respective rights, if they are to be enforceable and effective,

For a discussion of the definition of profiling, the harms of profiling and rights in relation to automated decision-making and profiling in a data protection framework and how these could have been better addressed in the GDPR and accompanying guidance, please see Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR by Frederike Klatheuner and Elettra Bietti, Winchester University Press (2018).

Both profiling and automated decision-making may lead to unfair, discriminatory and biased outcomes. There is international recognition of the potential harms, in the words of the Human Rights Council:

> *"automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights." (UN General Assembly, Human Rights Council: resolution / adopted by the General Assembly, 22 March 2017, A/HRC/34/L.7/Rev.1)*

Right to object for direct marketing

The right to object to personal data being processed for direct marketing purposes should be absolute (as in Article 21(3) of GDPR). The data subject should be informed of this right and the controller obliged to cease processing their personal data as soon as this right is exercised.

Right to restrict processing

The right to restrict processing of personal data is important where the accuracy or the basis for processing personal data is contested. Data subjects must be involved and updated on this process.

Prohibition on being subject to solely automated decision-making

A data protection law for India should provide effective protections from automated decision-making and profiling, as noted above.

With regards to automated decision-making, we recommend that the Indian law should be clear that such a right constitutes a prohibition and thus protects data subjects by default. Any exemption to this prohibition should be clearly and narrowly defined. This is particularly important as automated decision-making increasingly relies on advanced and complex processing and as a result can be difficult to interpret or audit, yet can still produce decisions that are inaccurate, unfair or discriminatory.

A right not to be subject to automated decision-making should be clear that it does not only apply to decisions 'based solely' on automated processing. The law should make clear that the right cannot be avoided by fabricating human involvement. As noted by the European data protection authorities (Working Party No. 29):

"To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis they should consider all the available input and output data."

Meaningful human involvement also requires that the individual providing human oversight has a sufficient level of technical understanding, that the system used to make decisions is sufficiently interpretable, auditable and explainable, and that this involvement is demonstrated in practice, for example through documentation, including data protection impact assessments.

In developing a right (or better said a prohibition) in relation to certain automated decision-making for India, much can be learned from the debate post GDPR, as to how Article 22 can be interpreted and improved.

Right to data portability

We agree with the White Paper conclusion that it is important to include concepts of data portability in a data protection law for India in order to ensure that the data subject is placed in a central position and has a full power over his or her personal data. We welcome the conclusion that every individual should have the right to demand that all personal data about that individual that is in control of the data controller be made available to them in a universally machine-readable format or ported to another service with the specific consent of that individual.

PART IV - REGULATION AND ENFORCEMENT

Chapter 1: Enforcement Models

General Comments/ Views on this Chapter:

The White Paper envisages three different enforcement models, 'command and control' regulation, self-regulation and co-regulation. However, the White Paper does not go into detail on these three options and how they would work in practice in India. A data protection law for India should be clear and comprehensive and supplemented by statutory codes of practices and regulatory guidance. Including detailed provisions on the face of the law which will be scrutinised by Parliament is important from a democratic perspective. If Codes of Conduct, drawn up with the involvement of industry, are to be relied upon, there must be sufficient consultation and oversight.

Chapter 2: Accountability and Enforcement Tools

A. Codes of Practice
B. Personal Data Breach Notification
C. Categorisation of Data Controllers
D. Data Protection Authority

General Comments/ Views on this Chapter:

Accountability

We agree that it is imperative that the principle of accountability is reflected in the data protection law for India. Accountability should include a requirement to be responsible for and to demonstrate compliance with the other data protection principles (see for example Article 5(2) of GDPR, which provides that a controller shall be responsible for, and be able to demonstrate compliance with the data protection principles). Important organisational measures for demonstrating compliance include data protection/ privacy impact assessments, appointment of data protection officers, data protection/ privacy by design and by default requirements and record-keeping obligations. These should be set out in law and can be supplemented by Codes of Conduct/ Practice and guidance from the Independent Data Protection Authority and as relevant, sector specific guidance, developed through public consultation and collaboration with the Data Protection Authority.

A lack of organisational measures should be linked to liability for harm resulting in the processing of personal data. For example, having appropriate and adequate organisational measures in place may be a way to demonstrate that a controller or processor is not responsible for an event giving rise to damage in a compensation claim. Indemnity provisions should be avoided, and each controller or processor should be held liable for the entire damage in order to ensure effective compensation of the data subject, although provision may be made for them to claim this back from other controllers/ processors who are responsible.

Enforcement Tools

A. Codes of Practice

We agree that it is important to incorporate and make provision for codes of practice within a data protection framework. These codes of conduct or practice may be issued by a data protection authority after appropriate consultation with all relevant actors, including industry, civil society and individuals. These codes should have weight from an enforcement and liability perspective in order to ensure that they are taken seriously by controllers and processors and individuals can rely on them in exercising their rights. The various matters on which codes may be issued should be set out in the law, as should the statutory weight of the code in terms of enforcement and liability. If the data protection authority is to issue non-statutory best practice guidance, the weight of this in terms of any enforcement decision should also be made clear.

B. Personal Data Breach Notification

Personal data breaches should be notified to both the data protection authority and to the affected data subject. Mandatory breach notification is already a fixture of a number of jurisdictions, including certain states in the US, in Colombia and the Netherlands. Notification will now also be required across the EU as a result of Articles 33 and 34 of GDPR.

In defining 'Personal data breach', India may wish to look to the GDPR, which in Article 3(11) defines 'Personal data breach' as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

There should be a presumption of notification of a breach, unless specific factors are met, for example there is unlikely to be a risk to the data subject. The law should specify the time limit for breach notification to the data protection authority (for example in the GDPR it is 72 hours).

The onus should be then on the controller and the processor (who should also have notification obligations) to explain and record if and why the notification is delayed. The law should also contemplate a timescale for notification to data subjects.

The data protection authority should be provided with sufficient resources to handle breach notifications and should provide guidance on reporting and measuring risk. The law should also specify what information should be provided to the data protection authority and to the individual when notifying a breach. This should include the nature of the breach, the categories and approximate number of data subjects concerned, the categories and approximate quantity of personal data concerned, the likely consequences of the breach, and the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

It is imperative that for a breach notification to be meaningful to data subjects, the notification should be in clear and plain language and include advice and the tools to take measures to protect from harm and to seek redress from harm suffered. An individual may suffer other harms (as well as privacy harms) as a result of a data breach; therefore individuals should be notified where there is a risk to their rights and freedoms and notification should not be limited to privacy harms.

C. Categorisation of Data Controllers

Privacy International's position is that all those processing personal data (controllers and processors) should be subject to comprehensive data protection legislation. On this basis we would recommend against categorisation and towards having stronger data protection practices for all processing. Registration, data protection impact assessments, data audits and data protection officers should all be included in the law. If categorisation is to be contemplated in the law then this should consider as a minimum the scale and sensitivity of the processing, the legal basis for the processing, the intrusive nature of the processing, and its potential to prejudice the rights of individuals and cause societal harms. The categorisation should focus primarily on the nature of the processing and not the data controller; for example, the size of an organisation should not preclude them from data protection requirements, as their data processing activity may be more intensive and sensitive than a larger organisation.

D. Data Protection Authority

Whilst international data protection agreements remain largely non-prescriptive on enforcement, there continues to be two models of enforcement that have been considered - the creation of an independent supervisory authority versus ministry-based enforcement model. Certain countries, such as Canada or Germany have federal and state authorities.

Of the seven international agreements and standards relevant to data privacy, five require the establishment of an independent supervisory authority. For example, whilst the OCED Principles did not call for an independent supervisory authority, both GDPR (previously Directive 95/46) and the Convention 108 of the Council of Europe did, and 90% of countries with data protection laws have opted for this model.

Without an independent supervisory authority, there is reason to doubt the impartiality, fairness and the effectiveness of this law altogether and it may affect the confidence of the public to rely on the legal framework for protection.

Therefore, a data protection law should provide for the establishment of an independent supervisory authority to oversee the way in which a body, public or private, uses personal data. Such an authority is essential in order to ensure a uniform and effective enforcement of the data protection framework, in particular when it comes to protecting the rights of data subjects.
The mere establishment of this independent authority is not sufficient. The law must ensure the following:

Procedural and administrative provisions

· Process for appointment: The law should provide for a process and timeframe for the appointment of the authority. This procedural outline is because in many cases there has been a time-lapse between the adoption of the law and the appointment of the independent supervisory authority. In some instances, this has been prolonged for long periods of time and this situation of limbo is not desirable.
· Composition and structure: The law should identify the composition of this authority, including the skills and expertise required.
· Resources: The law must stipulate that the independent data protection authority will be given sufficient resources, both financial, technical and human.
· Independent status: The law must stipulate that the independent data protection authority should remain administratively independent, 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.

Mandate and functions

· Monitor and enforce: The authority must be given the task to monitor and enforce the application of the law. This would also require periodic review of activities of those who are subject to the law.

· Mandate to investigate: This authority must be given the mandate to conduct investigations and act on complaints by issuing binding orders and imposing penalties when it discovers an institution or other body has broken the law. This includes to be able: to demand information form the controller or processor, to conduct audits, to obtain access to all the information they may need for the purpose of the investigation, including physical access to premises or equipment used for processing, if necessary.

· Mandate to receive and respond to complaints: Both individuals and public interest/ privacy associations should be given the right to lodge complaints with this independent authority. The independent authority should also be able to receive complaints of competent organisations based on evidence revealing bad practice before a breach has occurred.

· Power to impose sanctions: The independent authority must have the power to impose appropriate penalties including fines, enforcement notices, undertakings, and prosecution. This process of sanction should not depend on submission of the complaint by a data subject but can be imposed pro-actively by the independent data protection authority.

· Mandate to provide advice: The authority should advise the government, and the relevant bodies depending on the political system (Parliamentary or Presidential), as well as other public bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regards to the processing of their personal data.

· Issuing recommendations and guidelines: Derived from its power to investigate and impose sanctions, the independent data authority should also be capable of issuing recommendations and guidelines outlining its interpretation of some provisions or aspects of a data protection law, either in general or directed to a specific sector.

· Provide information: It should be part of the work of the authority to provide information to data subjects with regards to their exercise of their rights under the law in their country or elsewhere; the latter may require liaising with foreign supervisory authorities.

· Mandate to promote public awareness: Part of the role of the authority is to promote public awareness and understanding of data subjects' rights, risks, rules and safeguards as well as resources available to them to demand and enjoy those rights, as well as risks to be conscious of when it comes to the protection of their personal data.

· Special regulatory powers: On top of that, in some cases a data protection law can give the data authority powers to regulate certain aspects of the law (i.e. update definitions, security requirements, approve transborder data flows, among others).

Chapter 3: Adjudication Process

General Comments/ Views on this Chapter:

We agree that a separate, independent body, such as a data protection authority would be the most appropriate to adjudicate on disputes arising between an individual and a data controller due to a breach of any data protection obligation. Individuals should also have access to an effective judicial remedy through the courts. The form of adjudication will depend on what is best suited to the Indian judicial and regulatory context; however, it is important that the process is independent, fair and provides meaningful redress for individuals. The issue of the expertise and understanding of the issues of those adjudicating should also be considered. Compensation claims should be permitted.

The law 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. Provisions 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 4: Remedies

A. Penalties
B. Compensation

General Comments/ Views on this Chapter:

Penalties

It is important that penalties reflect the gravity of the violation, that they have a deterrent effect and that the upper limit of penalties is clearly stipulated in the law so that controllers and

processors understand the potential financial implications of a breach. In order to achieve this deterrent effect, enforcement is key and therefore the factors that the data protection authority would take into account in imposing a monetary penalty, should also be set out in the law. The amount of the penalty should reflect the nature, gravity and duration of the infringement; the nature and scope of the processing; the categories of data; the number of individuals involved and the level of damage suffered by them; the intentional or negligent character of the infringement; any action taken to mitigate the damage suffered by individuals; and the degree of responsibility taking into account technical and organisational measures, any previous breaches and adherence to codes of conduct. A fine should be assessed on a case by case basis, considering factors such as these. The duration of the breach is just one of these factors and a pay per day model may not adequately take into account the harm that can be caused by a breach lasting just one day.

Compensation

As set out in Part IV, Chapter 3, a data protection law for India should include provisions enabling individuals to receive compensation as a result of damage and/or distress caused as a result of a data controller and/or data processor failing to comply with their data protection obligations. It is important that the law is clear that individuals are entitled to seek compensation for material and non-material damage.

As noted in Part IV, Chapter 3, comprehensive collective redress provisions for breaches of data protection law should also be included in a data protection law for India or incorporated into India's consumer protection framework. Such provisions should permit qualified not for profit organisations to pursue data protection infringements on their own accord.

There are many unlawful data protection practices that can affect hundreds of thousands of individuals and that take place under the bonnet. Often these are only revealed by independent research and investigations by civil society organisations. Examples are numerous: Privacy International has recently published a report on the use, and possible abuse, of personal data in connected rental cars; Which?, a UK consumer organisation, has carried out research on connected toys widely available in the UK that could pose child safety risks; the Norwegian Consumer Council has exposed data-related safety problems with the Cayla doll and kids' smart watches, as well as unlawful practices by health and dating apps; and a US consumer group recently exposed potential mass surveillance by digital home assistants Amazon Echo and Google Home, through studying in detail their patent applications for these devices. Such cases can be taken up on behalf of individual consumers. However, experience shows that infringing

companies and organisations will not necessarily correct their practices to cover all individuals affected, or in all countries where they trade. The empowerment of collective action would ensure corrective action by organisations processing personal information, which would benefit all those affected. It would act as a deterrent for companies, and it would save time and money for the courts.

PART V - KEY PRINCIPLES OF A DATA PROTECTION LAW

We welcome the proposed data protection principles for India to inform the development of a data protection law for India. We consider that a data protection law for India should enshrine legal principles of data protection as is common practices in international, regional and national data protection frameworks. In developing these principles for inclusion in the law, consideration should be given to other internationally recognised principles of data protection such as lawfulness; fairness; transparency; data should be adequate, relevant and limited to necessity of purpose; data should be accurate and up to date; data must be secure; individuals have the right to be involved and in control of their data; and data controllers and processors must be accountable. Some of these principles are addressed in the White Paper; however, others such as transparency, fairness and security need to be explored and articulated further.