TAKSHASHILA
INSTITUTION

POLICY ADVISORY
FEBRUARY, 2018

A DATA PROTECTION FRAMEWORK FOR INDIA

In response to the White Paper released by the Justice Srikrishna Committee

February 2018

Rahul Matthan
Manasa Venkataraman
Ajay Patri

The Takshashila Institution
Bengaluru, India

This paper can be cited as "Rahul Matthan, Manasa Venkataraman, Ajay Patri, *A Data Protection Framework for India*, Takshashila Policy Advisory, 2018-01".

Table of Contents

Executive Summary

The Justice Srikrishna Committee (formally called the Committee of Experts under the Chairmanship of Justice B N Srikrishna) is tasked with framing a robust data protection law for India. In November, 2017, the Committee released the White Paper – exploring the contours of data protection legislation across the world, and called upon stakeholders to comment on what the Indian law on this subject should contain.

For the upcoming law on data protection, it is proposed that the law should be based on these principles:

- Reducing information asymmetry between the various stakeholders in the data ecosystem by creating clear reporting and compliance frameworks;

- Ensuring that the data collecting/processing entity continues to remain accountable and does not use the user's consent as a shield against abiding by the law;

- Creating and empowering "Learned Intermediaries", or independent professional data auditors, to conduct periodic checks on the data controllers and ensure that their processes are secure and transparent; and

- Crystallising the data rights that every individual is entitled to, and outlining harms that could arise from an abuse of these rights.

The comments to the White Paper are built upon the principle that the ideal data protection law should be based on a "ConsentPlus" model. The weight of accountability of the data collecting or processing entity should be equal, if not more than that of consent. The responses to the White Paper have been built on the frameworks crystallised in a 2017 discussion document, Beyond Consent: A New Paradigm for Data Protection.[1]

Response to Part II – Scope and Exemptions

Chapter 1: Territorial and Personal Scope

1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India should be?

The Indian data protection law should protect persons resident in India from data protection violations. It should extend to protecting foreign citizens living and working in India from privacy violations but should not extend to Indian citizens who are living or working in foreign countries as they will have to subject themselves to the laws of the country in which they are currently resident. Accordingly, the data protection law should apply to the processing of data of Indian residents regardless of whether the entity processing it has a presence in India or not or whether the processing is taking place in India or not.

The mere operation of a website or other internet based application that is accessible from India, but which is not directed at Indian residents, should not require the operator of the website or application to comply with the provisions of the Indian data protection law.

This should be the sole basis for jurisdiction and therefore issues of *legitimate interest* are not relevant in this context.

2. To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

The law should be made applicable in all cases where the data being processed pertains to an Indian citizen or resident regardless of whether the entity processing the data has an Indian presence or not. However, the law should not apply to the mere operation of a website or other internet based application that is accessible from India, but which is not directed at Indian residents.

3. While providing such protection, what kind of link or parameters or business activities should be considered?

Alternatives:

a. **Cover cases where processing wholly or partly happens in India irrespective of the status of the entity.**

b. **Regulate entities which offer goods or services in India even though they may not have a presence in India (modelled on the EU GDPR).**

c. **Regulate entities that carry on business in India (modelled on Australian law), business meaning consistent and regular activity with the aim of profit.**

In order for the data protection law to apply, the processing that is carried out should be in relation to consistent and regular business activities carried out by the entity in India in furtherance of an identifiable profit motive. The business should be carried out either through a place of business in India or remotely from outside India.

The law should not compel a foreign entity to establish an Indian office as that would be too onerous and would deter businesses from extending their services to India.

4. **What measures should be incorporated in the law to ensure effective compliance by foreign entities *inter alia* when adverse orders (civil or criminal) are issued against them?**

The data protection authority should have the ability to identify and hold accountable any presence in India (a subsidiary or place of business) of a foreign entity for compliance with any adverse orders.

5. **Are there any other views on the territorial scope and extra territorial application of a data protection law in India, other than the ones considered above?**

It is important to recognise that entities operating in multiple jurisdictions already have to comply with local laws wherever they operate. In designing our data protection law to be extra-territorial in application we should remain mindful of the fact that this could result in overlaps in law that could be very difficult to properly resolve.

Chapter 2: Other Issues of Scope

1. What are your views on the issues relating to applicability of a data protection law in India in relation to: (i) natural/juristic person; (ii) public and private sector; and (iii) retrospective application of such law?

Since the right to privacy is derived from the right to life and personal liberty guaranteed by the Constitution of India, the law must apply only to data of natural persons. The principles of autonomy and dignity do not apply to juristic persons. Thus, the principles of data protection should aim to protect the individual from harm.

The data protection law should be horizontally applicable to both government/public and private sectors. However, the remedies under the data protection law for any contravention by government/public and private entities must be strictly distinguished to ensure appropriate accountability.

The retrospective applicability of the data protection law would impose significant and unwarranted challenges for entities collecting and processing data as, for instance, this would require them to seek and obtain the consent of all those from whom they have collected data prior to the coming into force of the law. This would be incredibly difficult and, in many cases, infeasible. Data collected prior to the enactment of the data protection law should not require consent to be obtained again post the enactment of the data protection law.

2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?

Alternatives:

a. The law could regulate personal data of natural persons alone.

b. The law could regulate data of natural persons and companies as in South Africa. However, this is rare as most data protection legislations protect data of natural persons alone.

The law on data protection should protect the data of natural persons only. It should not extend to the protection of information belonging to other juristic entities.

3. **Should the law be applicable to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?**

Alternatives:

a. **Have a common law imposing obligations on government and private bodies as is the case in most jurisdictions. Legitimate interests of the State can be protected through relevant exemptions and provisions.**

While the data protection law should be broadly applicable to government/public and private entities processing data equally, the law should take account the fact that, given the fundamental differences between government and private entities, it might be appropriate, in some cases to have separate and distinct remedies for violation of the principles of data protection by government/public entities on one hand and private entities on the other.

In case, for any reason, such demarcation in redressal mechanism and remedies is not possible to achieve under one data protection law, then there should be separate laws regulating government/public entities and private entities.

4. **Should the law provide protection retrospectively? If yes, what should be the extent of retrospective application? Should the law apply in respect of lawful and fair processing of data collected prior to the enactment of the law?**

Alternatives:

a. **The law should be applicable retrospectively in respect of all obligations.**

b. **The law will apply to processes such as storing, sharing, etc. irrespective of when data was collected while some requirements such as grounds of processing may be relaxed for data collected in the past.**

In general, the new law should not have retrospective applicability. Therefore, any action taken prior to the coming into force of the law should not be required to comply with the provisions of the statute.

Having said that, in certain instances a more nuanced understanding of the law's applicability will be useful. For instance:

i. For data that has already been collected after obtaining consent, there should be no further need to obtain fresh consent as in many cases this will be difficult, if not entirely infeasible;

ii. However, any collection of data after the coming into force of the law must, under all circumstances, be in conformance with the law. This includes the obtaining of consent, sharing a notice, etc.;

iii. Any terms of service already agreed to before the coming into effect of the law should be amended, as required in order to make them compliant with the law during the transition period (please refer to the response to Question 5 of this chapter). If any terms need to be changed, then the consent of the data subject will have to be obtained afresh for all such changes; and

iv. Notwithstanding any previous agreement to the contrary in the terms of service or the privacy policy, the provisions of the new data protection law that relate to retention, use, transfer, disclosure, storage, maintenance, and security of data should become applicable once the transition period elapses. Entities that collect and process data must utilise the transition period to make alterations, if required, to their internal processes to ensure their compliance with the law once it comes into force. To the extent that this requires them to obtain fresh consent, they should do so.

5. Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law?

Yes. The law could incorporate a transition period to help regulated entities make changes to their processes to ensure compliance with the new law. Depending on the complexity of the transition particularly if new concepts of data protection are introduced into the Indian law, adequate time should be provided to complete this transition effectively.

6. Are there any other views relating to the above concepts?

[●]

Chapter 3: What is Personal Data?

1. What are your views on the contours of the definition of personal data or information?

The reason why data protection laws around the world have a definition of personal data is so that their provisions apply only to that category of data that is capable of identifying a person. This approach is based on the understanding that data, once categorised as such, is immutable. Accordingly, the law does not apply to non-personal data and allows this sort of data to be collected without any constraints of notice, consent, or any other provisions that apply to personal data.

Today, data is no longer immutable. When non-personal data is added to other non-personal data that has already been collected, it could, as a result of such combination, be transformed into personal data. Often, this transformation takes place as a result of the application of algorithms or other additional processes but for which the data would have remained non-personal. For these reasons, we believe that classification of data into personal data is no longer relevant.

Some data protection laws try to bypass this issue by defining personal data as data that is capable of identifying a person either by itself or in combination with other data already in control of the data controller. However, even this formulation is difficult, maybe impossible, to police in the context of current technologies.

The principal purpose of these classifications is to limit the requirement to comply with the provisions of data protection law to only that data which is personal data. This primarily refers to the obligation to obtain prior consent. Without such a classification, the data controller would be obliged to collect consent every time it collects any data. This classification attempts to limit the amount of times consent is sought.

We have proposed an accountability model for data protection, the details of which are set out later in our responses to this White Paper, that does not depend on the procurement of consent. Under this model, the data controller is

made liable for the harm it causes to the privacy of the data subject and the law does not allow the consent that has been provided by the data subject to dilute the responsibility of the data controller for the harm it has caused. Accordingly, we believe that classification of data as non-personal should not be allowed to dilute the liability of the data controller for the harm caused simply because at the time of collection, the data could not be classified as personal data.

Regardless of whether or not the Committee accepts the proposed Accountability Model, we would urge the Committee to be mindful of the consequences of such classification. Given the nature of data in the modern world, the law should not absolve the data controller of liability if the data collected was not personal at the time of collection. Instead, the law should impose a strict obligation on the data controller to monitor all data under its control (including data that is not ordinarily considered to be personal) to ensure that no harm comes to any data subject as a consequence of its use.

2. **For the purpose of a data protection law, should the term 'personal data' or 'personal information' be used?**

Alternatives:

a. **The SPDI Rules use the term sensitive personal information or data.**

b. **Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.**

Please see our comments on the need for such a classification and the consequences in context of the transmutable properties of modern data. Should the Committee still believe that such a classification is necessary, we would urge the Committee to ensure consistency in the use of terminology. Given this, *personal information* or *personal data* can be defined to mean the same thing and then used consistently. On a practical note, it is preferable to use *personal data*, to ensure parity with the terminology used in other jurisdictions.

3. **What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?**

Please see our comments on the need for such a classification and the consequences in the context of the transmutable properties of modern data. Should the Committee still believe that such a classification is necessary, we believe that personal data must be about, or relate to, a natural person in order to be considered within the purview of data protection law.

Personal data should include facts, opinions, and assessments, irrespective of their accuracy. However, there should be differences in the participation rights that individuals are entitled to with regard to these different types of personal data.

4. Should the definition of personal data focus on identifiability of an individual? If yes, should it be limited to an 'identified', 'identifiable' or 'reasonably identifiable' individual?

Please see our comments on the need for such a classification and the consequences in the context of the transmutable properties of modern data. Should the Committee still believe that such a classification is necessary, we believe that the Committee should acknowledge that there should be two broad categories of data: identified and identifiable. The classification is set out in more detail below:

Scope:

i. For Identified Data: Includes data that has been collected directly from an individual at the time of enrolment of that individual to the service provided by the data controller.

ii. For Identifiable (i.e., non-identified data): Includes the following: data that is collected in the course of the data subject's use of the service, or from ambient conditions such as through sensors and Internet of Things devices, data in the aggregate, de-identified data sets, ambient data (such as, a car registration number)

Governance Mechanism:

i. For Identified Data: Where data is collected at the time of signing up to services, we believe that the data subject can be provided notice of the

purpose to which such data will be put and be asked to consent to such collection and use;

ii. For Non-Identified/Identifiable Data: Where data is collected in the course of the data subject's use of the service, or from ambient conditions, we believe that notice and consent will not be practical and that the principle of accountability should be applied (please refer to the chapter on Accountability for more details).

Individual Participation Rights

i. For Identified Data: The full range of these rights will be available to an individual; and

ii. For Non-Identified / Identifiable Data: Individuals will have a limited set of participation rights, in which rights to consent, notice, access, rectification, etc., will not be available.

	Identified Data	**Identifiable Data (Non-identified Data)**
Scope	Includes data that has been collected directly from an individual at the time of enrolment of that individual to the service provided by the data controller.	Includes the following: data that is collected in the course of the data subject's use of the service, or from ambient conditions such as through sensors and Internet of Things devices, data in the aggregate, de-identified data sets, ambient data (such as, a car registration number).
Governance mechanism	Where data is collected at the time of signing up to a service, we believe that the data subject can be provided notice of the purpose to which such data will be put	Where data is collected in the course of the data subject's use of the service, or from ambient conditions, we believe that notice and consent will not be practical and that the principle of accountability should be applied

	and be asked to consent to such collection and use.	(please refer to the chapter on Accountability for more details).
Individual participation rights	The full range of these rights will be available to an individual.	Individuals will have a limited set of participation rights, in which rights to consent, notice, access, rectification, etc., will not be available.

5. Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymisation or psuedonymisation, for instance as the EU GDPR does?

[Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymised data falls outside the scope of personal data in most data protection laws while psuedonymised data continues to be personal data. The EU GDPR actively recommends psuedonymisation of data.]

In general, the data protection law should encourage data controllers to modify their use of data so that, as far as possible, they limit their use to data that does not relate to specific individuals.

The terms anonymisation and pseudonymisation both imply the application of certain specific techniques and processes to rid the underlying data of certain elements that identify such data as relating to a given data subject. In the spirit of creating a technology neutral law, we would recommend the use of the term *de-identification* as a technology neutral representation of the principle set out above. The law should encourage the use of de-identified data sets. This would refer to data sets that have been subjected to a process by which any characteristics that lead to identification of the individual in question have been removed or disguised.

It must be noted that anonymisation techniques are not fool-proof. In the deliberations leading up to the GDPR in the EU, the Article 29 Data Protection Working Party expressed reservations about the effectiveness of anonymisation

techniques to protect individuals.[2] Accordingly, the law should encourage data controllers to find ways to appropriately de-identify the data in their control without specifying the processes or techniques by which they should do it. Given that technology evolves rapidly and that data controllers who are much more familiar with the nature of the data under their control and the tools to de-identify them, the law should not attempt to be prescriptive.

The law should also consider imposing restrictions on re-identification or attempts to re-identify data sets that have gone through a process of de-identification. This would ensure that entities collecting and processing data do not resort to de-identification as a mere means of reducing the participation rights available to individuals.

6. **Should there be a differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonably identifiable? What would be the standards of determining whether a person may or may not be identified on the basis of certain data?**

Yes. The differentiated level of protection can be seen in the response to Question 4 of this chapter, where different sets of data rights are available to individuals depending on whether the data set in question is identified or identifiable.

We have recommended the application of the accountability principle in the case of identifiable data. There would be no additional need to define standards.

7. **Are there any other views on the scope of the terms 'personal data' and 'personal information', which have not been considered?**

[•]

Chapter 4: Sensitive Personal Data

1. What are your views on sensitive personal data?

As discussed earlier, we believe that the classification of data should not be allowed to dilute the liability of the data controller for harm. That said, there are certain types of personal data that should be accorded a higher level of protection under the law. Sensitive Personal Data refers to identifiable personal data of a sensitive nature. Data controllers should be additionally careful when the data they deal with is sensitive as the disclosure of such sensitive personal data could result in substantial harm, embarrassment, inconvenience, or discrimination to an individual.

2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? E.g. Financial Information/Health Information/Caste/Religion/Sexual Orientation. Should any other category be included?

[For instance, the EU GDPR incorporates racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.]

Yes. It is useful to define a category of information as sensitive personal data (SPD) and accord it with a higher degree of protection. The nature of this protection will be discussed in greater detail in the responses to Part III, Chapter 6 of the White Paper.

The categories of data that could be included within the scope of SPD are set out below, though it must be noted that the determination of whether a particular type of data qualifies as SPD is often dependent on the context. Illustrative examples of this are also set out below:

i. <u>Passwords along with associated user name and the service that they can be used to access.</u>

While the characters that comprise a password may be generic in nature, combining or linking them with other information, such as an email address, a bank account number, a user name, credit card details, etc., could turn them into SPD.

ii. Personal Financial information

Certain information about a person's finances, such as, the net worth of an individual or the debt status, could be deeply sensitive and therefore also qualify as SPD.

iii. Health information

Certain types of health information that discloses health conditions that could affect the reputation or the prospects of the data subject could be considered to be SPD.

iv. Sexual orientation

Similar to the case of health information, information related to an individual's sexual orientation that could lead to stigmatisation should fall within the ambit of SPD.

v. Biometric information, including genetic information

Biometric information collected with the intent of identifying a person should be considered to be SPD. For instance, a recording made by a CCTV camera that can clearly identify an individual would constitute biometric information but if it has not been recorded with the express purpose of identifying a person, it may not constitute SPD.

3. Are there any other views on sensitive personal data which have not been considered above?

[●]

Chapter 5: What is Processing?

a. What are your views on the nature and scope of data processing activities?

Most data protection laws attempt to define processing in order to specify the differing obligations that apply to entities that carry out differential types of processing. Thus, entities involved in collecting personal data might be obliged to collect consent while those that are only involved in other forms of processing that do not involve collection, do not.

As discussed earlier, we propose an Accountability Model under which the data controller will be held liable for all harm caused to the data subject as a consequence of their processing of the personal data. Under this model, the obligation to obtain consent applies only to those controllers who collect identified data from the data subject and hence, the requirements of notice and consent will be inherent in the nature of data collected. Accordingly, since this model already has a mechanism by which the data controller is required to obtain consent for collection, it is our view that the privacy law does not need to separately specify detailed regulations based on processing.

b. Should the definition of processing list only main operations of processing i.e. collection, use and disclosure of data, and inclusively cover all possible operations on data?

As mentioned above, there would be no need to specifically list out a definition for processing as, under the Accountability Model, the data controller will be liable for any type of processing that results in harm being caused to the data subject. That being the case, listing only some types of processing will limit the scope of the definition. Instead, processing should be given a descriptive definition that covers most of the existing operations that apply to personal data. This definition should also be broadly framed to ensure that new operations in the future can also be included with its ambit.

c. Should the scope of the law include both automated and manual processing? Should the law apply to manual processing only when such data is intended to be stored in a filing system or in some similar structured format?

Alternatives:

a. All personal data processed must be included, howsoever it may be processed.

b. If data is collected manually, only filing systems should be covered as the risk of profiling is lower in other cases.

c. Limit the scope to automated or digital records only.

Yes. The scope of the law should include both automated and manual processing. However, with regard to automated processing, the law should recognise that modern machine learning and black box algorithms are complex and it is often impossible to ascertain their logic. Accordingly, the law should take into account the need to implement alternative measures for the regulation of automated processing in the current context of big data. In particular, the law should not include obligations such as the obligation to provide the logic for automated decisions as is found in many data protection laws as this may not be feasible in the context of black box algorithms.

d. Are there any other issues relating to the processing of personal data which have not been considered?

[•]

Chapter 6: Entities to be Defined in the Law: Data Controller and Processor

1. **What are your views on the obligations to be placed on various entities within the data ecosystem?**

   We believe that the primary liability for compliance with the data protection law should fall on the data controller. If that data controller outsources any processing or any part thereof to a third-party processor under a data processing agreement, the data controller should ensure that such outsourced entity complies with the applicable data protection obligations or indemnifies the data controller for any harms that result as a consequence. For this purpose, the contract may also stipulate that appropriate indemnity clauses be included in the agreements between the data controller and the data processor

2. **Should the law only define 'data controller' or should it additionally define 'data processor'?**

   Alternatives:

   a. **Do not use the concept of data controller/processor; all entities falling within the ambit of the law are equally accountable.**

   b. **Use the concept of 'data controller' (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it.**

   c. **Use the two concepts of 'data controller' and 'data processor' (entity that receives information) to distribute primary and secondary responsibility for privacy.**

   It is sufficient for the law to define a data controller as an entity that collects and processes data. There is no need to have a distinction between a data controller and a data processor.

3. **How should responsibility among different entities involved in the processing of data be distributed?**

   Alternatives:

a. **Making data controllers key owners and making them accountable.**

b. **Clear bifurcation of roles and associated expectations from various entities.**

c. **Defining liability conditions for primary and secondary owners of personal data.**

d. **Dictating terms/clauses for data protection in the contracts signed between them.**

e. **Use of contractual law for providing protection to data subject from data processor.**

The responsibilities that any entity will have under the law will be dependent on the context in which it handles data.

For instance, as seen in the response to Question 4 of Chapter 3 of this White Paper, identified data is collected directly from an individual. In such cases, the data controller will be responsible for complying with consent and notice requirements under law. However, if a data controller is only engaged in processing data that has been collected by a different entity or that can be classified as identifiable data, then such a data controller will not be required to seek consent and provide a notice under law.

Under such circumstances, where processing has been outsourced, the data controller could use contractual protections to adequately safeguard the interests of the data subject. This would involve the use of appropriate indemnity clauses for non-compliance by the entity carrying out the outsourcing.

4. **Are there any other views on data controllers or processors which have not been considered above?**

[●]

Chapter 7: Exemptions for Household Purposes, Journalistic and Literary Purposes and Research

1. **What are the categories of exemptions that can be incorporated in the data protection law?**

   As a general rule, there should be no exemptions from the applicability of the data protection law. Any exemption granted must be circumscribed by a stated purpose, which should be as narrowly construed as possible.

2. **What are the basic security safeguards/organisational measures which should be prescribed when processing is carried out on an exempted ground, if any?**

   With the exception of household data, there should be no absolute exemption from compliance with all the obligations under the law. Instead, exemptions should only be offered with regard to compliance with certain aspects of the data protection law while ensuring that as far as possible, the data controller continues to be bound by the rest of the data protection obligations. For example, while law enforcement agencies may be granted an exemption from collecting consent during the course of the investigation of a crime, they should continue to be obliged to ensure that any data so collected is kept secure and not transferred or disclosed.

Domestic /Household Processing

1. **What are your views on including domestic/household processing as an exemption?**

   An exemption from the obligations under the law could be extended with regard to domestic and household processing.

2. **What are the scope of activities that will be included under this exemption?**

   Domestic/household processing must be provided the widest possible exemption under the law. These activities can be best described as non-commercial social activities conducted by individuals in their personal capacity. This would include the publication of content on personal blogs and one's social media profile.

This exemption would exclude activities that are being undertaken for professional or commercial reasons. For instance, a medical professional in possession of the data belonging to his patients will not be covered by this exemption.

It must be noted that individuals handling data belonging to other persons for domestic/household processing can still be liable for tortuous claims and potential criminal charges under other laws of the country.

3. Can terms such as 'domestic' or 'household purpose' be defined?

Please refer to the response to Question 2 above.

4. Are there any other views on this exemption?

[•]

Journalistic/Artistic/Literary Purpose

1. What are your views on including journalistic/artistic/literary purpose as an exemption?

Yes. There should be a limited exemption for journalistic purpose on the condition that only the obligations with regard to consent, notice, and choice be exempted.

2. Should exemptions for journalistic purpose be included? If so, what should be their scope?

Yes. There should be a limited exemption for journalistic purpose on the condition that only the obligations with regard to consent, notice, and choice be exempted.

The primary scope of journalistic activities would be the use of personal data for *publication*, which in itself can be interpreted broadly. In addition, to determine the extent of the exemption, the guidelines in use in the UK are instructive.[3] They permit the exemption subject to following:

i. The purpose of publication must have an element of fairness to it, as well as be guided by public interest;

ii. Adequate steps must be taken to protect the data; and

iii. The exemption should not be applicable in cases where the data is obtained from an entity in possession of the data without such entity's consent.

3. Can terms such as 'journalist' and 'journalistic purpose' be defined?

In order to identify who a journalist is, a journalistic purpose may be defined and the definition of a journalist may be tied into this. Some of the tests that have been applied include:

i. Is what the individual publishes newsworthy and of public interest?[4]

ii. Is there some degree of editorial oversight that ensures accountability?[5]

iii. Is the individual engaged in regularly gathering news and is their intention to publish news?[6]

A combination of these factors would help identify if an individual is engaged in a journalistic purpose. Care must be taken to exclude blogs, social media and other forms of internet publication that are not governed by the ethical standards that apply to traditional journalism from the scope of the journalistic exemption.

4. Would these activities also include publishing of information by non-media organisations?

No. Any publication of information by non-media organisations should not be covered under this exemption. Conventional forms of journalism are also subject to their own code of ethics, while publications by non-media organisations are not. This distinguishing factor should help govern the applicability of the exemption.

5. What would be the scope of activities included for 'literary' or 'artistic' purpose? Should the terms be defined broadly?

Granting specific exemptions may not be necessary with respect to “literary” or “artistic” works.

6. Are there any other views on this exemption?

[●]

Research/Historical/Statistical Purpose

1. **What are your views on including research/historical/statistical purpose as an exemption?**

   As mentioned in our response to Question 1 above, a limited exemption for this purpose could be provided such that the requirement for consent, notice, and choice may be exempted.

2. **Can there be measures incorporated in the law to exclude activities under this head which are not being conducted for a bonafide purpose?**

   We believe that the accountability principle could be applied to the processing of data under this exemption to ensure that any processing that is carried out on a *mala fide* basis by seeking to avail of this exemption is nevertheless caught under the provisions of the law.

3. **Will the exemption fail to operate if the research conducted in these areas is subsequently published or used for a commercial purpose?**

   Any data that is sought to be utilised for research/statistical/historical purposes must be processed in a de-identified form. Any re-identification or attempt to re-identify such data will make this exemption inapplicable.

   Further, the publication of any results from the processing of such data should also be in a de-identified form, or as an aggregate. Any attempt to use these results to target individuals for commercial gain would make the exemption inapplicable.

4. **Are there any other views on this exemption?**

   [•]

Investigation and Detection of Crime, National Security

1. **What are your views on including investigation and detection of crimes and national security as exemptions?**

   As mentioned above, while it might be necessary to provide an exemption to the consent, notice, and choice requirements for the collection and processing of information in the interests of national security, investigation, and detection of

crimes, law enforcement agencies should continue to be responsible for the security of the information they collect and be subject to all the other principles of data minimisation and purpose limitation. While there is a clear State interest in allowing for an exemption, the sensitivity of the information involved in these matters and the corresponding harm that may be caused to data subjects as a result of this would necessitate a countervailing check on unnecessary processing.

Further, any entity claiming this exemption should be able to demonstrate the need for the exemption in order to fulfil its functions.

2. What should be the width of the exemption provided for investigation and detection of crime? Should there be a prior judicial approval mechanism before invoking such a clause?

The relevant authority can be exempt from obtaining consent under this exemption category. However, the boundaries of this exemption should be circumscribed by purpose limitation and law enforcement agencies should be held accountable for the consequences of their processing. In the case of mass surveillance and other measures that could potentially have widespread consequences, it might be advisable to put in place a mechanism whereby prior judicial approval must be obtained before invoking such a measure. All the other protections provided for under the data protection law will continue to apply. Further, the scope of the exemption should be proportionate to the amount of information needed to adequately investigate or detect a crime.

3. What constitutes a reasonable exemption on the basis of national security? Should other related grounds such as maintenance of public order or security of State be also grounds for exemptions under the law?

Any exemption from the data protection law for matters of national security, including the maintenance of public order, must be approved by a designated body. This authority must have judicial representation on it in order to ensure that the proper checks and balances are in place. As the White Paper mentions, this could be similar to the FISA courts established in the USA.

4. Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail?

Yes, a review mechanism is necessary. The review mechanism must entail a process by which the Data Protection Authority has the authority to review the manner in which this exemption was availed to assess whether the invocation of the exemption was in fact necessary in the national interest. This review must be periodic and must occur at a frequency that is commensurate with the national security interest being used to justify the exemption and the nature of information involved. An effective review mechanism must look at the following:

i. Whether a proper claim of invoking the exemption was made at the time of collection of data.

ii. Whether the stated purpose for which the exemption was invoked was achieved.

iii. Whether the data collected was utilised for any purpose other than the one initially claimed.

In addition, the review mechanism must evaluate whether the exemptions granted under this category were granted for a limited period of time and if in fact that time period was honoured. If an entity requires a continuation of the exemption, it must approach the relevant authority for an extension of the time period for the exemption. The review mechanism should, in particular, operate to prevent undue and unnecessary extensions of the exemption.

5. How can the enforcement mechanisms under the proposed law monitor/control processing of personal data under this exemption?

A robust review mechanism as outlined in the response to Question 4 above, in addition to the principle of accountability, will be sufficient in ensuring that this exemption is not misused. A monitoring mechanism that engages in real time oversight might be too onerous to implement in practice.

6. Do we need to define obligations of law enforcement agencies to protect personal data in their possession?

The law enforcement agencies can only utilise the personal data in their possession to the extent that the designated authority has permitted the exemption. Any activity beyond the permitted exemption should open them up

for liability under the data protection law (please refer to the chapter on remedies).

7. Can the Data Protection Authority or/and a third-party challenge processing covered under this exemption?

As mentioned above, the Data Protection Authority should be granted the right to review the processing of data under this exemption. Third parties should be allowed to object to the Data Protection Authority with regard to such processing.

8. What other measures can be taken in order to ensure that this exemption is used for bona fide purposes?

An effective review mechanism, coupled with stringent penalties, can be sufficient to ensure that the exemption is only claimed for *bona fide* purposes. Please refer to the earlier responses in this chapter and the chapter on remedies.

9. Are there any other views on these exemptions?

[●]

Additional Exemptions

1. Should 'prevention of crime' be separately included as a ground for exemption?

Yes. A separate exemption for the 'prevention of crime' can be included within the law. The same standards as mentioned above, for investigation and detection of crimes, and national security, will apply in this case as well. Therefore, the exemption will be from the obtaining of consent, whereas all other protections under law will continue to remain applicable.

2. Should a separate exemption for assessment and collection of tax in accordance with the relevant statutes be included?

The avoidance of taxes is a crime and statutory exemptions exist under other legislations that permit the relevant authorities to conduct their investigations for assessment and collection of tax. There is no need to specify a separate exemption for this category under the data protection law.

3. Are there any other categories of information which should be exempt from the ambit of a data protection law?

Yes, there are additional grounds under which an exemption may be granted to the notice and choice requirement under the data protection law:

i. The processing of information that is necessary to comply with the order of a court, tribunal, or other statutory authority;

ii. An exemption for the processing of data for a purpose such that there may arise a grave threat to another individual's life if this processing activity of the controller is not carried out;

iii. An exemption for processing necessary for fraud prevention, due diligence to fight bribery, and anti-money laundering activities. Since India has global commitments towards thwarting terrorist financing, controlling money laundering, and eliminating bribery, it is important to ensure that Indian privacy rules do not directly conflict with these obligations.

Chapter 8: Cross-Border Flow of Data

1. What are your views on cross-border transfer of data?

Strict rules that limit cross-border transfers, particularly those based on jurisdiction by jurisdiction adequacy determinations, do not reflect the reality of global information flows. Today data moves across multiple paths -- intranets, emails, by virtue of access to centralised databases -- to company personnel around the world. For this reason, it makes no sense distinguishing between data flows within and outside the country. On the contrary it would be far more effective for organisations to implement consistent privacy policies across a region and the world.

A better approach would be to require organisations to remain accountable for the transfer of all personal information under their control, whether they are transferring such information domestically or across international borders. Such organisational accountability can be achieved through the use of codes of conduct, internal policies, procedures regarding handling of personal information, or contractual arrangements.

The law should recognise instances where such accountability may not be possible or practical. For example, where a disclosure is required by law, this sort of accountability will not be possible and the organisation should be relieved of its accountability obligations. Additionally, where the organisation determines that it cannot ensure that the recipient will protect the information appropriately, it should be possible to rely on consent for such third-party disclosures. For example, when an organisation forwards information to the immigration authorities so that a potential employee can be granted a work visa, accountability is not possible or impractical because there is no on-going relationship between the organisation and the third-party recipient. In such circumstances it should be possible to rely on consent.

2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, what should the adequacy standard be the threshold test for transfer of data?

Making the adequacy test the threshold test for the transfer of data may hinder free movement of data as the Data Protection Authority may not have arrived at a decision about the level of data protection in all countries to which the data might need to be transferred. As an alternative, the data protection framework may mandate the use of contractual provisions to ensure appropriate protection.

3. **Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfils the test for transfer?**

Restrictions on the transfer of data outside the country should be limited to information that is sensitive from a national security perspective. All other information transfers should be permissible with restrictions. Depending on the nature of the information, certain sensitive information may be required to be stored within the country. Such restriction may be mandated by sectoral regulators in the Code of Conduct formulated by them (e.g. Reserve Bank of India, Department of Telecommunication, etc.).

4. **Are there any other views on cross-border data transfer which have not been considered?**

[●]

Chapter 9: Data Localisation

1. What are your views on data localisation?

The primary reasons for seeking to incorporate data localisation measures seem to be:

i. To prevent foreign agencies from controlling the data belonging to Indians;

ii. To aid local law enforcement authorities by making it easier to have access to data;

iii. For the protection of the rights of data subjects.

Introducing regulations that require data localisation would significantly increase costs for Indian businesses since they would no longer be able to rely on economies of scale for data storage at global data centres. This would have the effect of making services more expensive for customers. Several studies indicate that data localisation also adversely affects the GDP of the country. In addition, allowing companies to store data centrally typically results in better and stronger protection than if data was required to be stored locally.

While localising data in India would ensure that it remains outside the reach of foreign governments, doing so will create barriers against transfer of data over the internet. This would have a negative impact on businesses that rely on cross-border transfer of data for providing services to customers in India and disrupt the provision of such services.

There is a compelling case to be made that access to an individual's data should not, in fact, be too easy for the State. Knowing that the State has ready access to one's data can create a chilling effect amongst individuals. This goes against the spirit of freedom of speech and expression embodied in the Constitution. Further, data localisation could be the beginning of a slippery slope towards more transparency over an individual's data. It could conceivably pave the way for calls to prohibit end-to-end encryption, which will jeopardise privacy even more.

Therefore, given the law will have limited exemptions for the State for compliance with the data protection law (please refer to the responses under Chapter 7 of this White Paper), the inclusion of data localisation for the reasons outlined above will be an excessive measure.

The inclusion of a right to data portability will, to a large extent, allay the concerns around data being taken out of the country forever. Once individuals are empowered with such a right, they will have the ability to retrieve their data from a data controller, even if such data is being stored or processed outside the territory of India. Not only does this lower the need for data localisation, it also bolsters the autonomy of individuals.

2. Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?

No. The data protection law should not have any general requirement around data localisation.

The need for such an exception can be examined for individual sectors on a case by case basis. If data localisation is desired for effective regulation of a particular sector, it can then be implemented for such limited purposes. This should typically relate to certain types of sensitive personal data.

For instance, there could be a stipulation that biological samples, such as, tissue, blood, and genetic samples, be stored on Indian territory only. It must be noted that this restriction should ideally apply to the physical samples themselves, and not necessarily to the information gleaned from them. Similarly, for reasons of security, certain data belonging to members of the armed personnel could be prevented from being transferred outside the country.

3. If yes, what should be the scope of the localisation mandate? Should it include all personal information or only sensitive personal information?

As mentioned in the previous response, any limited data localisation mandate should focus on certain types of sensitive personal data. The mandate itself must be determined on a case by case basis.

4. If the data protection law calls for localisation, what would be the impact on industry and other sectors?

The White Paper has addressed this question comprehensively. There will be economic repercussions to data localisation. This can be seen in the form of increased costs to do business, barriers to benefitting from global networks, and a negative impact on the start-up ecosystem, which will find it difficult to scale up quickly. The development of technologies such as Internet of Things, artificial intelligence, and machine learning would also be hindered since cloud computing and seamless data transfer are necessary for such technologies to operate. It will also affect start-ups and innovative new businesses from taking off as it would increase their cost of operations.

5. Are there any other issues or concerns regarding data localisation which have not been considered above?

[●]

Chapter 10: Allied Laws

Insurance Related Laws

The White Paper highlights the insurance sector, and the laws governing it in India, as one of the areas where the impact of the data protection law must be examined closely. One of the instances which merits greater scrutiny is the manner in which genetic information is treated in the insurance sector. More specifically, the use of genetic information to classify certain health conditions as pre-existing, and thereby excluding or restricting insurance coverage, is a cause for concern. This would amount to discrimination on the basis of one's genetic information, and consequently a violation of an individual's rights under the data protection law.

It would be prudent to adopt a stance similar to the one seen in the USA, where The Genetic Information Non-discrimination Act of 2008 (GINA) prohibits discrimination in the provision of health insurance on the basis of an individual's genetic information.

The Information Technology Act, 2000 (the IT Act) and Related Rules

The White Paper mentions the IT Act and the related rules as one of the allied laws that will need to be re-examined in the light of a new law on data protection. It is important that the provisions relating to data protection and privacy in these laws be repealed since they cannot co-exist with the framework that the new law will introduce.

Response to Part III - Grounds of Processing, Obligation on Entities and Individual Rights

Chapter 1: Consent

1. What are your views on relying on consent as a primary ground for processing Personal Data?

Alternatives:

a. Consent will be the primary ground for processing.

b. Consent will be treated at par with other grounds for processing.

c. Consent may not be a ground for processing.

The trend in data protection laws around the world, as evidenced by the GDPR provisions, is to move away from relying on consent as the primary legal basis for processing. Jurisdictions have concluded that relying on consent results in individuals experiencing consent fatigue (i.e., individuals simply click yes without reading the underlying information) and adds a substantial burden on organisations. Apart from the Ukraine, Russia, Colombia, and South Korea, which rely on consent as the **only** legal basis for processing, most countries around the world provide for a variety of legal bases for processing.

Thus, over-reliance on consent creates unnecessary burden on organisations and individuals without adding privacy protections. There are also a number of cases, such as in the employment context, where it may not be possible for an individual to give consent freely because of the imbalance of power between the employer and employees (or job applicants).

In Europe, it will soon be possible for Personal Data to be collected, used, and disclosed/ transferred to fulfil obligations under a legal relationship between the Data Controller and the individual and where required by law. Personal Data will be allowed to be collected, used, and disclosed/transferred where necessary for the purposes of legitimate interests pursued by the Controller or by a third party such as in order to provide a service to the data subject; where reasonably necessary for the purpose of managing or terminating an employment relationship; where required for internal administrative purposes; where

necessary and proportionate for the purposes of ensuring network and information security; and where necessary for the purposes of fraud prevention, due diligence to fight bribery, and anti-money laundering activities.

Given that the world is turning away from consent as the primary grounds for processing, it would be appropriate not to apply consent as the primary ground for processing in India. This is particularly relevant given the fact that India does not have a culture of privacy and is only just realising the implications of requiring a formal data protection law. Accordingly, we propose that the Indian data protection law rely on accountability as the primary means of securing personal privacy.

Under the accountability model, the data controller will be able to collect and process personal data wherever necessary for the purposes of the legitimate interests of the Data Controller but under all such circumstances, shall be accountable for all harms that will be caused to the data subject as a consequence.

Accordingly, we believe that consent should not be the primary ground for processing.

2. **What should be the conditions for valid consent? Should specific requirements such as 'unambiguous', 'freely given' etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?**

Where consent is used as a ground for processing, it should be provided with full knowledge of the consequences and should be provided voluntarily. However, any such consent should be capable of being expressed in different ways, such as, by providing implicit or explicit consent or authorisation. Implicit consent is expressed through actions rather than words of the individual. For example, the act of handing over a business card indicates that the recipient would be entitled to use the personal information found on the card to initiate future contacts.

There are other contexts where consent is hard or impossible to provide. In the context of mergers and acquisitions, for example, it might be required, as part of the due diligence process, to share personal information with prospective acquirers of company assets who need to review such information before

agreeing to acquire the company. Disclosing details of the proposed transaction to employees or customers raises the risk of "insider trading" and puts the deal in jeopardy. It would therefore be unworkable, and in many cases illegal, to provide sufficient information regarding potential transactions to individual employees and customers such that they can provide informed consent.

Such circumstances would be covered by the accountability model where the data can be shared, provided that the data controller is held liable for the consequences of its actions and, in particular, any harm that are caused as a result of sharing such personal data.

3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?

As discussed above, the accountability model does not depend on consent and accordingly, will avoid consent fatigue that results from a multiplicity of notices. However, it deprives the data subject of necessary autonomy and agency in determining the bounds of his privacy.

A technology driven granular opt-out model will restore that agency and ensure that users have the necessary autonomy to opt out from the collection and processing of specific types of personal data. Thus, while data controllers might not be able to collect prior consent, it should be possible to design privacy settings to allow data subjects to opt out after the collection of data at some later point in time.

4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?

As discussed above, the accountability model does not depend on consent and accordingly, will not require consent to be set out based on different standards or contexts. That said, the law should allow consent can be expressed in different ways - both implicit and explicit – as well as through authorisation.

5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?

Yes, stringent conditions for obtaining consent would be detrimental to day-to day business. Detailed notices, along with the requirement to obtain consent for

various types of data processing, can be extremely costly to implement. We believe that this is largely mitigated by the framework that we proposed in our response to Question 1 in this Chapter.

6. **Are there any other views regarding consent which have not been explored above?**

[●]

Chapter 2: Child's Consent

1. **What are your views regarding the protection of a child's personal data?**

We agree, as stated in the White Paper, that children are a vulnerable class of data subjects. Accordingly, we think the following approach must be adopted with respect to the processing of their data:

i. Sensitive Personal Data and Identified Personal Data of children below 14: There must be an absolute prohibition on the processing of Sensitive Personal Data of all children who have not attained the age of 14. While this age limit is a line in the sand at the moment, there is at least one other jurisdiction that recognises that the processing of data of children below a certain age may be harmful.

ii. Sensitive Personal Data and Identified Personal Data of children above 14, and Identifiable Personal Data: For both classes of data, explicit parental consent must be the foundation for processing. While this is difficult to implement, the harms that it seeks to prevent cannot be negated. This must also be subject to a strict negative list of purpose limitation that must be identified by the government from time to time. Under all circumstances, the data controller must be accountable for the harm caused to children as a consequence of their processing of the data.

2. **Should the data protection law have a provision specifically tailored towards protecting children's personal data?**

Yes, the data protection law must have a specific provision in order to be able to operationalise our answer in Question 1 above.

3. **Should the law prescribe a certain age-bar, above which a child is considered to be capable of providing valid consent? If so, what would the cut-off age be?**

Yes, however, this must tie into the age of majority.

4. **Should the data protection law follow the South African approach and prohibit the processing of any personal data relating to a child, as long as she is below the age of 18, subject to narrow exceptions?**

No. While in general, processing of personal information pertaining to children must not be allowed, there are a number of industries that process the information of children during the ordinary course that would not be able to survive without such processing, and would also need some workable exceptions to ensure that their processing of information is not overly onerous. For instance, schools, paediatric hospitals, sports training facilities, and other such service providers deal with children and regularly process their data. The law should not make the use by children of these facilities too much of an onerous burden. That said, strict regulations should be placed on ensuring that these industries take adequate care to ensure that no harm befalls any children as a result of the manner in which they process and store such data.

5. **Should the data protection law follow the Australian approach, and the data controller be given the responsibility to determine whether the individual has the capacity to provide consent, on a case by case basis? Would this requirement be too onerous on the data controller? Would relying on the data controller to make this judgment sufficiently protect the child from the harm that could come from improper processing?**

No. This would be onerous on the data controller and inappropriate in the Indian context given the diversity of the country and the size of its population and geographical size.

6. **If a subjective test is used in determining whether a child is capable of providing valid consent, who would be responsible for conducting this test?**

Alternatives:

a. The data protection authority

b. The entity which collects the information

c. This can be obviated by seeking parental consent

We do not believe that a subjective test is the best approach for this.

7. **How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required?**

Short of extremely onerous measures such as physical verification or time-stamped video recordings of consent, we are not aware of any other reliable ways in which a data controller may be certain that they have obtained consent from the parents of the child.

8. **Would a purpose-based restriction on the collection of personal data of a child be effective? For example, forbidding the collection of children's data for marketing, advertising and tracking purposes?**

Yes, a purpose-based restriction on the processing of children's data would greatly help mitigate the risk that it might be processed for purposes detrimental to the interests of the child. The government must identify and include a negative list of purposes for which no child's data may be processed.

9. **Should general websites, i.e. those that are not directed towards providing services to a child, be exempt from having additional safeguards protecting the collection, use and disclosure of children's data? What is the criteria for determining whether a website is intended for children or a general website?**

No, general websites must not be subject to those safeguards other than with respect to information that it has, with actual knowledge, obtained from children.

To determine whether a website is intended for children or not, a reasonability standard may be implemented, i.e., if the data controller is able to reasonably anticipate that its services/website would be used by children. This standard can be fine-tuned over time.

10. **Should data controllers have a higher onus of responsibility to demonstrate that they have obtained appropriate consent with respect to a child who is using their services? How will they have —actual knowledge of such use?**

There is no fool proof way in which a data controller will have actual knowledge that its services are being used by children. To that end, a reasonability standard may be implemented, i.e., if the data controller is able to reasonably anticipate that its services/website would be used by children, it must have the onus to demonstrate that consent has been obtained.

11. Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?

[●]

Chapter 3: Notice

1. **Should the law rely on the notice and choice mechanism for operationalising consent?**

   If individuals are properly informed about the collection and use of their personal information, they will be able to make more informed decisions about whether that information may be used and how. Provision of notice is important regardless of whether consent is required for the collection and processing of that information.

   However, there are a number of instances where the provision of notice should not be required. This would include situations where the provision of notice is impossible or would involve a disproportionate effort, such as processing for archiving purposes in public interest, scientific or historical research purposes or statistical purposes, or if the requirement to provide the notice would render impossible or seriously impair the achievement of the objectives of that processing (for example, in connection with any sort of investigation). In addition, notice should not be required where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by law, including a statutory obligation of secrecy. Finally, notice should not be required where the purposes of the collection and use are obvious to the individual – for example, when an individual hands a business card to another person.

2. **How can notices be made more comprehensible to individuals? Should government data controllers be obliged to post notices as to the manner in which they process personal data?**

   Notice requirements should apply uniformly across all sectors to ensure consistency. Notices can be made more comprehensible to users by streamlining and sorting the content of notices served to them based on relevance to the individual and requiring them to be made intelligible. Furthermore, by specifically implementing an accountability framework we could ensure that the data controllers will not be able to side-step their liabilities.

3. **Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?**

Privacy impact assessments are useful tools but should be reserved for activities that pose a high risk to the privacy of individuals since they are lengthy and impose excessive costs on the ecosystem. In the Indian context, since the data economy is at a nascent stage and the manpower and expertise required to conduct these audits is currently lacking, the imposition of mandatory privacy impact assessments should only be reserved for matters that will have a serious impact on individual privacy as it may place unnecessary barriers on these industries and hamper their growth.

4. **Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?**

Alternatives:

a. **No form-based requirement pertaining to a privacy notice should be prescribed by law.**

b. **Form-based requirements may be prescribed by sectoral regulators or by the data protection authority in consultation with sectoral regulators.**

Notices need to be meaningful in that they need to convey information that is relevant to the user succinctly and cogently. For that, the data protection law should primarily require notices to be clear and accessible. However, the privacy law should avoid including prescriptive provisions as to what exactly the notice should contain and should particularly avoid making form-based prescriptions. Instead, guidelines and basic requirements as to what the notice should contain should be stipulated. As long as such a notice is provided in a clear and accessible manner, no additional requirements need be imposed on data controllers.

Organisations should have the flexibility to determine the timing of the notice. In some cases, notice can be provided in advance or at the time of collection, whereas in other cases, such as in case of cookies or when the information is not obtained directly from the individual but from a third-party, it may not be

practical to give notice until after the time of collection. The manner in which cookies function requires that the cookie be activated, and thus begin collecting information, before any notice can be given. Similarly, if a consumer uses an ATM, he or she must insert a card which entails the collection of information by the financial institution in order to commence the transaction, or to determine in what language the notice should be given. Thus, the financial institution cannot provide notice regarding the manner in which information will be used until after some information is already collected. The appropriate timing of the notice, therefore, may vary from industry to industry or depend on the data collection methods used.

The other issue that needs to be considered in the context of notice is its frequency. If organisations are required to issue new notices whenever they make any changes to data collection, use, and disclosure practices, and if these changes happen too frequently, customers may simply stop reading these notices. Rather than requiring thousands and thousands of individual notices, the organisation should only be required to post a notice or privacy policy on its website.

5. How can data controllers be incentivized to develop effective notices?

Alternatives:

a. Assigning a 'data trust score'.

b. Providing limited safe harbour from enforcement if certain conditions are met.

If a 'data trust score' is assigned, then who should be the body responsible for providing the score?

Assigning a data score may incentivise organisations to improve their data protection policies. However, the benefits of the transparency and objectivity of a data trust score should be weighed against the time and effort that may be involved in implementing such a system. This might overburden the Data Protection Authority and therefore may not be easy to practically implement. As an alternative, the Data Protection Authority could provide samples/models of the types of notices that they consider to be best in class. That will give

organisations (particularly small and medium-sized organisations in a country that does not yet have a corporate culture of data protection compliance) an easy way to understand what their notices should look like and to adopt those practices.

6. **Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by a government entity?**

As mentioned earlier, we do not believe that consent should be the sole ground under which data should be collected and/or processed. Even assuming we should use consent, centralising a consent dashboard with a government authority is not a feasible solution. Instead, the government should suggest a technological framework for such a dashboard based on open architecture so that the required consent information is made available through open APIs. This will allow the consent dashboard to be maintained by the data controller in a format that is easily accessible by data subjects. Also, it would allow for granular opt-out consent at any time which is one of the key elements of our proposed model.

7. **Are there any other alternatives for making notice more effective, other than the ones considered above?**

[●]

Chapter 4: Other Grounds of Processing

1. **What are your views on including other grounds under which processing may be done?**

There are certain additional grounds of processing that should be included. Our detailed suggestions have been provided in our subsequent answers.

2. **What grounds of processing are necessary other than consent?**

We would suggest four additional grounds of processing:

i. Performance of contract - Personal Data may be collected, used, and disclosed/transferred to fulfil obligations under a legal relationship between the Data Controller and the individual, and so processing should be permissible if required as part of the contract between two parties.

ii. Public interest - If the processing is necessary to be carried out by the government for the exercise of official authority of government representatives or when it is necessary for a prevention/investigation of a crime. Processing may also be in the public interest if it is carried out by a charitable organisation.

iii. Vital interest of the subject - Processing may become necessary to avoid a threat to the life and security of the data subject, such as, where the data subject is injured or disabled and may not be capable of providing consent.

iv. Legitimate interest of the controller – If the processing of personal data is necessary for the legitimate interests of the data controller, such as, if the personal data is required to be processed in order to enable the organisation to provide a service to that individual, or if the personal data is processed by an employer for the purpose of managing or terminating an employment relationship between the organisation and the individual, or where the transmission of personal data within the organisation (or group of organisations) is necessary for internal administrative purposes, including the processing of clients' or employees' personal data, or if such processing is necessary and

proportionate for the purposes of ensuring network and information security, or if such processing is necessary for the purposes of fraud prevention, due diligence to fight bribery, and anti-money laundering activities.

3. **Should the data protection authority determine residuary grounds of collection and their lawfulness on a case-by-case basis? On what basis shall such determination take place?**

Alternatives:

a. **No residuary grounds need to be provided.**

b. **The data protection authority should lay down 'lawful purposes' by means of a notification.**

c. **On a case-by-case basis, applications may be made to the data protection authority for determining lawfulness.**

d. **Determination of lawfulness may be done by the data controller subject to certain safeguards in the law.**

No additional residuary grounds of collection need to be provided and their lawfulness should be determined on a case-to-case basis. Any other construct may overburden the authority and end up being unfair to various classes of data controllers. It will also act as a hindrance for carrying out secure, low-risk processing by controllers. The authority should clearly lay down the standards for other grounds of processing on the basis of which controllers can process the data of individuals without their consent.

4. **Are there any alternative methods to be considered with respect to processing personal data without relying on consent?**

As mentioned above, consent should not be the only grounds for processing as that would make India an outlier in the world. We have listed several alternative grounds for processing in our answers above.

Chapter 5: Purpose Specification and Use Limitation

1. What are your views on the relevance of purpose specification and use limitation principles?

While it is useful to ensure that Personal Data is only collected by data controllers for specified and legitimate purposes, it may not always be possible, particularly in the context of modern big data applications, to always specify the purpose in advance with a high degree of certainty. Therefore, while purpose specification and use limitation should establish the broad boundaries within which Personal Data can be collected, appropriate flexibility should be offered so that these restrictions do not come in the way of using data effectively and in the best interests of the data subject. For that reason, the data protection law should also contain provisions outlining fair processing requirements.

However, in the context of processing by government and/or public sector undertakings, it might be necessary to spell out certain baseline standards for purpose specification and use limitation. Where government and/or public sector entities invoke a statutory exemption from their obligations under the data protection law and are thereby collecting data from an individual as part of their statutory authority, they should be able to demonstrate that the data so collected was used for specified purpose only. They should not have the ability to further process such data beyond the stated purpose. This position will help individuals hold the State accountable for its activities.

2. How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies?

As outlined in the White Paper, it is difficult to state in advance all the uses that a particular data set can be put to at the time of collection. Accordingly, we suggest the implementation of certain fair processing requirements that describe the circumstances under which data could be processed to allow for the use of new technologies.

In addition, we recommend the application of the principle of Accountability (as discussed elsewhere in these responses) in cases where a data controller uses data for a purpose other than the one for which it was collected. Any harm

resulting from such further processing of data can result in liability for the data controller.

3. **What is the test to determine whether a subsequent use of data is reasonably related to/ compatible with the initial purpose? Who is to make such determination?**

The use of fair processing principles and the Accountability principle as outlined in the previous response can help avoid the need for determination of reasonableness/compatibility with an initial purpose. The use of the Accountability principle, in particular, shifts the focus from questions of reasonableness/compatibility to whether harm was caused to an individual due to the processing of data for a purpose not originally outlined. This will also help streamline the functions of the data protection authority under the law.

4. **What should the role of sectoral regulators be in the process of explicating standards for compliance with the law in relation to purpose specification and use limitation?**

Alternatives:

a. **The sectoral regulators may not be given any role and standards may be determined by the data protection authority.**

b. **Additional/ higher standards may be prescribed by sectoral regulators over and above baseline standards prescribed by such authority.**

c. **No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators.**

Sectoral regulators can have the ability to prescribe additional/higher standards over and above these foundational standards outlined in response to Question 1 above.

5. **Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?**

[•]

Chapter 6: Processing of Sensitive Personal Data

1. **What are your views on how the processing of sensitive personal data should be done?**

   Sensitive personal data should only be processed with prior consent. The data controller should be held accountable for any material or non-material harm that is caused to the data subject as a result of the processing.

2. **Given that countries within the EU have chosen specific categories of —sensitive personal data, keeping in mind their unique socio-economic requirements, what categories of information should be included in India's data protection law in this category?**

   Please refer to our response to Question 2 in Part II, Chapter 4.

3. **What additional safeguards should exist to prevent unlawful processing of sensitive personal data?**

   Alternatives:

   a. **Processing should be prohibited subject to narrow exceptions.**

   b. **Processing should be permitted on grounds which are narrower than grounds for processing all personal data.**

   c. **No general safeguards need to be prescribed. Such safeguards may be incorporated depending on context of collection, use and disclosure and possible harms that might ensue.**

   d. **No specific safeguards need to be prescribed but more stringent punishments can be provided for in case of harm caused by processing of sensitive personal information.**

   Any collection of sensitive personal data must be preceded by consent and notice.

   In addition to this, the principle of Accountability should apply in the case of sensitive personal data. Therefore, if an entity processes sensitive personal data and such processing results in harm to the individual, then the entity can be held liable, regardless of consent being obtained. The liability that is ascribed to

the entity in such cases can be more stringent, primarily through the imposition of higher fines.

In addition to this, the law should stipulate that sensitive personal data be stored in a de-identified form to ensure greater level of protection. Further, any re-identification or attempt to re-identify such data sets should also attract liability under the law.

4. **Should there be a provision within the law to have sector specific protections for sensitive data, such as a set of rules for handling health and medical information, another for handling financial information and so on to allow contextual determination of sensitivity?**

Where appropriate, sectoral regulators should be allowed to implement sector-specific protections for sensitive personal data because in certain circumstances, the implications of processing can only be determined contextually. Therefore, sectoral regulators should be encouraged to determine additional safeguards for processing depending on the sensitivity of the information and the harms that may arise from unlawful processing.

5. **Are there any alternative views on this which have not been discussed above?**

[•]

Chapter 7: Storage Limitation and Data Quality

1. What are your views on the principles of storage limitation and data quality?

One of the key concepts of fair processing as generally understood is that personal data should not be retained for longer than is necessary for the purposes for which it was collected. On the other hand, as discussed earlier, it is difficult to exhaustively describe the purposes to which data can be put in the context of modern big data algorithms. That said, for the most part, big data analysis usually does not require the data that is being processed to be personal data. Accordingly, the data protection law should encourage data controllers to either erase, destroy, or de-identify personal data as soon as possible after the purpose for which the personal data was collected has been achieved. Since data retention is tied closely with the limitation principle, no minimum or maximum retention time should be prescribed.

2. On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?

Alternatives:

a. The individual

b. The entity collecting the data

The entity collecting the data must have the primary responsibility of ensuring the accuracy of the data. The individual in all such cases must also have a right to access the information collected and seek rectification if there are inaccuracies. As outlined in the response to Question 4, Part II Chapter 3, this will apply in the case of identified data.

For identifiable data, the individual will not have the right of access and rectification. However, if the processing of data in such cases results in harm to the individual, the Accountability principle will apply and the entity processing the data can be held liable.

3. How long should an organisation be permitted to store personal data? What happens upon completion of such time period?

Alternatives:

a. Data should be completely erased

b. Data may be retained in anonymised form

As pointed out in the White Paper, it may not be feasible to have a blanket prescription of a fixed time period for the retention of all kinds of data. Given this, the data protection law can forego the stipulation of a fixed time period for retention.

Data collectors must be allowed to determine the retention period most appropriate for the data. The broad principle should be that data should only be retained for as long as required for the purpose or under the law. Indicative retention periods can be provided based on the relevant sector or to the type of data in question, as a good practice measure.

Having said that, depending on the sector or organisation in question, some data may need to be held longer than the purpose detailed. For example, an employer would need to hold data relating to employees past their period of employment for matters such as future claims or litigation. The standard, however, should be that organisations should have the authority to implement the retention period best applicable to them and their business practices.

Note: The recommendations in this response are subject to any data retention requirements that might be provided for under other laws.

4. If there are alternatives to a one-size-fits-all model of regulation (same rules applying to all types of entities and data being collected by them) what might those alternatives be?

We would recommend against applying different rules to different entities in order to ensure consistency across all data controllers.

5. Are there any other views relating to the concepts of storage limitation and data quality which have not been considered above?

The following additional points may be relevant:

i. In relation to shared data, all organisations in possession of that data should destroy or de-identify the same after the stated purpose has been met.

ii. If a data subject has challenged the data being held by a data controller as being inaccurate, the data subject should be given the opportunity to rectify it.

Chapter 8: Individual Participation Rights-I

1. What are your views in relation to the above?

We agree that the right to information, knowledge of purpose specification, and rectification of inaccurate data are essential rights in a data protection law.

2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?

Individuals should be able to access information that they have provided to the data controller. However, as it is normal for the data controller to layer an individual's personal information with other information and other observable behaviour, it might be difficult and technically infeasible to provide individuals access to this information.

Legally, privileged information would not be accessible to an individual data user. Similarly, if data is held for journalism or any other purpose for which there is an exception under the law, its access would be restricted to the data subject. Where the personal information of other individuals would be compromised if the requesting individual's data is shared[7], this would also be restricted to the user requesting information.[8]

The requesting individual should also not have access to unstructured data, as sharing this information might result in compromising other individuals' personal data.

3. What should be the scope of the right to rectification? Should it only extend to having inaccurate date rectified or should it include the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?

The data subject should have the right to ask the data controller to rectify the inaccurate data. However, as mentioned above, the right to rectification should be limited to data that has been actually provided by the data subject and not to identifiable data that has been collected by the data controller through observation or as part of the individual's interactions with the data controller. While the option to seek judicial appellate remedies should not be denied to the data subject, it should be available to the data subject once the data controller

denies or refuses rectification without any reason. In this case, the data subject would be able to make a case for harm arising from such non-rectification as well, enabling him to move court for appropriate remedies. The right to rectification must apply only to identified data.

4. Should there be a fee imposed on exercising the right to access and rectify one's personal data?

No. There is no need for a fee to be imposed to exercising the right to access and rectify identified data. As mentioned in the answer to Question 3, Chapter 8, Part III of this White Paper, this right will only apply to identified data and not to non-identified / identifiable data.

5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?

No specific time period should be specified. Instead this should be left to the respective data controllers to determine based on their own specific circumstances. However, the Data Protection Authority should have the ability to assess whether any time specified is reasonable.

6. Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?

No, the right to access logic behind all automated decisions would not always be feasible. In black box audits, for instance, this would not be possible. The proposed data protection statute should provide for an audit mechanism which checks for bias at the margin. If the algorithm is seen to be causing harm, then the data controller can be required to make appropriate changes to mitigate the harm that is being caused.

Similarly, an audit that compares the logic of an automated output to the input that was computed could also be undertaken to check for algorithmic bias. This can then be rectified at the margin.

7. What should be the exceptions to individual participation rights?

Individual participation rights should not apply to aggregated or identifiable data. They should not be exercised in situations where compliance with a

request is impossible or requires disproportionate effort. For example, it may be very difficult to accede to a request for access to all the email correspondence relating to a given individual's personal data. The question as to what may amount to a disproportionate effort may have to be defined on a case by case basis. Similarly, the exceptions as set out in the answer to Question 2 in this chapter should be applicable here as well.

8. **Are there any other views on this, which have not been considered above?**

[•]

Chapter 9: Individual Participation Rights-2

1. What are your views on the above individual participation rights?

We agree that the right to object to processing, the right to object to processing for the purpose of direct marketing, the right to not be subject to automated decision making, the right to data portability, and the right to restrict processing are essential rights in a data protection statute.

2. The EU GDPR introduces the right to restrict processing and the right to data portability. If India were to adopt these rights, what should be their scope?

It appears that for the right to restrict processing to apply under the GDPR, the user must identify the information that is being processed and then request that processing be stopped. While the right itself is desirable as a means to ensure that data is processed securely, the subject might not always be able to apply this right as a preventive measure. As our model stresses on accountability of the data controller, the right to restrict processing must be available to the data subject on the basis of the data audit too. If the data controller is found to be processing inaccurate information in an audit or processing the data in an insecure manner, the data subject should be able to exercise this right.

The right to data portability should also be allowed under the Indian statute. Again, the onus need not be on the individual to elaborate exactly what uses his data is put to by the controller or what processes the controller uses. It should be enough if the data subject is aware of the main aspects of his data shared with the controller and what the resulting service is (for instance, as done in cases of mobile number portability).

3. Should there be a prohibition on evaluative decisions taken on the basis of automated
decisions?

Alternatives:

a. There should be a right to object to automated decisions as is the case with the UK.

b. There should a prohibition on evaluative decisions based on automated decision making.

No. Automated decision-making algorithms should not be subject to a blanket ban under the data protection law. However, in order to ensure that the use of decision-making algorithm does not lead to discriminatory or detrimental results, the audit mechanism suggested in this paper should be implemented which will adequately ensure that the algorithm meets the code of conduct in place and does not detrimentally affect the data subjects.

4. Given the concerns related to automated decision making, including the feasibility of the right envisioned under the EU GDPR, how should India approach this issue in the law?

There should be scope for automated decision making under the Indian data protection law. In fact, data users may sometimes prefer automated decisions as they are quicker and provide benefits by reducing information asymmetry (for instance, food delivery applications recommending places to eat from on the basis of historical data about the user may be convenient and beneficial). That said, there should be protection against unintended harms occurring as a result of automated decision making.

That said, the risks of automated decision making may be checked by data audits that look for biases along the margin and check for harm caused by these automated processes.

The data controller will continue to be accountable for arbitrary automated decision making. In addition to there being a right against automated decision making, the data controller should ensure that all data processes that lead to automated decisions are done with diligence, are transparent, and are secure. Every audit, risk and impact assessment of the data controller will capture the logic and impartiality behind the data controller's algorithms making automated decisions, holding the data controller accountable for its actions.

5. Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations?

It might be better if the right against processing for the purpose of direct marketing is addressed via sector specific regulations. Until that time, however, if the data user's variety of choice is impacted by direct marketing and if the inconvenience caused by this amounts to a harm, then the data subject will be able to exercise the right to object to processing, requiring the controller to stop targeted marketing to the subject.

6. Are there any alternative views which have not been considered?

[●]

Chapter 10: Individual Participation Rights-3

1. What are your views on the right to be forgotten having a place in India's data protection law?

The right to be forgotten does not provide any additional protection to individuals over and above the right to deletion. In the context of organisations other than internet search engines, the right to be forgotten is essentially a restatement of the right to request deletion. If the right to be forgotten is included in India's law, it should be limited to internet searches engines.

Having said that, our recommendation is that since Indian privacy jurisprudence is still nascent, the right to be forgotten should be developed by judicial precedent and does not need to be reflected in the statute.

2. Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

The right to be forgotten in the context of internet search raises complex issues relating to freedom of the press and the deletion of information that may have historical or social value. Our recommendation is that the right to be forgotten should not be included in the new law. If at all required after the enactment of the privacy law, it would be better for this jurisprudential principle to be built by the courts on a case-by-case basis rather than set it out in the statute *ex ante*.

3. Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

Outside of the online search context, the right to be forgotten is simply a right to request deletion and does not significantly increase protections for individuals.

4. Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controller's possession?

Outside of the online search context, the right to be forgotten is simply a right to request deletion and does not significantly increase protections for individuals.

5. **Whether a case-to-case balancing of the data subject's rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise? If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority or courts?**

   The burden of determining the balance between public interest and individual rights, if left to companies, should subject them to significant penalties if those companies have adopted a fair process but a court later disagrees with the final decision. Thus, while the companies should be held accountable, they should not be penalised where they have followed a legitimate process. The courts should perform a case-by-case balancing and interpretation of this right.

6. **Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (Over and above possible general exemptions such as national security, research purposes and journalistic or artistic expression)?**

   Yes, the right for freedom of expression and the right to have national figures held to account are important rights that need to be taken into account. The security, research, and journalistic and artistic expressions are not sufficient.

7. **Are there any alternative views on this?**

   [•]

Response to Part IV

Chapter 1: Enforcement Models

1. What are your views on the above described models of enforcement?

A model of co-regulation is best suited for an Indian data protection statute.

Any data protection law in India should be centred around two principles:

i. Striving for greater information symmetry; and

ii. Holding the data controllers accountable. Given that data collection and processing take place across sectors, a "command and control" legislation would be inadequate and swiftly redundant. On the other hand, while industries should be allowed to develop their own frameworks for data protection, it is necessary to have an umbrella statute, under whose aegis sector specific guidelines can develop.

The co-regulation model will be an effective means to solve the problem of information asymmetry and lack of accountability.

2. Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?

Yes. A co-regulation approach to a data protection enforcement mechanism would: (i) be an umbrella legislation, applying across industries and not specific to an industry; and (ii) be timeless and relevant in the face of technology that has already developed and is likely to come about in the future. It is also the most effective means of ensuring controllers' accountability, and creating a user-centric data ecosystem.

3. What are the specific obligations/areas which may be envisaged under a data protection law in India for a (i) "command and control" approach; (ii) self-regulation approach (if any); and (iii) co-regulation approach?

The table below outlines what the statute should cover and what industry bodies should specify under a co-regulation approach:

Item	Data Protection Statute	Sector Specific Regulations
Definitions	The statute should set out the ambit of the terms like "personal information", "sensitive personal information", "data audit", etc.	
Principles	The principal data protection statute should lay down the extent of the role consent and accountability should play. It will enumerate the specifications of consent that controllers need to demonstrate to have taken from data subjects. It will also lay down when the principle of accountability will operate and to what extent it will hold the controller liable	Sector specific guidelines should lay down context specific issues relating to consent (e.g. minor's consent for the collection of genetic data) and the accountability attached to data controllers in those cases.
Rights and Harms	The statute will contain an inclusive list of data subjects' rights. It will also contain a set of harms that will allow the data subject to approach the Data Protection Authority for appropriate remedies. The statute will also explain the extent of these rights, and the injuries the data subjects would have to demonstrate in the event of a harm.	
Processes	The statute will lay down the foundational principles for secure and transparent processing of data. In the event of conflict between the sector specific guidelines governing these processes, the statute will prevail. The statute must also set out the kinds of security processes that the controller must have in place (e.g. risk assessments, impact assessments, designated data protection officer, etc.)	Along the lines of the principles and compliances outlined in the statute, the sector specific guidelines should specify what operations the controller must conduct to securely process its subjects' data. The guidelines must prescribe the frequency and contents of the DPIAs and risk assessments the controller must perform at operative periods, a

		hierarchical representation of the people responsible for these processes at various junctions, etc.
Liability	The statute must set out the kinds and extent of liability of a defaulting data controller. It may also outline the mitigation mechanisms available to the controller.	
Registration	There should be no registration requirement under the statute save for narrow, specific purposes such as registration to allow data localisation.	Compliance with secure data practices must be a mandatory stipulation while registering an entity to carry on business in a specific sector. The certificate of registration must mandate that the controller is to comply with the data protection statute as well as the authoritative sector specific guidelines applicable to it.
Data Audits, enforcement mechanism	The statute must lay down the kinds and frequency of audits that the controller should conduct. It should also set out the qualifications of data auditors. Constitution and powers and functions of the Data Protection Authority, Data Protection Appellate Tribunal, and each controller's data protection officer.	The contents of data audits specific to the sector must be enumerated by the recognized industry body.
Codes of conduct	The statute must only mandate that all data controllers must comply with the codes of conduct applicable to them. It may annexe a non-binding Model Code of Conduct to enable controllers to create their own.	While each controller may have its detailed operational code, these must be in line with the codes of conduct prescribed by the statutorily recognised industry body. These codes, then ratified by the Data

		Protection Authority, will bind all data controllers in the concerned sector.

4. Any alternative views to this?

[●]

Chapter 2: Accountability and Enforcement Tools

1. What are your views on the use of the principle of accountability as stated above for data protection?

As discussed earlier, the trend in data protection laws around the world is to move away from relying on consent as a primary legal basis for processing. The consent model results in individuals experiencing consent fatigue and adds a substantial compliance burden on organisations. We believe that under these circumstances, the principle of accountability is appropriate to address the privacy concerns under the proposed Indian data protection law.

Under the accountability model, the data controller should be able to collect and process personal data wherever necessary for the purposes of the legitimate interests of the data controller. However, under all such circumstances, the data controller shall be accountable for all harms that will be caused to the data subject as a consequence.

2. What are the organisational measures that should be adopted and implemented in order to demonstrate accountability? Who will determine the standards which such measures have to meet?

Accountability should not be regarded as a monolithic concept, one that requires compliance with a rigid set of organisational measures. Organisations should be able demonstrate their accountability through multiple paths.

In fact, requiring organisations to jump through specific administrative hoops in order to demonstrate compliance would defeat the intent of the accountability approach. The purpose of the accountability principle is to ensure that organisations take reasonable steps to ensure that personal data is handled in a way that it does not cause harm to the data subject.

To achieve this, the data controller is encouraged to adopt practices consistent with the principles set out elsewhere in the law and to implement policies and procedures to give effect to those principles. It is preferable to encourage organisations to take steps that are truly privacy enhancing in the context of what they are doing with the data, rather than imposing monolithic requirements across all data controllers. For example, having a formal

governance structure makes sense for an organisation with 100,000 employees but makes little sense for a company with 20 employees.

3. **Should the lack of organisational measures be linked to liability for harm resulting from processing of personal data?**

The focus of the enforcement activities should be on those situations where individuals have been harmed. The enforcement efforts should not focus on whether an organisation had perfect policies and procedures but whether individuals were harmed as a result of actions or inactions of the organisation.

4. **Should all data controllers who were involved in the processing that ultimately caused harm to the individual be accountable jointly and severally or should they be allowed mechanisms of indemnity and contractual affixation of liability inter se?**

Companies should be allowed to create mechanisms of indemnity and apportion liability amongst themselves contractually. Given the complex nature of processing and the multitude of entities involved, it would be unfair to hold companies that are complying with the law and the obligations to be strictly liable for the failure of another organisation. Therefore, the liability for harm caused to individual must be allocated to the data controllers who have not met their obligations and have caused the resultant harm. Organisations are experienced at allocating risk in that way through contractual mechanisms and should be permitted to do so.

5. **Should there be strict liability on the data controller, either generally, or in any specific categories of processing, when well-defined harms are caused as a result of data processing?**

No. Strict liability is too stringent a standard to apply for data processing. In order to promote innovation and development, organisations should be able to apportion risk and responsibility. The entity that causes the harm to the individuals should be held liable, not the entity that has fully complied with its legal obligations and not caused the harm.

6. **Should the data controllers be required by law to take out insurance policies to meet their liability on account of any processing which results in harm to**

data subjects? Should this be limited to certain data controllers or certain kinds of processing?

Insurance obligations should not be imposed on data controllers. However, the controller should be free to take out an insurance policy to indemnify themselves of liability under the data protection regime.

7. **If the data protection law calls for accountability as a mechanism for protection of privacy, what would be the impact on industry and other sectors?**

Accountability would ensure that all organisations are responsible to keep their data secure in accordance with the risks of harm associated with their processing of data. Since the data subject may not be in a position to assess the consequences of providing consent, it might be advisable to shift the burden to the data controller who is best placed to ensure that their processing of personal data is in the interests of the data subject. The accountability framework addresses that situation.

8. **Are there any other issues or concerns regarding accountability which have not been considered above?**

[●]

Chapter 2A: Codes of Practice

1. What are your views on having codes of conduct?

We believe that codes of conduct are desirable. They will allow industries to create sector specific norms, allowing for them to accommodate themselves to the compliance requirements under the data protection law. These codes of practice can be drafted in consultation with the Data Protection Authority and ratified by it to give them the force of law. All obligations under data protection regime including industry specific codes of practice, audit and revision requirements, risk assessment, and data protection impact assessments etc., should be included in the codes of practice of a data controller. Adoption of these codes of practice and demonstration of implementation of these codes of practice should serve as evidence of compliance with the controller's obligation under the data protection regime.

2. What are the subject matters for which codes of practice or conduct may be prepared?

The codes of practice must cover how the data controller would implement all their obligations to the data subject under the data protection law. An illustrative list of the topics that codes of practice should cover are set out below:

i. Standards of fair and transparent processing;

ii. Legitimate interests of data controllers in specific contexts;

iii. Pseudonymisation (or other kinds of de-identification) of identified data. Requirements of de-identification and what would constitute re-identification of personal data;

iv. Implementation of privacy by design and privacy by default;

v. Security breaches and accompanying notifications;

vi. Processes to be followed in transferring identified/identifiable personal data to third parties;

vii. Applicable rights of data subjects and what how these may be exercised;

viii. Risk and impact assessments before data is collected and before every major step in the processing phase;

ix. Best practices for all processes (from consent to dispute resolution to secure disposal of data); and

x. Audit standards to be followed by internal auditors as well as third party auditors.

3. What is the process by which such codes of conduct or practice may be prepared? Specifically, which stakeholders should be mandatorily consulted for issuing such a code of practice?

Codes of conduct should be prepared by the registered/statutorily authorised industry association of the data controller. The member entities of such associations as well as their customers should be mandatorily consulted before such codes are issued.

As codes of conduct would largely be concerned with compliance of internal data security standards and the conduct of data audits, it would be sufficient if the members of the industry body agree to these terms.

4. Who should issue such codes of conduct or practice?

The statutorily recognised industry body should issue codes of practice. These guidelines can then be ratified by the Data Protection Authority.

5. How should such codes of conduct or practice be enforced?

The data protection statute should contain a provision allowing industry specific data security standards to be binding codes of conduct. If these standards are found to be in line with the Data Protection statute, then they will be ratified by the Data Protection Authority. Once ratified, the codes of conduct become statutorily enforceable. Compliance would be necessary to avoid being penalised. This will ensure that they are still complied with in accordance with the act.

6. What should be the consequences of violation of a code of conduct or practice?

The penal consequence of violating a code of conduct also depends on its severity. If a procedural compliance is overlooked, but no harm or drastic consequence occurs to the user as a result of this, then a fine would be sufficient. However, if there has been a graver compliance violation, or harm has been caused to a data user then the penalty should be higher (our views on penalties have been set out in greater detail in Part IV Chapter 4A).

If a suit has been filed by a harmed data subject, and the reason for such harm is found to be non-compliance of codes of conduct, then the subject must be able to file a suit for damages.

7. Are there any alternative views?

[●]

Chapter 3B: Personal Data Breach Notification

1. What are your views in relation to the above?

Breach notification obligations can serve important individual and public policy objectives. From the individual perspective, the primary purpose of notification is to enable individuals to mitigate the risk of identity theft or fraud when a breach occurs. On the other hand, the primary purpose of reporting a breach to the government is to enable the authorities to exercise their regulatory oversight functions, for example, to identify persistent or systemic security problems and take action as needed to address those problems and to assist individuals who may be harmed by a breach. In addition, reporting obligations serve to motivate organisations to implement more effective security measures to protect sensitive information.

The goal of breach notification provisions should be to define a reasonable and balanced notification trigger that ensures that individuals receive notice when there is a significant risk of substantial harm as a result of a security breach but that does not result in over-notifying and desensitising individuals to important notices. Most security breaches do not result in significant harm. Businesses increasingly store and transmit customer data in unique media forms that require highly specialised and often proprietary technology to read, including sophisticated encryption. Thus, even if customer data finds its way into the wrong hands, the data often is not in a readable or usable form. Notification requirements should recognise this and the appropriate response to each breach should also differ. Moreover, because notification to individuals and public authorities serves different purposes, there should be different notification triggers for both groups.

Individuals

The primary purpose of providing notices to individuals is so that they can take steps to mitigate the harm that might result from a breach. Individual notification requirements should therefore be risk-based. Notification should focus on the harm to sensitive financial and health information. If there is a significant risk that sensitive financial information has been compromised in a breach and that this will be used to commit identity theft or to make fraudulent

transactions using an individual's account, then the individual should be notified. Similarly, in situations where there is a significant risk that sensitive health information compromised in a breach will be used to cause the individual significant harm such as, for example, loss of business or employment opportunities because of an individual's health, then the individual should be notified.

Public Authorities

The primary purpose of government reporting is to enable the authorities to identify persistent or systemic problems and take action as needed to address those problems. It does not make sense for the law to require government authorities to be notified about a security breach believed to affect only a few individuals (in addition to notifying the individuals themselves). Frequent reporting about relatively minor security breaches will overwhelm the public agencies responsible for consumer protection and data security regulation, whose resources are most likely already stretched thin. Consequently, only major breaches (e.g., those affecting more than 10,000 individuals) or breaches involving significant risk to individuals should be reported. An appropriate threshold should be selected. In addition, the public authority may also wish to require reporting whenever there has been a material privacy breach that involves suspected criminal activity outside the organisation regardless of the number of individuals affected.

Separately, irrespective of whether the data controller notifies the DPA or the data user of a breach, these instances should always be captured in the controller's data protection audits and risk assessments.

2. How should a personal data breach be defined?

The law should specify the types of information that would be subject to these obligations. Notification should only be required in the context of information that could be used to cause the "significant harm" that the notification requirement is designed to help individuals mitigate. The notification obligation should be limited to identifiable and unencrypted data that includes one or more sensitive data elements, such as, in case of financial information, account information together with any password or pin number that can be used to

access the underlying account and in the context of medical data, the individual's name together with some sensitive health data elements, such as, a medical diagnosis.

This would encourage organisations that can both work proactively to strengthen safeguards for this sort of information and, if various security breach incidents do occur, focus their responses on those incidents that relate to this information. Data that have been de-identified, encrypted or otherwise adequately secured (using other technology), however, should not be covered because an incident affecting such data does not pose a high risk of significant harm to individuals. Similarly, data that is publicly available should be excluded.

3. When should personal data breach be notified to the authority and to the affected individuals?

While notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the scope and nature of the breach, remedying any ongoing breach and identifying potentially affected individuals, the law should permit notification to be delayed at the request of a law enforcement agency in order to carry out its own investigation. For example, before notification is provided and before a breach is publicised in the media, law enforcement will have a better opportunity to catch the culprits involved (thereby, preventing future breaches from occurring or mitigating the harm felt by individuals). Setting a specific time period such as 72 hours is unrealistic and will result in the notification containing insufficient information in order to be useful to individuals or to regulators.

4. What are the circumstances in which data breaches must be informed to individuals?

Answered in Question 2, Chapter 2, section B of Part IV of this White Paper.

5. What details should a breach notification addressed to an individual contain?

Depending on when the breach notification is sent to the individual, it should:

i. Contain a clear summary of what happened, what caused the breach and why it was not foreseen;

ii. Clearly state the measures that the data controller has taken/is taking to mitigate the damage or to undo the impact of the breach;

iii. State whether any personal data of the subject has been compromised;

iv. Outline the steps that the data subject can take to protect himself/ herself;

v. Provide the subject with the option to withdraw their data from the controller's database.

6. Are there any alternative views in relation to the above, others than the ones discussed above?

Upon notification to the Data Protection Authority, the data controller must work with the authority to diagnose and mitigate the risks associated with the personal data breach. The authority may pose questions to the data controller to assess whether the data breach has been caused due to a widely prevalent system vulnerability – in which case, the authority may inform other data controllers of the same and require them to apply appropriate solutions.

Chapter 3C: Categorisation of Data Controllers

1. **What are your views on the manner in which data controllers may be categorised?**

   Data controller should not be categorised on the basis of their turnover. Data protection is a cost of business and must be applicable across businesses of all sizes.

2. **Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?**

   No. It is unlikely that a classification of controllers would aid in mitigating risk and facilitating compliance.

3. **Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?**

   No. It might be harmful to approach a categorisation of controllers in this manner. A presupposition of harm for classification could either cause a chilling effect on business or may be used by controllers to take shelter under its loopholes.

4. **What are the factors on the basis of which such data controllers may be categorised?**

   We do not recommend that data controllers be categorised.

5. **What range of additional obligations can be considered for such data controllers?**

   Based on the responses set out above, we do not recommend any additional obligations.

6. **Are there any alternative views other than the ones mentioned above?**

   [●]

REGISTRATION

1. Should there be a registration requirement for certain types of data controllers categorised on the basis of specified criteria as identified above? If yes, what should such criteria be; what should the registration process entail?

Registration should not be mandated under the data protection statute. In fact, it should not be the rule under the data protection statute, but the exception. For instance, while the statute need not make any mention of registering each data controller, it might make a specific provision requiring registration if data is sought to be localised in India.

Sector specific registration of each controller should also include compliance with data protection standards as relevant to that sector as a mandatory condition for registration.

2. Are there any alternative views in relation to registration?

[●]

DATA PROTECTION IMPACT ASSESSMENT

1. What are your views on data controllers requiring DPIAs?

DPIAs are useful to ensure that data controllers plan for and implement effective mechanisms to assess new technologies in order to consider the associated risks and likelihood of their occurrence. They assist in mitigating the costs and damage to an organisation's reputation that would accompany a breach of the data protection law.

Data controllers should be required to conduct DPIAs before deploying any new technology or an update to their software, especially for processing non-anonymised, individual level data. However, given that the Indian data protection regime is nascent, care should be taken to ensure that the DPIA obligations are not too stringent as that would place an onerous burden on the data controllers.

2. What are the circumstances when DPIAs should be made mandatory?

DPIAs should only be required in cases where the controller is looking to adopt new technologies to process identified or identifiable information and there is a serious risk of negative and unknown consequences to privacy as a result. The use of DPIAs by data controllers should certainly be encouraged but should not be mandated under all circumstances. For example, it does not make sense to mandate PIAs when the consequences are already known and certain measures and procedures are commonly applied, no impact assessment should be required. In addition, the frequency of such impact assessments should be determined by the organisation itself so that it does not become another costly and unnecessary administrative burden.

In addition, there should be no compulsory requirement to make such assessments public or file them with the regulator as this would discourage their use and possibly compromise the integrity of the assessment itself. They have the greatest value as a powerful internal tool that would enable organisations to manage and mitigate their risks. Organisations that do carry out such assessments should maintain appropriate records that can be inspected by authorities in the event of a compliance or enforcement investigation.

3. Who should conduct the DPIA? In which circumstances should a DPIA be done (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?

The internal data protection officer should conduct the DPIA, along with the operations, risk assessment, legal, and compliance teams.

The Data Protection Authority should not be burdened with impact assessments as this could raise issues of conflict of interest.

4. What are the circumstances in which a DPIA report should be made public?

DPIAs need not be made public. Imposing a requirement to make such assessments public or file them with the regulator would discourage their use and possibly compromise the integrity of the assessment itself. Their value as a powerful internal tool enabling organisations to manage and mitigate their risks would be severely undermined. Organisations that do carry out such assessments should maintain appropriate records that can be inspected by authorities in the event of a compliance or enforcement investigation. It is sufficient if the Data Protection Authority and the auditors to have access to these assessments.

5. Are there any alternative views on this?

[●]

DATA PROTECTION AUDIT

1. What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?

Providing for data protection audit provisions would offer an effective method by which the data controller can consistently and adequately review their data protection practices and establish a clear strategy for compliance with the data protection law. The law should not stipulate the periodicity with which internal audits should be conducted as this must be established by sectoral requirements with due regard to the cost and other implications of such an obligation on small businesses. Audit requirements can be set as per the Codes of Practice established within the relevant organisation.

2. Is there a need to make data protection audits mandatory for certain types of data controllers?

No, data protection audits need not be made mandatory for certain categories of controllers.

3. What aspects may be evaluated in case of such data audits?

A data audit should evaluate the following:

i. Compliance with the legal obligations that the controllers are bound by;

ii. The details of the controller's information governance system, adequacy and accuracy of its data security architecture;

iii. The purpose, extent, and period of data retention;

iv. The security processes the data controller ought to have in place, and the extent of its compliance with these norms;

v. Details of data requests (access, process queries, removal requests, etc.) made on the controller by data subjects or by the Data Protection Authority (e.g. transparency reports);

vi. Measures taken by the controller to increase privacy awareness within its organisation;

vii. The risk assessments that data controllers had conducted before collecting/processing data;

viii. Record of DPIAs conducted by the controller;

ix. If any breach has occurred; whether this warrants notification to the data subject and whether the data protection authority was informed of the same.

4. Should data audits be undertaken internally by the data controller, by a third party (external person/agency), or by a data protection authority?

By a third party (external person/agency), qualified for this purpose.

5. Should independent external auditors be registered/empanelled with a data protection authority to maintain oversight of their independence?

It is not recommended that the auditor, either external or internal, be subject to registration or monitoring by the Data Protection Authority. However, in time the Data Protection Authority may establish a system of certification under which the auditors are rated based on their compliance with norms stipulated by the Data Protection Authority. The focus should be to create a market for auditors without imposing unnecessary compliance related burdens.

6. What should be the qualifications of such external persons/agencies carrying out data audits?

Data auditors should be persons with the technical knowledge of data processing. They should also be certified by an independent, registered association to conduct these audits.

7. Are there any alternative views?

[●]

DATA PROTECTION OFFICER

1. What are your views on a data controller appointing a DPO?

Companies may appoint a person as a DPO, to oversee the healthy collection and processing of personal data.

2. Should it be mandatory for certain categories of data controllers to designate particular officers as DPOs for the facilitation of compliance and coordination under a data protection legal framework?

Yes. Data controllers collecting personal data from more than 1,000 individuals, or having a turnover of more than Rs. 100 crores should be mandatorily required to designate a DPO.

3. What should be the qualifications and expertise of such a DPO?

The DPO should be qualified as a lawyer, or as a data professional with sectoral expertise.

4. What should be the functions and duties of a DPO?

The DPO should oversee compliance of the data protection requirements set out in the statute and in the codes of conduct applicable to the controller.

In order to ensure independence and transparency of operations, the DPO should have structural independence within the organisation. The DPO should report directly to the board of directors of the controller.

5. Are there any alternative views?

[●]

DATA PROTECTION AUTHORITY

1. What are your views on the above?

The Data Protection Authority should be a separate independent authority responsible for investigations into violations and for ensuring compliance with the data protection framework. The list of powers and functions of the data protection authority under the proposed statute appears to be comprehensive.

2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

Yes, it is essential to constitute a specialised quasi-judicial body to monitor and ensure compliance with the statute. This body will also be the first forum for data subjects' grievance redressal.

3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

This might be an inadequate measure. The mandate of the CIC under the RTI Act is:

i. Post facto redressal mechanism, i.e., the CIC's duties kick in when a citizen has been unable to file a complaint with some of the other authorities under the RTI Act;

ii. The scope of CIC's authority extends only to government bodies falling within the scope of the RTI Act.

Additionally, the duty of the data protection officer is highly technical and specific to the data protection statute. Quite like having a specialised body such as the Competition Commission of India constituted under the Competition Act to oversee the fair market behaviour of sellers across Indian markets, the Data Protection Authority should be born out of the statute governing data protection.

4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

The Data Protection Authority should be a quasi-judicial body comprised of five members. The members comprising the Authority may be individuals with a background in law, regulatory affairs, information technology, and economics such that the body provides a holistic perspective on the subject of the statute. Equally, given the high level of technical expertise required for the functioning of the DPA and the fast pace at which technology develops, there should also be a technical advisory committee providing research and advisory support to the DPA. This could be housed in an existing academic or research institution, and be independent of the authority itself.

5. **What is the estimated capacity of members and officials of a data protection authority in order to fulfil its functions? What is the methodology of such estimation?**

We have answered this question in our response to Question 4 of Chapter 2, section D, Part IV of this White Paper.

6. **How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?**

The members should be appointed by a selection committee comprising members from the appropriate department of the government and from the judiciary. The appointment should be made in consultation with relevant industry organisations participating with the Data Protection Authority under the co-regulatory model.

7. **Considering that a single, centralised data protection authority may soon be overburdened by the sheer quantum of requests/complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction be? What should be the constitution of such state level authorities?**

State level data protection authorities should be set up to administer the data protection law within the state. The constitution of state level authorities can be determined by a selection committee constituted at the state level and based on the recommendation of the national authority.

8. **How can the independence of the members of a data protection authority be ensured?**

It is essential that the Data Protection Authority comprise of members other than the executive, including members from a legal background and independent representatives of the private sector. A DPA comprised of people from versatile backgrounds would go a long way in ensuring that the body's independence is retained. Additionally, the members of the authority should be granted an assured term unless they become disqualified to hold the post. Their salaries should be drawn from the consolidated fund of India and their membership should have representation from the government, industry, and civil society.

Constituting a separate, independent technical advisory body would go a long way in ensuring the DPA's independence.

9. Can the Data Protection Authority retain a portion of the income from penalties / fines?

Yes, the Data Protection Authority should be allowed to retain a percentage from penalties. This will assist the DPA's internal funding as well as allow it to carry out awareness activities.

10. What should be the functions, duties and powers of a data protection authority?

The DPA should be authorised to:

i. Conduct *suo motu* investigations on a data controller's processing and security practices;

ii. Entertain complaints filed by the Data Auditor and adjudicate on matters of non-compliance by the data controller;

iii. Entertain complaints by harmed data subjects, investigate, and adjudicate on whether the data controller is liable to remedy the harm caused to the data subject;

iv. Prescribe guidelines to be followed by data controllers on secure processing, storage, and transfer of data;

v. Prescribe guidelines to be followed by data auditors on the principles to be borne in mind in a data audit; and

vi. Prescribe registration and certification standards for data controllers and data auditors alike.

vii. The DPA should also be empowered with the same powers of a civil court for the summoning of witnesses, documents, and to pass any orders or decrees of a civil nature, etc.

11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

The DPA would only be able to set broader scale standards, from the perspectives of privacy, fairness, and security. The more detailed standards would be better set by recognised industry associations. The DPA can then ratify these standards if they comply with the principles of the data protection statute. The operational standards that each data controller processes data by will have to comply with the industry specific guidelines ratified by the data protection authority.

The DPA is a creation of the legislature – it is constituted by an act of the government and is tasked with the duty of enforcing the law. The DPA is a wing of the government.

12. Are there any alternative views other than the ones mentioned above?

[●]

Chapter 3: Adjudication Process

1. What are your views on the above?

While the concept of a Data Protection Authority may greatly benefit the enforcement of the data protection law, the involvement of the Consumer Dispute Redressal Forums may not be appropriate. These forums may not have the requisite technical expertise or qualifications to adjudicate a dispute of this nature. The TDSAT may, for similar reasons, also not be appropriate to adjudicate disputes relating to data protection.

The Data Protection Authority should be the primary adjudicating body under this statute. That said, it would be useful to constitute zonal offices of the DPA. Similar to the manner in which India is divided into various regions for compliance with the Companies Act, it should be segmented into zones on the basis of the density of data being processed in that zone.

2. Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

Yes. The Data Protection Authority (through its zonal officers) should be the adjudicating authority for all complaints from data subjects, data auditors, and any other entities about violations of the data protection law.

3. Where the data protection authority is given the power to adjudicate complaints from individuals, what should be the qualifications and expertise of the adjudicating officer appointed by the data protection authority to hear such matters?

This question has been answered in Question 4, Chapter 2D (*Data Protection Authority*).

4. Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT)?

No. Appeals from the orders of the Data Protection Authority should lie with a specialised appellate tribunal constituted under this statute.

5. **If not the Appellate Tribunal, then what should be the constitution of the appellate authority?**

There should be one Data Protection Appellate Tribunal (DPAT) in every zone. It should be comprised of three members (the composition may be similar to the answer provided in Question 4, Chapter 2D (*Data Protection Authority*)).

6. **What are the instances where the appellate authority should be conferred with original jurisdiction? For instance, adjudication of disputes arising between two or more data controllers, or between a data controller and a group of individuals, or between two or more individuals.**

The DPAT may have original jurisdiction if the damages sought by the data subject exceed Rs. 50 crores.

It is not necessary to have disputes between data controllers and individuals or between data controllers *inter se* to be referred to a higher tribunal.

7. **How can digital mechanisms of adjudication and redressal (e.g. e-filing, video conferencing etc.) be incorporated in the proposed framework?**

Digital friendliness of adjudication should not be a provision in the data protection statute. This is a separate issue of judicial robustness that must take place independently.

8. **Should the data protection authority be given the power to grant compensation to an individual?**

Yes. The Data Protection Authority should also be able to pass other orders such as injunctions in favour of an individual.

9. **Should there be a cap (e.g. up to Rs. 5 crores) on the amount of compensation which may be granted by the data protection authority? What should be this cap?**

Yes, there should be an upper limit on the amount of compensation up to which the Data Protection Authority can award compensation.

10. **Can an appeal from an order of the data protection authority granting compensation lie with the National Consumer Disputes Redressal Commission?**

No. Appeals must lie only before the statutorily recognised appellate authority.

11. Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

No.

12. In cases where compensation claimed by an individual exceeds the prescribed cap, should compensation claim lie directly with the National Consumer Disputes Redressal Commission?

No. All claims with caps higher than what the DPA can award, should lie with the DPAT.

13. Should class action suits be permitted?

Yes. Especially in cases where a class of individuals suffer the same harm (i.e., discriminatory results by a decision making algorithm), they should be permitted to file class action suits.

14. How can judicial capacity be assessed? Would conducting judicial impact assessments be useful in this regard?

Judicial impact assessments would be useful. Impact assessments closely tied to what the objective of the law is, are an effective means to create a feedback loop. The DPA should be required to release an annual report with statistics of its performance. At this stage, it is difficult to propose an exhaustive list of things that the impact assessment will measure. Until more clarity is obtained on this front, the law should mandate the DPA to conduct annual performance assessments and release the statistics.

15. Are there any alternative views other than the ones mentioned above?

[●]

Chapter 4: Remedies

A. PENALTIES

1. What are your views on the above?

We agree that penalties charged to the defaulting data controller act not only as a sanction but also a deterrent against similar future conduct. As the statute is not intended to be a mere penal statute, but for the larger realignment of the data processing ecosystem to more secure standards, this should be reflected even in the punitive provisions. Penalties should be charged if there is demonstration of negligence or wilful misconduct, or if the controller's processes did not follow the due diligence set out in its codes of practice and in this statute. While the statute is centred on protecting the data subject by holding the controller accountable, it should also be fair to the controllers and encourage their participation in the new regime.

The statute should allow for mitigation of penalties charged on the data controller once the controller demonstrates that it undertook efforts to mitigate the harm caused to the data subject. However, in cases where there is wilful misconduct or lack of diligence on part of the controller, no mitigation may be allowed.

Penalising a data controller up to a percentage of its global turnover would be onerous. While stringent penalties for data breaches are important to protect the interests of the data subject, the threat of overlapping penalties on a data controller's global turnover could cause a chilling effect on the ecosystem. Therefore, it is better to tie the penalty to the domestic turnover of the data controller or to have a mechanism that says that the penalty should be a certain upper amount (e.g. Rs. 1 crore) or 4% of average domestic turnover over the last 3 years, whichever is higher. A per day fine for non-compliance could also be introduced for some of the offences.

2. What are the different types of data protection violations for which a civil penalty may be prescribed?

Civil penalties must be imposed for:

i. Non-adherence to the processing guidelines set out under the Act or ratified by the Data Protection Authority (including standards for the collection of data, lawful processing of data, compliance measures such as risk and impact assessments, lawful transfer, and disposal of data);

ii. Storage of data beyond the time frame specified by the controller to the data subject;

iii. Storage or processing of data for purposes other than those represented by the data controller;

iv. Failure to conduct both, internal and statutory, data audits;

v. Failure to comply with the recommendations of data audits;

vi. Failure to comply with a direction / order of the Data Protection Authority.

3. Should the standard adopted by an adjudicating authority while determining liability of a data controller for a data protection breach be strict liability? Should strict liability of a data controller instead be stipulated only where data protection breach occurs while processing sensitive personal data?

No. At the nascent juncture of drafting a data protection law for the first time, it might be detrimental to have a strict liability standard for offences by data controllers. Since data flows often take place between multiple data controllers, applying strict liability to all or any one of them when the breach may have been caused on account of the fault of only one of them, may be unfair. Instead, it might be advisable to evaluate the data processing standards that each of the data controllers used and determine which one or more of them was responsible for the breach. Once this has been done, the liability for the breach should be appropriately applied to those data controllers.

A strict liability standard is best derived after the ecosystem has become familiar with the statute and there is enough precedent to navigate the unintended consequences of such a standard.

4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

Any penalties calculated should be proportionate to the harm caused after the data controller has failed to remedy the data breach. While determining such penalty, the relevant authority should take into account:

i. The nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

ii. The intentional or negligent character of the infringement;

iii. Any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects;

iv. The degree of responsibility of the data controller or data processor taking into account the technical and organisational measures implemented by them; and

v. Any relevant previous infringement by the data controller or data processor. These penalties and obligations would be applicable to public authorities/government bodies which are acting as data controllers or data processors as well.

5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (of the preceding financial year as in EU GDPR) or should it be a fixed upper limit prescribed under law?

It could be both, a prescribed upper limit or 4% of the average domestic turnover of the defaulting data controller of the previous 3 years, and whichever figure is higher could be the penalty that the controller must pay. The mitigation efforts undertaken by the data controller should also factor into the final penalty it is called upon to pay. In the case of violations that have cross border implications, it must be kept in mind that global companies will have to deal with penalties applied by the various jurisdictions within which they operate. Accordingly, it may be appropriate to limit the penalty to the turnover of those organisations within India rather than use a global turnover criteria.

6. Should the turnover (referred to in the above question) be the worldwide turnover (of preceding financial year) or the turnover linked to the processing activity pursuant to a data protection breach?

While it is better for the penalty payable to the turnover linked to the processing activity in question, this might not always be possible to calculate. In these circumstances, the civil penalty must be charged to the controller's domestic turnover.

7. Where civil penalties are proposed to be linked to a percentage of the worldwide turnover (of the preceding financial year) of the defaulting data controller, what should be the value of such percentage? Should it be prescribed under the law or should it be determined by the adjudicating authority?

The upper cap for civil penalties could be prescribed under the law. As proposed under the GDPR, 4% of average domestic turnover over the last 3 years could be a reasonable figure.

8. Should limit of civil penalty imposed vary for different categories of data controllers (where such data controllers are categorised based on the volume of personal data processed, high turnover due to data processing operations, or use of new technology for processing)?

No. The civil penalty imposed must be related to the nature of the data breach, the demonstrability of the harm caused, and the sensitivity of personal data that is the subject of such breach and the harm caused. The harm caused may not be related to the volume of personal data, turnover or the use of new technology. A small company may process highly sensitive personal data and therefore, imposing varying limits may not be practical. The statute should only prescribe an upper limit of the penalty payable. The Data Protection Authority should have the discretion to assign the specific amount payable by the erring data controller. Additionally, the Data Protection Authority should be vested with the power/discretion to award a lesser penalty if the data controller makes a prima facie case for such pardon.

9. Depending on the civil penalty model proposed to be adopted, what type of factors should be considered by an adjudicating body while determining the quantum of civil penalty to be imposed?

Any penalties calculated should be proportionate to the harm caused after the data controller or processor has failed to remedy the data breach. While determining such penalty, the relevant authority should factor in:

i. The nature, gravity and duration of the infringement taking into account the nature, scope, or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

ii. The intentional or negligent character of the infringement;

iii. Any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects;

iv. The degree of responsibility of the data controller or data processor taking into account the technical and organisational measures implemented by them; and

v. Any relevant previous infringement by the data controller or data processor.

10. Should there be a provision for blocking market access of a defaulting data controller in case of non-payment of penalty? What would be the implications of such a measure?

No. First of all, such a provision might lead to questioning the jurisdiction of the Data Protection Authority to restrict the controller from operating in a free market. Secondly, such a provision might be too invasive to innovation and might adversely impact investments.

11. Are there any alternative views on penalties other than the ones mentioned above?

None of the penalties detailed in this Chapter should apply to public authorities/government bodies which are acting as data controllers or data processors. There should be a mechanism for determining the penalties

applicable in such cases and attributing appropriate deterrent punishment for government bodies responsible for the breach of the data protection law. This is similar to the approach outlined in the GDPR. A fine may not suffice as an adequate deterrent to a government body for breach of the data protection law.

B. COMPENSATION

1. What is the nature, type and extent of loss or damage suffered by an individual in relation to which she may seek compensation under a data protection legal regime?

The individual data user may seek damages for harms caused to him. The statute should include a list of harms such as financial harm, reputational harm, harm due to discrimination and harm due to restriction of choice. The harm should also include indirect harm caused to a data subject as a result of negligence or default on the part of the data controller. Indirect harm is said to have occurred to a data subject if he is able to demonstrate it in any manner. For instance, indirect financial harm may occur to the data subject even if he has not suffered any financial losses but is still able to quantify the harm caused to him.

2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?

A number of factors should be considered while calculating compensation for breach of data protection obligations:

i. Whether the breach was intentional or negligent;

ii. Whether the harm caused to the data subject was material or non-material;

iii. If harm caused was material, the financial impact of the harm;

iv. Whether the breach is capable of being remedied;

v. Measures adopted by the data controller to minimise the impact of the breach; and,

vi. Other factors as may be determined by the adjudicatory authority.

3. What are the mitigating circumstances (in relation to the defaulting party) that may be considered while calculating compensation for breach of data protection obligations?

The following mitigating circumstances could be considered in a case for compensation for losses arising out of breach:

i. If the data controller has shown that the breach occurred due to unforeseen circumstances or due to a fault beyond the controller's power;

ii. If the controller has arrested the harm from continuing or has reversed any portion of the harm caused to the subject; and

iii. The extent of harm that the data user has suffered.

4. Should there be an obligation cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to data protection breach by such data controller (without the individual taking recourse to the adjudicatory mechanism)? What should constitute significant harm?

No. An adjudication process is necessary to ensure that the data controller does not use compensation as a shield. Allowing such a provision would raise concerns of arbitrariness in both, informing the data user of a harm and also in compensating him justifiably. It is also a principle of natural justice that no one can be a judge in his own cause – a data controller cannot sit in judgment of its own default as this might be detrimental to the data subject. Some form of adjudication or third-party intervention is necessary to ensure that the data controller does not use its power to compensate the harmed subject as a shield.

5. Are there any alternative views other than the ones mentioned above?

The data protection law should, in its design, encourage data controllers to remedy breaches. When a breach can be remedied effectively and no harm has been caused to the data subject, the law should not require the data controller to pay compensation to the data subject.

C. OFFENCES

1. What are the types of acts relating to the processing of personal data which may be considered as offences for which criminal liability may be triggered?

Criminal liability should not be imposed for offences under the data protection law. If a breach of the data protection law also qualifies as an offence under the Indian Penal Code, 1860, or under other statutes that impose criminal sanctions, then criminal liability as provided under such statutes should apply. The data protection law itself should not impose additional criminal liability.

2. What are the penalties for unauthorised sharing of personal data to be imposed on the data controller as well as on the recipient of the data?

Data controllers should be liable to pay compensation to persons affect by unauthorised sharing of personal data and should be directed to cease further sharing of data. The quantum of compensation should be determined using the factors provided in response to question 2 of Chapter 4, section B, Part IV of this White Paper.

3. What is the quantum of fines and imprisonment that may be imposed in all cases?

We recommend that no fines or imprisonment be imposed. The data protection law should require the data controller to provide compensation to affected persons and to remedy breaches within a reasonable time.

4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

We do not believe that criminal sanctions like fines or imprisonment should be imposed. Compensation should be linked with the harm caused to the data subject and not with the nature of data. Material harms should be provided with a higher compensation than non-material harms irrespective of the nature of data involved in the offence.

5. Who will investigate such offences?

The Data Protection Authority will investigate these offences.

6. Should a data protection law itself set out all relevant offences in relation to which criminal liability may be imposed on a data controller or should the extant IT Act be amended to reflect this?

The data protection law should not provide for criminal liability. Criminal liability should only be imposed if the act/omission of the data controller also constitutes an offence under other penal laws.

7. Are there any alternative views other than the ones mentioned above?

The offences segment should apply strictly to the government. In the interest of protecting highly sensitive personal data that the government is privy to, the data protection law must attach similar criminal liability to the government as it does to data controllers who are private entities.

REFERENCES

1 Rahul Matthan, *Beyond Consent: A New Paradigm for Data Protection*, Takshashila Discussion Document, 2017-03"

2 Article29 Newsroom – News Overview – European Commission, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, (accessed February 4, 2018)

3 Data Protection and Journalism, https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, (accessed February 9, 2018)

4 Charles Huggins v Melba Moore & The Daily News 94 NY2d 296 (1999).

5 O'Grady v Superior Court 44 Cal Rptr 3d 72 (Ct App 2006).

6 Ibid.

7 Taylor Wessing, An Introduction to Subject Access Rights, https://united-kingdom.taylorwessing.com/globaldatahub/article_intro_sar.html, (accessed February 9, 2018)

8 SOAS University of London, https://www.soas.ac.uk/infocomp/dpa/access/, (accessed February 10, 2018)