White Paper on Data Protection Framework for India

iSPIRT Response

About iSPIRT

iSPIRT (Indian Software Product Industry Round Table) is a think tank for the Indian software Product Industry. Our mission is to build a healthy, globally-competitive and sustainable Indian Software product industry.

We believe that India is at a unique tipping point where only a fraction of its users have gone online, and a majority are yet to do so. It is important we build the right set of protections and empowerments for these users as they enter the digital world.

It is equally important not to limit our thinking to simply "protection" of data. We must also question how we can "empower" users, who will be data rich before they are economically rich, to use their data for their own benefit. iSPIRT has presented some of its views on how to Protect and Empower in response to the questions posted by Srikrishna Committee below.

Table of Contents

Part I: Context Setting: India In A Digital World

Introduction

As the world hurtles towards a data-driven, digital-first future there is a real opportunity for India to emerge as a leader in driving policy that simultaneously empowers and protects the individual. With this vision for India in mind, the iSPIRT community has engaged deeply with the White Paper of the Committee of Experts on a Data Protection Framework for India ("Consultation Paper"). We have developed six overarching core principles which we believe are most crucial to ensure the dual goals of a citizen-centric approach to data protection, and data empowerment for the individual. These six principles are as under, and frame our response to the Consultation Paper:

1. **Restoring balance between the individual and the data controller**

The law must use principles of accountability and empowerment to balance the inherent positional inequality between the individual and the data controller. This can be achieved by first and foremost ensuring that the building blocks of India's data protection law are centered around safeguarding individual privacy and data, and mitigating against any potential or existing privacy harms. Placing the individual at the centre of India's proposed law increases the potential for it to be adaptable and future-proof, capable of encompassing emerging technologies and data use cases as they evolve.

2. **Data should be used to empower and not for harm**

Championing transparency increases the likelihood for the law to be carried across various jurisdictions and in turn drives user consent that is both informed and meaningful. Once individuals are able to easily comprehend and feel empowered to exert a level of control over their personal data, their ability to harness the potential of this data for their own economic benefit (and hence that of the nation) increases. Conversely, in cases where data sharing has already occured, a higher onus must be placed on the data controller to inform the user about such activities.

3. **Individuals have rights over their data**

iSPIRT advocates for a "rights-based model" for data ownership as guided by three principles: accountability, autonomy and security. Together these principles will ensure that individuals are provided a right to fair treatment, right to information, right to port (transfer) data from one data controller to another, right to restrict processing, and right to the security of his/her data. Classifying data types, whether sensitive, personal, etc. should take into account social implications and norms in order to best protect the individual under all possible associations.

4. **Data controllers must be accountable**

Regardless of data type, whether it be personal or even sensitive, the law must hold data controllers accountable for any and all privacy harm caused by their actions. The "data

controller" is the entity that has legitimately been provided control of the data, and hence determines the primary purpose of the data collection and therefore also holds primary responsibility for upholding an individual's right to privacy and rights to protection against harms via data.

5. Times of disruptive change require agile regulators

The law should empower regulators by providing a framework with a set of principles which are timeless, along with a mechanism that can change with the times and a context to provide suitable intervention. Regulators should have the flexibility to oversee all data processing activities that are primarily digital in nature. In cases where the law provides exemption, such as data collection for purposes having a well-defined and overwhelming public benefit, the regulator should be properly equipped to evaluate and adapt accordingly.

6. Balancing India's needs for privacy, transparency and development

Overall, the law should strive to create a balance between protecting personal privacy, providing transparency and accountability for institutions (including government), and ensuring development, growth, and empowerment for the individual and other market participants. By harmonizing various existing laws, balancing surveillance efforts, and striving for a practical approach to balancing privacy and development, particularly among social sector players, Data Protection laws can ultimately drive sustained growth.

Finally, the iSPIRT community is encouraged by the proposal of innovations such as the Trust Score and Consent Dashboard. As a community we are highly optimistic for India's adoption of a visionary and comprehensive Data Protection Law and thank the Justice Srikrishna Committee for their efforts in spearheading the same. We look forward to a continued engagement in bringing these policies to the forefront.

Please find below our formal reply to the Call for Responses on the White Paper.

1. It is important that the preamble to the law recognize that we are moving into a world with a lot of data. As a result, it is important that this be used for the empowerment of the people - both individually, and as a society. An equally important aim is to prevent harm to the individual from the changed circumstances.

2. The law must also recognise that these changes are accelerating, and that it would be impossible at this time to cover everything, and hence a framework is required with a set of principles, along with a mechanism that can change with the times.

3. Many elements of consent and breach are related to the contract between the user and the service provider which is to the disadvantage of the user. It is important that data protection, privacy, and empowerment of data principles are created to restore this balance. This applies more so when the service provider is a public entity, and there may be no explicit contract.

Part II: Scope & Exemptions

Part II Chapter 1: Territorial & Personal Scope (Jurisdiction)

Questions

1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India should be?
    - Data protection law should be centered around the person, their data, and the privacy harms, both real and potential caused to them.
    - For India's data protection law to apply, there must be a link to the Indian jurisdiction. One or more of the following being under Indian law should mean that it is covered by this law:
        - The person (subject / whose data is being protected)
        - The activity which generates the data
        - Data processing, or the privacy harm
    - It is possible that the Union government may have to work on international forums to create a new International convention for this purpose. An example of an international treaty which addresses data protection across different countries is Treaty No. 108 created by the Council of Europe[1].
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?
    - To the fullest extent possible.
    - Penalties must be prescribed, and if not enforceable, alternate penalties like restricting market access must be specified.
3. While providing such protection, what kind of link or parameters or business activities should be considered? Alternatives:
    - The person (data subject), the activity, or the harm should occur within India's jurisdiction. Business / commercial intent is not required.
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?
    - Allow for escalation clauses.
    - Allow for restricting market access.
    - Allow for using treaties (bilateral or multilateral treaties) for redressal.
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?
    - In addition to the data controller, the law must provide for private remedies against deliberate attacks on individuals and/or systems.

[1] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Part II Chapter 2: Other Issues Of Scope

Questions

1. What are your views on the issues relating to applicability of a data protection law in India in relation to
    - (i) natural / juristic persons;
        - Data relating to natural persons should be protected by the law.
        - However, this protection must extend to juristic persons as well, to the extent that this data could be traced (or there is a reasonable likelihood that it may be traced) to a natural person.
    - (ii) public and private sector; and
        - The provisions of the proposed data protection law must apply uniformly to the public as well as the private sector, and to governments (international, central, and state governments included).
        - The legitimate interests of the State may be protected through relevant exemptions such as those recognised by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India and Others.[2]
        - In the case of regulated entities, including in sectors such as finance and telecom, subordinate sector specific regulation should be issued by the appropriate regulators.
        - Any data protection authority proposed to be established under this law should be independent and vested with judicial powers, and should not be subordinate to other sectoral, independent regulators.
    - (iii) retrospective application of such law?
        - The law should be implemented in a phased manner, with public awareness preceding penalties. However, the law must specify how to deal with data that has been collected in the past, and is in the control of data controllers.
2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?
   Alternatives:
    - See our response to Q1 above.
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:
    - 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 other provisions. These Exemptions must be questionable/audit-able/revocable via defined process. The law may also propose time bounded / purpose limited exemptions.

[2] 2017 (10) SCALE 1. Hereafter referred to as "Puttaswamy".

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?
    - The law will apply to processes such as storing and sharing, irrespective of when data was collected while some requirements such as grounds of processing may be relaxed for data that was collected in the past. For data collected in the past, data controllers must be allowed to continue to use it as they were doing prior to the law but they should also be restricted from sharing it afresh across organisational boundaries as the law restricts it for any data. Users must be protected from harm caused to them from loss of previously-collected data and from processing of previously-collected data.
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, time must be provided for compliance. This may be sector specific.
6. Are there any other views relating to the above concepts?
    - A lot of data has been collected under different legal frameworks by public authorities, and under 'contract' by private authorities. It is important that there is a public clarification of how these will be harmonized under the new law irrespective of when it was collected, with residents having an option to opt out of data processing / sharing. If opt-out is not feasible then the restrictions imposed on the data collector should be greater.

Part II Chapter 3: What Is Personal Data

Questions

1. What are your views on the contours of the definition of personal data or information?
    - Personal data should include Identified data, and reasonably identifiable data.
    - The following aspects may be considered while determining the contours of the definition of personal data:
        i. Whether the information is 'public': For instance, if a photograph is taken on the street, with people in the image. While this is not private, it may be personal. Perhaps the people in the photograph are not identified, but they could be identifiable.
        ii. How intimate is the information: For instance, a person's browsing history on a website (or a collection) may not have her name, or identity information, and neither may the person be readily identifiable. Yet, this data represents behaviour and interests, which are very personal and intimate. This data must be protected.
2. For the purpose of a draft data protection law, should the term "personal data" or "personal information" be used?
    - Either “personal data” or “personal information” may be used, as long as the same term is used consistently across the data protection law. International practices indicate the use of either term as acceptable - while the EU GDPR uses “personal data”, the laws of Australia, Canada and South Africa use “personal information”.
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?
    - Yes, facts, opinions and assessments all qualify as 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?
    - Yes, it is important that the definition of personal data focus on identifiability of an individual. “Reasonably identifiable” is the preferred standard.
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.]
    - The law should let anonymized data be outside the purview of personal data.
    - The law should also set a high bar on what constitutes anonymised data: simply disguising identity from data is not enough to render it anonymised. An

individual's data should be regarded as anonymised only if nothing about the individual's identity can be inferred from that data and the likelihood of such inference taking place in the future (given reasonable amount of computing resources) is small.
    - Pseudonomized data should be subject to the "reasonably identifiable" standard under the law.
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?
    - Both "identified" and "reasonably identifiable" data constitute personal data and should be treated similarly. The standard must be "reasonably identifiable".
7. Are there any other views on the scope of the terms "personal data" and "personal information", which have not been considered?
    - The law must hold data controllers accountable for the privacy harm caused by their actions, even if the data itself is not sensitive, or even personal.
    - In addition, the law could extend the limits of protection based on whose data it is. For example, for a child, any identifiable data should be considered as sensitive/private and treated according to those rules. This ensures that children are protected at levels far greater than others.

Part II Chapter 4: Sensitive personal data

Questions

1. What are your views on sensitive personal data?
   Sensitive Personal Data or Information ("SPDI") should be defined by intimacy, expectations of privacy, as well as potential harm that may befall the individual whose data it is. Social norms may play a role in establishing expectations of privacy. . For example, while some might consider data related to income and wealth to be sensitive personal information, in addition to those listed in the provisional views of the Consultation Paper.[3]

2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? Eg. 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.]
   The law **should not** identify a set of data as sensitive. However, sectoral regulators may determine some kinds of information as sensitive..

[3] Consultation Paper, page 43, para 4.3

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

   SPDI is not absolute. There is a requirement for public disclosure of certain information (for instance, wealth of electoral candidates), and the fact that such information is SPDI should not be a bar on such necessary public disclosure. Similar expectations may be present while dealing with public health, and contagious diseases. On the other hand, sensitivity is required in dealing with SPDI - there are cases where people have not wanted to get treatment for HIV due to fear of having to register with a real identity.

Part II Chapter 5: What Is Processing

Questions

1. What are your views on the nature and scope of data processing activities?
    - The law should cover data processing activities which are (partially or entirely) digital (electronic) in nature.

2. 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?
    - The law cannot cover all possible operations on data, nor should it attempt to do so.

3. 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:
    - Limit the scope to automated or digital records only
4. Are there any other issues relating to the processing of personal data which have not been considered?
    - Linking of data obtained from multiple sources should be considered in processing.

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

Questions

1. What are your views on the obligations to be placed on various entities within the data ecosystem?
    - Primary accountability must rest with the data controller.
2. Should the law only define “data controller" or should it additionally define 'data processor"?
   Alternatives:
    - The law must use the two concepts of “data controller" and 'data processor" to distribute primary and secondary responsibility for privacy. A data controller collects information from an individual and exercises control over it, including determining the manner of the processing. A data processor receives information from the data controller and processes it based on instructions received from the data controller.
3. How should responsibility among different entities involved in the processing of data be distributed?
   Alternatives:
    - Making data controllers the key owners and making them accountable[4].
    - Use of contractual law for providing protection to data subject from data processor.
4. Are there any other views on data controllers or processors which have not been considered above?
    - Liability must depend on harm / potential harm caused. Criminal liability must be provided for 'reckless' use.
    - The size of operations of the data controller may also be a relevant factor to be considered while determining liability.
    - Allow for piercing corporate contracts / veils, such that businesses do not outsource liability to smaller firms.
    - Data subjects must have the right to sue data controllers and data processors for ham suffered. Data subjects be allowed to sue data controllers with whom they have a business relationship, as well as controllers, and processors who have their data, and caused them harm.

[4] The owner must be the individual whose data it is. However, it is in the custody of the data controller, who must be accountable for their conduct and downstream entities on the data trail.

Part II Chapter 7: Exemptions for Household purposes, journalistic and literary purposes and research

Questions

1. What are the categories of exemptions that can be incorporated in the data protection law?
    - Exemptions must be provided for in 2 situations only:
        i. A well defined, and sufficient public benefit, or
        ii. To prevent significant hardship for existing practices.
    - Where data is collected, and processed under separate laws, those uses may be recognized as exemptions, until such time as the laws are harmonized. For instance,
        i. The census is done under a certain law.
        ii. Electoral rolls are prepared under certain laws
        iii. Banking confidentiality laws apply to bank transactions
        iv. Telecom licensing agreements apply to telecom data.
        v. Medical data regarding communicable diseases (is there a law?)
    - Where no law law exists, but there is a precedent / custom, it should be considered for formalization under the newly created authority.
    - Where the exemption is provided for, the exempt entity must inform the data protection authority (perhaps register with it), and provide periodic reports.
    - Where the exemption is provided, the data must be held securely, and must not be shared without the consent of the individual whose data it is, unless such subsequent sharing is also exempted.
    - The publication of statistical data should be encouraged by all data controllers.
    - The publication of anonymous data should be encouraged by all public data controllers.
    - A legal requirement must be created for a data controller to share data about a community with that community. Such data may be anonymised for the purpose of sharing. For instance, a taxi company may be compelled to share anonymised trip information with the city, so that the city can do a better job of planning, and traffic management.

2. What are the basic security safeguards / organisational measures which should be prescribed when processing is carried out on an exempted ground, if any?
    - Where the exemption is provided for statistical purposes, or for research purposes, the data should be maintained in a virtual data room[5], which can be used to answer various questions, but cannot reveal data about individuals.

[5]Virtual data rooms enable multiple entities to exchange data with each and to process such data in such a manner that ensures that no secret information held by any of the entities is revealed to other entities. Such services can be provided by a trusted service provider or be implemented using modern cryptographic techniques.

- Where individual data is used, all identifiers should be masked, or replaced by a hashed equivalent for most purposes. Going beyond the masked data should be done under very controlled conditions.
- Penalties for breaches should be high.

Domestic / Household Processing

1. What are your views on including domestic / household processing as an exemption?
    - See response to Q1 in this chapter.
    - An explicit exemption may not be required for this.
2. What are the scope of activities that will be included under this exemption?
3. Can terms such as “domestic” or "household purpose" be defined?
    - 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?
    - See response to Q1 in this chapter.
    - These activities are expected to result in public benefit. As a result, exemptions may be provided, where the results are available for the public.
2. Can there be measures incorporated in the law to exclude activities under this head which are not being conducted for a bonafide purpose?
    - Providing for these exclusions may be harder to do via definitions. However, significant penalties may be associated with those found misusing these exemptions.
3. Will the exemption fail to operate if the research conducted in these areas is subsequently published / or used for a commercial purpose?
    - The publication of the research is the public benefit. However, granular data may not be published. The fact that some research may lead to commercial benefit is not relevant for the law, as long as the citizens are protected from harm.
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?
    - These activities are expected to result in public benefit, and must be exempt.
    - All investigations of crime, and for prevention of crime, deal with personal information - demographic, transactional, and behavioral, and result in moral judgements, etc.
    - While the activities may be exempt, disclosure of such information may be highly prejudicial - this should be done only through a judicial process.
    - For instance, evidence may be presented in a court of law. This must be exempt.

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?
    - In a fast changing world, it is hard to predict these. Significant latitude must be provided, with significant repercussions for misuse.
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?
    - In a fast changing world, it is hard to predict these. Significant latitude must be provided, with significant repercussions for misuse.
4. Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail?
    - Yes, a review mechanism is a must. Every access to personal data must be logged by the data controller, and made available to the data protection authority.
5. How can the enforcement mechanisms under the proposed law monitor / control processing of personal data under this exemption?
    - All access and processing must be logged and audited.
6. Do we need to define obligations of law enforcement agencies to protect personal data in their possession?
    - Yes
7. Can the Data Protection Authority or / and a third-party challenge processing covered under this exemption?
    - Yes
8. What other measures can be taken in order to ensure that this exemption is used for bona fide purposes?
    - Periodic review, and statistical disclosure is important.
9. Are there any other views on these exemptions?

Additional Exemptions

1. Should 'prevention of crime' be separately included as ground for exemption?
    - These activities are expected to result in public benefit, and must be exempt.
    - Significant latitude must be provided, with significant repercussions for misuse.
    - A review mechanism is a must. Every access to personal data must be logged by the data controller, and made available to the data protection authority.
    - Such an exemption may be made visible to the data subject after a fixed period of time, and the subject must be allowed to file a complaint for misuse under this act.
2. Should a separate exemption for assessment and collection of tax in accordance with the relevant statutes be included?
    - Significant latitude must be provided, with significant repercussions for misuse.
    - The relevant statutes must be harmonized with the data protection law.

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

Part II Chapter 8: Cross-Border Flow of Data

Questions

1. What are your views on cross-border transfer of data?
    - It is a reality in today's world. However, the data protection authority should be able to pro-actively regulate this.
    - The individual should have the choice as well. So, if data is moving cross border, they should be informed.
2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, should the adequacy standard be the threshold test for transfer of data?
    - An adequacy framework should be developed for cross border data flows. It is important that the country consider the establishment of mutual / multi-lateral treaties with regards to data. This will require the maturity of these frameworks.
3. Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfils the test for transfer?
    - User consent for this data transfer should be the over-riding factor.
4. Are there any other views which have not been considered?

Part II Chapter 9: Data Localisation

Questions

1. What are your views on data localisation?
    - Agree with the provisional views.
    - Flexibility must be provided to the data protection authority

Part II Chapter 10: Allied Laws

Comments are invited from stakeholders on how each of these laws may need to be reconciled with the obligations for data processing introduced under a new data protection law.

- The proposed privacy bill should acknowledge the set of laws that already exist, and define the treatment of data.
- However, each of these laws should be revisited, and harmonized with the new law.
- In particular, this law must be harmonized with:
    - **Right To Information Act**: The privacy protection, and the transparency provisions in various laws could result in conflict. This must be explicitly considered.
    - **Representation of Peoples Act**: The privacy provision, and the public disclosures required could result in conflict.
    - Additional applicable acts, agreements, and regulatory agencies with whom to harmonize: Banking Secrecy Act, licensing agreements with telecom operators, Credit Information Companies Act, Census, Unique Identity Authority of India Act, Information Technology Act, RBI.

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

Part III Chapter 1: Consent

Questions

1. What are your views on relying on consent as a primary ground for processing personal data?
   Alternatives:
   - Consent will 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?
   - Yes, consent should be unambiguous and freely given. However, In the event that the data is required for the provision of the service, it may result in the denial of the service (which should be pointed out).
   - Essential services present a complication. Since the service is essential, the user may have to provide information, and her consent cannot be considered to be freely given. The responsibility of the data collector / processor must be higher.
   - Consent is often bundled, and the data protection authority should be able to adjudicate on the reasonableness of these bundles - for the public sector, and also the private sector.
3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?
   - An informed consent by a user naturally leads to a reduced liability for a data controller in case of any unwanted incident. However, given the reality of consent fatigue, we have a situation of reduced liability for the data controller and no significant enhancement in awareness of the user. In addition, there is no mechanism where the industry is aligned and incentivised to invest resources in reducing consent fatigue and enhancing user awareness. Thus, there is a case for the law to link reduction in consent fatigue to reduction in liability for the data controller. While we understand that currently there may not be creative solutions to measure and solve the consent fatigue problem, creating an industry aligned structure will commit resources (to reduce liability with reduced consent fatigue) to a win-win outcome.

4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?
   - Data controllers should be allowed to make context-specific determinations, and this should be monitored by the data protection authority.

5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?
    - This may be true in some business domains but in general, it is not true. The data protection authority (DPA) or individual regulators can define cases of exceptions wherein the consent capture process is allowed to be simplified.
6. Are there any other views regarding consent which have not been explored above?
    - Consent should be required for all situations where personal data crosses national borders, as well as corporate borders.
    - Consent should have a provision for revoking based on automated time bound or direct action revocation. This provides the data subject control over their actions and ability to revoke permissions if required to protect from new harms. This is also useful to re-establish a child's consent as and when they become adults as per law.

Part III Chapter 2: Child's Consent

Questions

1. What are your views regarding the protection of a child's personal data?
    - Agree with the provisional view that a child's consent is not valid. Mechanisms must be devised to take the consent from an adult with a legally established relation with the child (parent, legal guardian, teachers-for marksheet, attendance etc).
    - However, a view must be formed on the potential harms to the child before regulating this differently. In particular, profiling and marketing are not harmful activities by themselves. It is what is done with the profile, or the product that is being marketed which makes them potentially harmful.
    - Also, this type of consent must be revisited when the child turns 18 or older. And provisions made for revocation of consent if the child (then adult) so wishes.
2. Should the data protection law have a provision specifically tailored towards protecting children's personal data?
    - Only to state that consent needs to be from a responsible adult, and that the data protection authority should continue to stay mindful of this aspect.
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?
    - The law should do this (i.e. provide an age bar of less than 18) only as long as it remains compatible with other laws. For example, most contracts signed by minors are not regarded as valid unless accompanied by an adult's signature. The same should be true for consent.
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, with appropriate controls for transparency and purpose limitation (e.g. informed parental consent) and accountability, there is no need for such a strong measure.
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 is onerous for the data controller and will create usability barriers for adult users.
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:
    - This can be obviated by seeking parental consent

7. How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required?
    - The process for capturing parental consent should be secure. Consent should be closely tied to the parent's identity (e.g, via a KYC), so that it is difficult for any other individual to provide consent on their behalf.
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?
    - It could be effective but it may be quite hard to implement.
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?
    - The key is to prevent a child from coming to harm due to privacy violations. If the service is not suitable for children, that must be covered by other laws. However, each service must carry out their own risk assessment for privacy harms to children, and to find ways to obtain meaningful consent.
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?
    - Yes. The key is to prevent a child from coming to harm. If data controllers can identify the user, they can certainly figure out if it is a child, and if the consent is valid.
11. Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?

Part III Chapter 3: Notice

Questions

1. Should the law rely on the notice and choice mechanism for operationalising consent?
    - Yes
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?
    - Yes. Govt. data controllers can be mandated to use specific language, and standardize notices.
3. Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?
    - The Data Protection Authority should have the capability to bring in subordinate regulation to deal with the effectiveness of notices. This is likely to change with time, technology, and design.
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:
    - No form based requirement pertaining to a privacy notice should be prescribed by law.
5. How can data controllers be incentivised to develop effective notices?
   Alternatives:
    - Assigning a “data trust score".
    - Providing limited safe harbour from enforcement if certain conditions are met.
6. If a “data trust score" is assigned, then who should be the body responsible for providing the score?
    - Multiple private sector entities should be allowed to build these scores, and market them.
    - The Data protection authority can license these score providers based on various conditions.
7. 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?
    - A technology solution is required to regulate consent & sharing of data. A technology based solution is required for users to be able to identify where their personal (identified) data resides, and where they have provided consent. This solution should provide for logging, which can be audited, and also be used to create such a dashboard.
    - The Data Protection Authority should propose creating such a framework and ensure that all registered data controllers abide by this framework.

- A single, centralized entity is not required for this purpose, but interoperability between different entities that run / manage consent dashboards is needed.

8. Are there any other alternatives for making notice more effective, other than the ones considered above?
    - Notice must be required for all data where the user is identified. This notice must be provided at the time of 'identification', or of creating the data.
    - Some standardization will be required for the types of use, that the data will be put to.

Part III Chapter 4: Other Grounds of Processing

Questions

1. What are your views on including other grounds under which processing may be done?
    - We agree with most of the provisional views i.e. that a ground other than consent is required. However, it should be rarely used, and each such use must be logged - for the citizen to look at, and for subsequent audit.
    - This subsequent audit will allow a citizen to take such a use to court (to the DPA), and can lead to significant repercussions for misuse.
2. What grounds of processing are necessary other than consent?
    - Compliance with the law
        i. Includes grounds such as investigations into crime, national interest,.
    - Performance of Contract (with the Individual)
    - Emergency situation
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:
    - Determination of lawfulness may be done by the data controller subject to certain safeguards in the law.
4. Are there any alternative methods to be considered with respect to processing personal data without relying on consent?
    - The processing activity must be logged, and available for audit by the user, and by the DPA.
    - Consent is not applicable when the data is not 'identified'. However, if the data is 'identifiable', the controller must take significant care to prevent harm to the data subject.

Part III Chapter 5: Purpose Specification and Use Limitation

Questions

1. What are your views on the relevance of purpose specification and use limitation principles?
    - Purpose Specification, and Use Limitations are valuable elements in the consent framework. A user only consents to data collection, and processing with these in mind. Changing these arbitrarily (one-sided) based on later developments is not acceptable - this invalidates consent, and must not be permitted.
2. How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies?
    - They must not be allowed. Companies should go back to the user.
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 individual to whom the data belongs.
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:
    - No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators.
5. Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?
    - Sectoral regulators may specify specific purposes, and use limitations, which the data controller can refer to in the notice - thus simplifying the communication with the user.

Part III Chapter 6: Processing of Sensitive Personal Data

Questions

1. What are your views on how the processing of sensitive personal data should be done?
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?
3. What additional safeguards should exist to prevent unlawful processing of sensitive personal data?
   Alternatives:
   - 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.
   - 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.
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?
   - No. Let the sector specific regulator decide the specifics, the law can provide the principles and directions.
   - In case of data pertaining to more than one sector (e.g., medical insurance) a union of individual sector rules should apply.
5. Are there any alternative views on this which have not been discussed above?

Part III Chapter 7: Storage Limitation and Data Quality

Questions

1. What are your views on the principles of storage limitation and data quality?
    - Mostly agree with the provisional views.
2. On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?
   Alternatives:
    - The individual
3. How long should an organisation be permitted to store personal data? What happens upon completion of such time period?
   Alternatives:
    - Data may be retained in anonymised form, and for this the same principles of anonymisation should be followed as used for anonymous data sharing.
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?
    - The model of proportional regulation may be used, where the restrictions are higher based on the size of the entity (in terms of number of users, business, etc.) Larger businesses pose more systemic risk, and must be monitored closely. All businesses should be monitored for customer harm, grievance redressal, etc.
5. Are there any other views relating to the concepts of storage limitation and data quality which have not been considered above?

Part III Chapter 8: Individual Participation Rights-1

Questions

1. What are your views in relation to the above?
    - It is important that the law reflect the fact that the data controller is but a custodian. In the event that the data is co-created through transactions on the data controller's systems, the individual still has a right to this information - which includes the right to confirm, access, rectify, and share.
2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?
    - There is a classification of information, which ranges from that provided by the individual directly (e.g., filling out a Web form with personal information), indirectly (e.g., carrying out a transaction in their bank account), or is the result of observation, and the application of intelligence by the data controller (e.g., an app tracking typing patterns of the user and using that to build a predictive model of typing to help the user type faster). Restrictions, and costs may depend on these categories.
3. What should be the scope of the right to rectification? Should it only extend to having inaccurate data 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?
    - Facts can be rectified, opinions not.
    - The right may include going to the court.
4. Should there be a fee imposed on exercising the right to access and rectify one's personal data? Alternatives:
    - There should be no fee imposed.
5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?
    - Yes. For data available online, it should be very quick (1 day), however, for other data, it should be 1 to 3 weeks.
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?
    - It may not be technically feasible. However, the DPA should encourage all data controllers and data processors to move towards that state. Incentive mechanisms (like trust scores) could be used to encourage data controllers/processors to be open about their algorithms.
7. What should be the exceptions to individual participation rights? [For instance, in the UK, a right to access can be refused if compliance with such a request will be impossible or involve a disproportionate effort. In case of South Africa and Australia, the exceptions vary depending on whether the organisation is a private body or a public body.]
    - Since the raw, factual data belongs to the individual, there should be no exceptions.

- Exceptions may be prescribed for 'opinions'

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

Part III Chapter 9: Individual Participation Rights-2

Questions

1. What are your views in relation on the above individual participation rights?
    - Mostly agree with these views on portability and processing.
    - For automated decisions, the focus should be on the potential harm, and amelioration of that harm.
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?
    - India should adopt the right to data portability completely.
    - The right to restrict processing may depend on the contract with the user.
3. Should there be a prohibition on evaluative decisions taken on the basis of automated decisions ?
   Alternatives:
    - There should be a right to object to automated decisions as is the case with the UK.
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 has been significant changes in technology, which will require a second look at this right.
    - It is possible that this can be addressed through prevention of harm to the individual through their data.
5. Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations?
    - Direct marketing, and other activities could be addressed in some sectors, but for the rest, some guidance must be provided.
    - The common guidance could be through accountability for harm.
6. Are there any alternative views in relation to the above which have not been considered?

Part III Chapter 10: Individual Participation Rights 3- Right to be forgotten

Questions

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 should be explicitly addressed in the data protection law. However, **it may be very limited**, and allowed to adapt through jurisprudence, and regulation.
    - The right applies to facts involving the 'subject'. It cannot be used to remove an 'opinion'. As we understand it, in the EU, this appears to be focused on how these facts are reported in public records, news, and on various websites; and is implemented by ensuring that search engines are barred from displaying these specific results.
2. Should the right to be forgotten be restricted to personal data that individuals have given out themselves?
    - Yes, this could be included in the bill.
3. Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?
    - Yes, it generally applies to data which is not private, while individual participation rights apply mostly to private data, which is in the custody of a data controller. For instance, expunging a criminal record which happened a long time ago from all newspapers, and online news.
4. Does a right to be forgotten entail prohibition on display / dissemination or the erasure of the information from the controller's possession?
    - It should be a prohibition on display, as well as continued normal internal use of the information in the possession of the controller.
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 balancing should be on the DPA / Courts. The penalty size may depend on the privacy harm that is caused, and the circumstances of the data being erased.
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)?
    - The right itself should be treated as a special exemption, and exercised through a court, or the DPA process.
7. Are there any alternative views to this.
    - The right to be forgotten is an innovation to protect users from the harm caused by the infinite memories now being created through digital means. It is similar to the courts sealing records of juveniles, or placing limitations on reporting of certain cases.

- It is important that this right be exercised in a controlled manner, under court control, till sufficient jurisprudence is created.

Part IV Regulation And Enforcement

Part IV Chapter 1: Enforcement Models

Questions

1. What are your views on the above described models of enforcement?
    - We believe that the co-regulation model is the right model. The other regulators must defer to the DPA for data protection related issues.
    - For the most part, the DPA must prescribe a technology framework, and an audit model for day to day operations. The DPA can then focus on auditing operations, and dealing with exceptions.

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

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

    - The DPA must specify the framework for managing consent, the individual participation rights, and an audit framework.
    - It should then focus on the auditing (to prevent over consenting, consent fatigue, and abuse), as well as handling complaints, and exceptions.
    - The prevention of harm, and provision of recourse to the data subject is an important dimension that the DPA can focus on.
    - The other regulators must defer to the DPA for data protection related issues.

4. Are there any alternative views to this?

Part IV Chapter 2: Accountability and Enforcement Tools

Questions

1. What are your views on the use of the principle of accountability as stated above for data protection?
    - The prevention of harm, and provision of recourse to the data subject is an important dimension for the DPA.
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?
    - The DPA must work with the regulators, and industry bodies to create these standards.
3. Should the lack of organisational measures be linked to liability for harm resulting from processing of personal data?
    - Yes
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?
    - Contractual mechanisms should be allowed for the fixation of liability. However, the penalties, etc. cannot be determined contractually, they must be done through the law, or the DPA
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?
    - Yes
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?
    - By law, data controllers should be required to take out third party (user) insurance in the interest of user protection. Insurance of the Data Controller itself may not be required by law but they must be provided the facility to do the same.
7. Should this be limited to certain data controllers or certain kinds of processing?
    - No, it should apply to all data controllers.
8. If the data protection law calls for accountability as a mechanism for protection of privacy, what would be impact on industry and other sectors?
    - There may be issues during transition, but
        i. A well defined privacy structure, including accountability, and availability of insurance will help create a robust industry, which is privacy conscious as well.
        ii. A vaguely worded law, or the lack of guidelines, or insurance, will create significant confusion, and will prevent the industry from developing.

9. Are there any other issues or concerns regarding accountability which have not been considered above?
    - Accountability is the primary tool for balancing out the relationship between the data controller and data subject. The law, and the resulting enforcement mechanisms must define the various privacy harms, and use this mechanism to compensate the data subject, and penalize the controller.

Enforcement Tools

A. Codes of Practice

Questions

1. What are your views on this?
    - Such codes of practice should be blessed by an authority - one of (the DPA, the regulators, MEITY).
    - Regulators must be allowed to create subordinate legislation in line with this law, which may include specific codes of practice.
2. What are the subject matters for which codes of practice may be prepared?
    - Identifying where an individual's data may be (the dashboard), and mechanisms for exercising the various participation rights.
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?
    - Such codes of practice should be blessed by an authority - one of (the DPA, the regulators, MEITY).
    - Regulators must be consulted
4. Who should issue such codes of conduct or practice?
    - Such codes of practice should be blessed by an authority - DPA or MEITY.
5. How should such codes of conduct or practice be enforced?
    - Through mandatory audits, which are submitted to the sector regulators, and the DPA.
6. What should be the consequences for violation of a code of conduct or practice?
    - Fines / Penalties, Loss of License
7. Are there any alternative views?

B. Personal Data Breach Notification

Questions

1. What are your views in relation to the above?
    - **Data breaches will happen**. It is important to be prepared to deal with attackers, breaches, and to devise protection from harm for individuals.
2. How should a personal data breach be defined?
    - Unauthorized access to data constitutes a data breach.
    - Access outside the scope of consent and purpose (even if by authorized personnel) constitutes a data breach.

3. When should personal data breach be notified to the authority and to the affected individuals?
    - As soon as the business is aware of a potential data breach, it must notify the authority.
    - If notification of the data breach will result in **prevention of further harm** to the user, they must notify the potentially impacted users immediately.
    - However, if there is no further harm, they may take time (2 weeks) to come up with an initial report, including the individuals who may be affected. At this time, the affected individuals must be notified.
4. What are the circumstances in which data breaches must be informed to individuals?
    - Always.
5. What details should a breach notification addressed to an individual contain?
    - Date of breach, data that was accessed / stolen, possible remedies.
6. Are there any alternative views in relation to the above, others than the ones discussed above?

C. Categorisation of Data Controllers

Questions

1. What are your views on the manner in which data controllers may be categorised?
    - Mostly in line with the provisional views.
    - Controllers should be classified based on systemic risk - number of people, and the sensitivity of the data they store.
2. Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?
3. Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?
    - Yes
4. What are the factors on the basis of which such data controllers may be categorised?
    - On the sensitivity of the data that they have (based on potential harm)
    - On the volume of data (number of customers) that they have
5. What range of additional obligations can be considered for such data controllers?
6. Are there any alternative views other than the ones mentioned above?
    - Irrespective of the categorisation, all data controllers must ensure that they honor all the data protection rights of an individual and comply with a set of basic data protection and data empowerment requirements as decided by the DPA.

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?
    - Yes, there should be a registration requirement and based on the category (a function of sensitivity of data and volume of data) of the data controller they should have have the option to self-register with the DPA.
2. Are there any alternative views in relation to registration?

Data Protection Impact Assessment

1. What are your views on data controllers requiring DPIAs or Data Protection Impact Assessments?
    - Periodic DPIA must be done for all data controllers.
    - The periodicity must be determined based on severity of harm, and systemic risk.
2. What are the circumstances when DPIAs should be made mandatory?
3. Who should conduct the DPIA? In which circumstances should a DPIA be done
    - By an external professional qualified to do so
4. What are the circumstances in which a DPIA report should be made public?
    - Always.

5. Are there any alternative views on this?
    - DPIA reports must be filed with the regulator periodically.
    - Technology must be used for this purpose, to ensure that the regulator has a consistent, up to date view on the risk scenarios.

Data Protection Audit

1. What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?
2. Is there a need to make data protection audits mandatory for certain types of data controllers?
    - Yes
3. What aspects may be evaluated in case of such data audits?
    - All aspects related to security, confidentiality of the data, data quality, consent mechanism, various participation rights, etc.
4. Should data audits be undertaken internally by the data controller, a third party (external person / agency), or by a data protection authority?
    - Data audits should be automated (as far as possible).
    - Auditors should be required to certify that they have tested the correctness of the data audit software, and processes.
5. Should independent external auditors be registered / empanelled with a data protection authority to maintain oversight of their independence?
    - Yes, Auditors, and Compliance software (RegTech) should be certified, and empaneled.
6. What should be the qualifications of such external persons / agencies carrying out data audits?
7. Are there any alternative views on this?
    - Audit reports must be filed with the regulator periodically.
    - Technology must be used for this purpose, to ensure that the regulator has a consistent, up to date view. In particular, sectoral regulators should be able to use these audits to look for “over consenting”, for outliers, and for abuse of the data.

Data Protection Officer

1. What are your views on a data controller appointing a DPO?
    - For larger controllers, an independent DPO is a must, in addition to a CISO
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
3. What should be the qualifications and expertise of such a DPO?
4. What should be the functions and duties of a DPO?
5. Are there any alternative views?

D. Data Protection Authority

Questions

1. What are your views on the above?
    - Broadly agree with the provisional views.
    - However, the DPA must be tech enabled, accessing all data from controllers, grievances, etc. in a digital manner.
    - For this purpose, the data controllers, must also use empanelled providers to perform audits, ongoing compliance testing, and reporting. The DPA must set down the technical standards for this reporting, and the data that they would like to see.
2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?
    - Yes
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?
    - No, the RTI act serves as an oversight for public bodies to provide transparency. The DPA must provide oversight for public, and private entities to enable privacy, and 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?
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?
6. How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?
7. Considering that a single, centralised data protection authority may soon be over-burdened 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?
8. How can the independence of the members of a data protection authority be ensured?
9. Can the data protection authority retain a proportion of the income from penalties / fines?

- No

10. What should be the functions, duties and powers of a data protection authority?
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 government may set up various technical committees to support the DPA for the technical standards, as the technology evolves over a period of time.
    - However, the government should not have any operational role in the DPA.
12. Are there any alternative views other than the ones mentioned above?

Part IV Chapter 4: Remedies

A. Penalties

Questions

1. What are your views on the above?
    - It is important that the penalties consider the potential harm caused to the data subject for determining penalties.
    - These should be civil penalties for all offenders. However, this may not be sufficient for govt. entities, which may require additional deterrents.
    - Criminal penalties should be pursued against hackers, etc. (May be through other laws)
2. What are the different types of data protection violations for which a civil penalty may be prescribed?
    - It is important that the penalties consider the types of potential harm caused to the data subject
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?
4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?
5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (for the preceding financial year) or should it be a fixed upper limit prescribed under law?
    - This may be required for the deterrent component of the penalty.
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?
    - The entire turnover, as it would be difficult to calculate the processing activity alone.
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?
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)?
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?

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

B. Compensation

Questions

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 law should provide guidance on this aspect. However, loss may be tangible (funds stolen from a bank account), or intangible (reputational loss). Tangible harm should be compensated in full, while the intangible harm must be capped.
2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?
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?
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?
    - Any such compensation must be reported to the DPA, and the DPA must publish periodic reports.
5. Are there any alternative views other than the ones mentioned above?
    - In addition to legal recourse and compensation, the data controllers must also provide technology based remedial actions to rectify or limit further harms.

C. Offences

Questions

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?
    a. For the most part, criminal liabilities should be placed on malicious actors, such as hackers, etc. as well as others who are not registered to work with data. This would be for deliberate attempts to compromise systems, steal data, corrupt data, and cause harm to data subjects.
    b. Such penalties may also be considered for reckless endangerment of data.
    c. Data subjects must be able to ask a data controller / processor how they got access to any personal data. If they are unable to point to a valid source, the data controller can be subject to civil / criminal liabilities.
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?
3. What is the quantum of fines and imprisonment that may be imposed in all cases?
4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

5. Who will investigate such 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?
7. Are there any alternative views other than the ones mentioned above?

Part V: Summary

We provide some feedback on the proposed key principles.

Principle		Feedback & Suggestions
Data empowerment	<This principle is not mentioned in the report currently and should be considered for incorporation>	The law must use principles of accountability and empowerment to adjust the positional inequity between a data controller, and a data subject. The law must seek to empower the individual through control of their data.
Technology agnosticism	The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance.	The regulator must use all available technology (as it changes) to meet the objectives of the law. The law should encourage data controllers to use technology enabled tools to protect the data subjects from harm.
Holistic application	The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims.	The carve outs must be appropriate, and certain obligations (such as data protection) should not be exempt. The law must provide a balance between transparency, privacy, and the development agenda for the state. Not for Profit, political & social intent organisations should also fall under the law.
Informed consent	Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria.	Consent has not worked in the past and data controllers have used the blanket consent to their advantage. The law should clearly bring out the responsibility of the data controller beyond consent. The individual is in major cases not equipped to be sufficiently informed. Informed consent assumes a certain level of evolution and empowerment of the users, in the current case those assumptions may not be

		true.
Data minimisation	Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.	To strengthen this principle, a penalty provision is required on data controllers to deter collecting additional information in the spirit of Data Minimisation. Else the principle will become a matter of opinion. May be consider organisation in similar business to publish the data captured and stive for minimisation in a transparent manner.
Controller accountability	The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing.	Any data sharing must be with the consent of the data subject.
Structured enforcement	Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity (e.g., a central data protection authority and its subsidiaries). This must coexist with appropriate, potentially decentralised, enforcement mechanisms.	This capacity of the authority must be strengthened through the use of technology (e.g., automated logging protocols, consent dashboard).
Deterrent penalties	Penalties on wrongful processing must be adequate to ensure deterrence.	