Views on Data Protection-White Paper

By

Naavi

Founder www.naavi.org

SCOPE AND EXEMPTIONS **1.Territorial and Personal Scope** **The power of the State to prescribe and enforce laws is governed by the rules of jurisdiction in international law. Data protection laws challenge this traditional conception since a single act of processing could very easily occur across jurisdictions. In this context, it is necessary to determine the applicability of the proposed data protection law.** **For a fuller discussion, see page 24 above.**	
Questions	**Answers**
1.What are your views on what the territorial scope and the extra-territorial application of a data protection law in India?	**1. The law should be applicable for Activities of collection, storing, processing, of information that occurs in any system involving at least one computer located within the borders of India.**
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?	**2. When a contravention of the law occurs outside the territory of India, or by an entity residing outside India, the law should be applicable**
3.While providing such protection, what kind of link or parameters or business activities should be considered?	**3. All activities including marketing, profiling, data collection, analytics etc.**
Alternatives:	**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.	**All three alternatives are relevant** **The scope of the law should cover the rights of Indian Citizens primarily. However it cannot ignore the possibility of rights of others being violated during an activity in India.**
4.What measures should be incorporated in the law to ensure effective compliance by foreign entities inter alia when adverse orders (civil or	**In respect of contravention of the law by an entity residing outside India there would be a jurisdictional hurdle. It would require assistance from the other country. In order to ensure that there is mutual assistance, protection to the rights of persons who are not citizens of India through processing happening in India should be made available only on a mutual cooperation basis and not automatically.**

criminal) are issued against them? 5.Are there any other views on the territorial scope and the extra-territorial application of a data protection law in India , other than the ones considered above?	
2. Other Issues of Scope **There are three issues of scope other than territorial application. These relate to the applicability of the law to data relating to juristic persons such as companies, differential application of the law to the private and the public sector, and retrospective application of the law.** **For a fuller discussion, see page 30 above.**	
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 person; (ii) public and private sector; and (iii) retrospective application of such 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. 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 other provisions. b.Have different laws defining obligations on the government and the private sector.	1. **It should apply to Organizations and Natural persons to the extent they represent business and both public and private sector.** 2. **No retrospective application should be there. There has to be a definite time line with sufficient time for stake holders to prepare themselves.** 3. **Data of Companies is not relevant. Privacy is applicable to natural persons. Data of Companies is protected under ITA 2000/8 as part of cyber crime prevention and IPR.** 4. **No Personal information can be recognized for companies.** 5. **Should be applicable to Government subject to necessary exemptions in terms of law enforcement and security.** 6. **Exemptions should also be provided to individuals collecting personal information for household purposes and social activities not involving commercial resons.**

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

3. Definition of Personal Data

The definition of personal information or personal data is the critical element which determines the zone of informational privacy guaranteed by a data protection legislation. Thus, it is important to accurately define personal information or personal data which will trigger the application of the data protection law.

For a fuller discussion, see page 34 above.

Questions 1. What are your views on the contours of the definition of personal data or information? 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.	**Classification can be** **1. Basic Personal Information which includes Name and Address as well as IP Address** **2. Sensitive personal Information which includes E Mail address, Mobile Number, Aadhaar Number, PAN Number etc** **3. Highly sensitive Personal information which includes Password and Biometric** **4. Sensitive Sectoral Activity information such as Health and Financial Information** **5. Any other information which the data subject declares as confidential information which may include sexual orientation or political affiliation etc.**

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? 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? 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.] 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 determing whether a person may or may not be identified on the basis of certain data? 7. Are there any other views on the scope of the terms ?personal data' and ?personal information', which have not been considered?	**6. Other than the above, Facts, Opinions or assessments cannot be considered as personal information** **7. "identified" includes identifiable with available associated information. "reasonably identifiable" is speculative and not to be considered as "Identifiable.** **8. Anonymized and Pseudonomized data should be outside the definition of protected personal information.** **9. If anonymization or pseudonomization fails, the responsibility should be boarne by the "Anonymizer" or "Pseudonomizer" who would be either the Data Controller or the Data Processor**
4. Definition of Sensitive Personal Data **While personal data refers to all information related to a person's identity, there may be certain intimate matters in which there is a higher expectation of privacy. Such a category widely called ?sensitive personal data' requires precise definition.** **For a fuller discussion, see page 41 above**	
Questions 1 What are your views on sensitive personal data?	**Already provided above in the classification.**

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.] 3.Are there any other views on sensitive personal data which have not been considered above?	
5. Definition of Processing Data protection laws across jurisdictions have defined the term ?processing‘ in various ways. It is important to formulate an inclusive definition of processing to identify all operations, which may be performed on personal data, and consequently be subject to the data protection law. For a fuller discussion, see page 44 above.	
Questions 1. What are your views on the nature and scope of data processing activities? 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? 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: 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	**1.Processing includes “Collection”, “Storing” any kind of modification including arranging and rearranging, analyzing of data.** **2.Manual processing in preparation for processing using a computer resource should come under the definition.** **3. “Automatic Processing” is not proper usage for computer operation which is already defined in ITA 2000/8** **4. Manual processing not associated with either prior or post usage on a computer should be outside the scope of this “Personal Information Protection Law”.**

only. 4.Are there any other issues relating to the processing of personal data which have not been considered?	
6. Definition of Data Controller and Processor **The obligations on entities in the data ecosystem must be clearly delineated. To this end a clear conceptual understanding of the accountability of different entities which control and process personal data must be evolved.** **For a fuller discussion, see page 48 above.**	
Questions 1.What are your views on the obligations to be placed on various entities within the data ecosystem? 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. 3.How should responsibility among different entities involved in the processing of data be distributed? Alternatives: a.Making data controllers key owner 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	**Apart from the two categories "Data Controller" and "Data Processor", the law should recognize a third category of intermediaries called "Data Trusts" as organizations.** **The Data Trusts would be professional independent specialized organizations who take the deposit of personal information from members and issue a "Pseudonymous ID". Data controllers who collect data should collect only the pseudonomized ID issued by a Data Trust of their choice. The Data Trust would then release the appropriate class of personal data such as Basic data, sensitive data or confidential data etc based on the requirement of the Data Controller after a professional assessment of the Privacy notice and consent requirements. Data Trusts would be registered and accredited with the Data Protection Authority of India.** **A "Data Manager" can assist as individual professional in acting as Customer Relation Managers on behalf of Data Trusts as a bridge between the data subject and the data trust. The Data Controller who have a vested interest in the data will only obtain data from the Data Trust and not directly. Data Trusts should maintain arms length relationship with Data Controllers. The infrastructure should be similar to the structure of SEBI-Mutual Funds-Asset Management Companies Portfolio Managers.** **The Data Trust may provide "Secured Personal Data Storage" as a service and Data Controllers may pay a price for using the data which should cover the costs of the Data Trusts and also leave**

protection to data subject from data processor. Are there any other views on data controllers or processors which have not been considered above?	**a surplus to be paid to the data subject who "Licenses" his data to the Data Trust.** **(More details of the suggested scheme are available at www.naavi.org)**
7. Exemptions **A data controller may be exempted from certain obligations of a data protection law based on the nature and purpose of the processing activity eg. certain legitimate aims of the state. The scope of such exemptions, also recognised by the Supreme Court in Puttaswamy needs to be carefully formulated.** **For a fuller discussion, see page 52 above.**	
Questions 1.What are the categories of exemptions that can be incorporated in the data protection law? 2.What are the basic security safeguards/organisational measures which should be prescribed when processing is carried out on an exempted ground, if any? Domestic /Household Processing 1.What are your views on including domestic/household processing as an exemption? 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? 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? 2.Should exemptions for journalistic purpose be included? If so, what should be their scope? 3.Can terms such as ?journalist' and ?journalistic purpose' be defined?	**Exemptions for National Security, Law Enforcement, Personal household use, Public Interest and exceptional circumstances with a due process.** **Exemptions are also important from the point of view of the security of the data subject himself as in the case of Health data when the data subject needs medical attention.** **Domestic and Household processing must be exempted.** **No exemption is required for journalistic or literary purpose. Any privacy invasion for journalistic purpose should be justified under the "Public Good" reasons and if it fails, the defamation charge should be faced by the journalist.** **Privacy protection may cease after the death of an individual when literary or artistic freedom can take over. During the life time, literary work should also be subject to defamation issue.**

4.Would these activities also include publishing of information by non-media organisations? 5.What would be the scope of activities included for ?literary' or ?artistic' purpose? Should the terms be defined broadly? 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? 2.Can there be measures incorporated in the law to exclude activities under this head which are not being conducted for a bonafide purpose? 3.Will the exemption fail to operate if the research conducted in these areas is subsequently published/ or used for a commercial purpose? 4.Are there any other views on this exemption?	**Deindeintification and Psudonomization should take care of the statistical purpose and research purpose. Historical purpose can be on anonymity/pseudonomity basis during the life time of the data subject.**
Investigation and Detection of Crime, National Security 1.What are your views on including investigation and detection of crimes and national security as exemptions? 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? 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? 4.Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail? 5.How can the enforcement mechanisms under the proposed law monitor/control processing of personal data under this exemption?	**Law Enforcement has to be exempted.** **There is already certain procedures prescribed under ITA 2000 and Telegraph Act for interception of privacy and this law has to integrate its provisions with the existing laws without creating a conflict.** **Where "Exemption" is disputed, the grievance redressal mechanism can take care of resolving the dispute.** **Tax collection is part of Governance and should be in the exempted category along with "Law Enforcement".** **Prevention of Crime is part of the Law Enforcement obligation**

5. Do we need to define obligations of law enforcement agencies to protect personal data in their possession? 7.Can the Data Protection Authority or/and a third-party challenge processing covered under this exemption? 8.What other measures can be taken in order to ensure that this exemption is used for bona fide purposes? **9** Are there any other views on these exemptions? Additional Exemptions 1. Should prevention of crime' be separately included as ground for exemption? 2. Should a separate exemption for assessment and collection of tax in accordance with the relevant statutes be included? 3.Are there any other categories of information which should be exempt from the ambit of a data protection law?	
8. Cross Border Flow of Data **Given the advent of the Internet, huge quantities of personal data are regularly transferred across national borders. Providing strong rules to govern such data flows is vital for all entities in the data eco-system.** **For a fuller discussion, see page 62 above.**	
Questions 1. What are your views on cross-border transfer of data? 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? 3.Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfils the test for transfer? 4. Are there any other views which have not	**It is reasonable to insist that cross border transfer should be only with the permission of the Data protection Authority and after a copy is made available in India.** **Highly sensitive personal data such as Biometric should not be allowed to be sent out of India.** **Data Protection Authority may consider permissions only on the basis of a reciprocal arrangement with other countries and only after one copy is always stored in India.**

been considered?	

9. Data Localisation

Data localisation requires companies to store and process data on servers physically located within national borders. Several governments, driven by concerns over privacy, security, surveillance and law enforcement, have been enacting legislations that necessitate localisation of data. Localisation measures pose detrimental effects for companies may, harm Internet users, and fragment the global Internet.

For a fuller discussion, see page 69 above.

Questions	
1.What are your views on data localisation?	**This is related to Cross border movement.**
2.Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?	**By default Data must be held locally. Exceptions are subject to Data Protection Authority permission on reciprocal arrangements with the other country.**
3.If yes, what should be the scope of the localisation mandate? Should it include all personal information or only sensitive personal information?	**Biometric should be out of the purview of cross border transfer and has to be held only locally.**
4.If the data protection law calls for localisation, what would be impact on industry and other sectors?	**If the data localization is restricted to "holding a copy in India", there will be only positive impact.**
5.Are there any other issues or concerns regarding data localisation which have not been considered above?	

10. Allied Laws

Currently, there are a variety of laws in India which contain provisions dealing with the processing of data, which includes personal data as well as sensitive personal data. These laws operate in various sectors, such as, the financial sector, health sector and the information technology sector. Consequently, such laws may need to be examined against a new data protection legal and regulatory framework as and when such framework comes into existence in India.

For a fuller discussion, see page 76 above.

Questions	
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.	**Data protection law has to be aligned with other laws.** **It is possible for this law to be made as an add on to the Information Technology Act by way of a new chapter.**

GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS	
1. Consent **Most jurisdictions treat consent as one of the grounds for processing of personal data. However, consent is often not meaningful or informed, which raises issues of the extent to which it genuinely expresses the autonomous choice of an individual. Thus, the validity of consent and its effectiveness needs to be closely examined.** **For a fuller discussion, see page 78 above.**	
Questions 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. 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? 3.How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this? 4.Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations? 5.Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided? 6. Are there any other views regarding consent which have not been explored above?	**Consent is unavoidable but unlikely to be effective because of the "consent fatigue" factor.** **I have suggested the "Data Trust" model of intermediation which is precisely meant to address this issue.** **Otherwise, Informed Consent is cannot be expected in a country of multiple languages and low literacy levels.** **It would be a farce if too much reliance is placed on the online consents which are "Undigitally signed" and cannot be fully enforced.** **Kindly give a serious thought to the "Data Trust Model" if necessary with further reference to the details provided in www.naavi.org.** **Further clarification if required can be provided on the thought which can be fine tuned if required.** **This would be a deviation from the global practice including GDPR and would be unique to India.**

2. Child's Consent

It is estimated that globally, one in three Internet users is a child under the age of 18. Keeping in mind their vulnerability and increased exposure to risks online, a data protection law must sufficiently protect their interests.

For a fuller discussion, see page 85 above.

Questions	
1. What are your views regarding the protection of a child's personal data? 2.Should the data protection law have a provision specifically tailored towards protecting children's personal data? 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? 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? 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? 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	**A Child cannot be identified except by self-declaration. Hence it is difficult to rely on any consent to eliminate mis declaration.** **Data Controllers should be exempted from liabilities where there is a false declaration subject to "Due Diligence" to be exercised to identify the age of the data subject where feasible.** **Where there is a declaration, parental consent should be a must.** **The age for the purpose of parental consent should be upto 16 years.** **If the service provider undertakes the responsibility that the service provided or content is meant for or appropriate for children, then the self consent can be accepted.**

consent 7.How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required? 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? 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? 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? 11.Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?	
3. Notice **Notice is an essential prerequisite to operationalise consent. However, concerns have been raised about notices being ineffective because of factors such as length, use of complex language, etc. Thus, the law needs to ensure that notices are effective, such that consent is meaningful.** **For a fuller discussion, see page 92 above.**	
Questions 1. Should the law rely on the notice and choice mechanism for operationalising consent? 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? 3.Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?	**Notice is essential but not sufficient for the reasons stated earlier for which the concept of Data Trust was recommended.** **The Data Trusts can be rated according to their practices and can be audited and down graded where required as a means of maintaining the standards.**

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. 5. How can data controllers be incentivised 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? 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? 7.Are there any other alternatives for making notice more effective, other than the ones considered above?	
4. Other Grounds of Processing **It is widely recognised that consent may not be sufficient as the only ground for lawful processing of personal data. Several other grounds, broadly conforming to practical requirements and legitimate state aims, are incorporated in various jurisdictions. The nature and remit of such grounds requires determination in the Indian context.** **For a fuller discussion, see page 99 above.**	
Questions 1. What are your views on including other grounds under which processing may be done? 2. What grounds of processing are necessary	**Can be considered on case to case basis by the Data protection Authority.**

other than consent? 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. 4.Are there any alternative methods to be considered with respect to processing personal data without relying on consent?	
5. Purpose Specification and Use Limitation **Purpose specification and use limitation are two cardinal principles in the OECD framework. The principles have two components- first, personal data must be collected for a specified purpose; second, once data is collected, it must not be processed further for a purpose that is not specified at the time of collection or in a manner incompatible with the purpose of collection. However the relevance of these principles in the world of modern technology has come under scrutiny, especially as future uses of personal data after collection cannot always be clearly ascertained. Its relevance for the Indian context will thus have to be assessed.** **For a fuller discussion, see page 105 above.**	
Questions 1.What are your views on the relevance of purpose specification and use limitation principles? 2.How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies? 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?	**Necessary. It is an established practice alrady available under Section 79 rules.**

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. 5.Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?	
6. Processing of sensitive personal data **If ?sensitive personal data‘ is to be treated as a separate category, there is a concomitant need to identify grounds for its processing. These grounds will have to be narrower than grounds for general processing of personal data and reflect the higher expectations of privacy that individuals may have regarding intimate facets of their person.** **For a fuller discussion, see page 111 above.**	
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: 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.	**Necessary. It is an established practice already available under Section 43A rules.**

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. 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? 5. Are there any alternative views on this which have not been discussed above?	
7. Storage Limitation and Data Quality **Related to the principle of purpose specification is the principle of storage limitation which requires personal data to be erased or anonymised once the purpose for which such data was collected is complete. Personal data in the possession of data controllers should also be accurate, complete and kept up-to-date. These principles cast certain obligations on data controllers. The extent of such obligations must be carefully determined.** **For a fuller discussion, see page 117 above.**	
Questions 1. What are your views on the principles of storage limitation and data quality? 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 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	**The onus of data accuracy in the recommendation given here in would be on the Data Trusts.**

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

8. Individual Participation Rights-1

One of the core principles of data privacy law is the ?individual participation principle? which stipulates that the processing of personal data must be transparent to, and capable of being influenced by, the data subject. Intrinsic to this principle are the rights of confirmation, access, and rectification. Incorporation of such rights has to be balanced against technical, financial and operational challenges in implementation.
For a fuller discussion, see page 122 above.

Questions	
1. What are your views in relation to the above? 2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access? 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? 4. Should there be a fee imposed on exercising the right to access and rectify one's personal data? Alternatives: a. There should be no fee imposed. b.The data controller should be allowed to impose a reasonable fee. c.The data protection authority/sectoral regulators may prescribe a reasonable fee. 5.Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be? 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?	**Yes. The access right can be absolute only for the determination of accuracy.** **In other cases, there has to be a measured approach supported by sector specific guidelines and a quick dispute resolution mechanism.** **The dispute resolution mechanism should include an automatic permission under emergencies where a responsible independent party (eg Doctor in the case of Health information) takes the responsibility.** **No fee should be levied.** **Since Data Trusts are professional organizations, Data Controllers can share the information more easily with them even if some restrictions on disclosure to the data subject is required. In such exceptional circumstance, the Data Trust would act as a trustee of information from both sides and like an escrow arrangement try to protect the interest of both the parties.**

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.] 8. Are there any other views on this, which have not been considered above?	
9. Individual Participation Rights-2 **In addition to confirmation, access and rectification, the EU GDPR has recognised other individual participation rights, viz. the right to object to processing (including for Direct marketing), the right not to be subject to a decision solely based on automated processing, the right to restrict processing, and the right to data portability. These rights are inchoate and some such as those related to Direct Marketing overlap with sectoral regulations. The suitability of incorporation of such rights must be assessed in light of their implementability in the Indian context.** **For a fuller discussion, see page 129 above.**	
Questions **1**. What are your views in relation on the above individual participation rights? 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? 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. 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? 5.Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations? 6.Are there any alternative views in relation to the	**Data Portability can be provided across the Data Trusts. They shall guide the data subjects in protecting their rights including making Data Controllers pay for the commercial exploitation of the data under permission.**

above which have not been considered?	

10. Individual Participation Rights-3: Right to be forgotten

The right to be forgotten has emerged as one of the most emotive issues in data protection law. The decision of the European Court of Justice in the Google Spain case and the repeated reference to this right in Puttaswamy necessitates a closer look at its contours, scope and exceptions, particularly as it raises several vexed questions relating to the interface between free speech, privacy and the right to know.
For a fuller discussion, see page 137 above.

Questions	
1.What are your views on the right to be forgotten having a place in India's data protection law? 2.Should the right to be forgotten be restricted to personal data that individuals have given out themselves? 3.Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights? 4.Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controller's possession? 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? 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)? 7.Are there any alternative views to this **.**	**Right to be forgotten is not feasible from the security point of view and has to be rejected.**

General Observations

The Data Protection Authority should form a "Jurisdictional Umbrella" for Indian data processors when there is a conflict of interest with the foreign regulators such as GDPR.

No penal action is to be allowed on an Indian Citizens or Company, except through the Indian Data Protection Authority.

Personal Data has to be declared as a "Property" on which the individual has the sole right to commercialize and it should be considered as leased out whenever it is given out in exchange of a service.

The Data Trust model is specifically structured to make it possible. If Data is the new oil and data analytics is a good commercial proposition, then the data subjects who provide the raw material must get some reward and this is possible only if Data Trust model is adopted.

Na.Vijayashankar (Naavi)
9343554943
37, 20th Main, BSK First Stage, Bangalore 560050