PART V
SUMMARY

Key Principles of a Data Protection Law

A data protection framework in India must be based on the following seven principles:

1. Technology agnosticism- The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance.

2. 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.

3. 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.

4. 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.

5. 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.

6. Structured enforcement- Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms.

7. Deterrent penalties- Penalties on wrongful processing must be adequate to ensure deterrence.

In order to achieve these principles, the Committee requests your views on the White Paper. The key issues analysed in the White Paper and questions raised for consultation under each head are summarised below for convenience. We would be grateful if your answers are brief and targeted to the questions asked. Any other views on the subject will also be appreciated.

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

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

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

   Alternatives:

   a. Cover cases where processing wholly or partly happens in India irrespective of the status of the entity.
   b. Regulate entities which offer goods or services in India even though they may not have a presence in India (modelled on the EU GDPR)
   c. Regulate entities that carry on business in India (modelled on Australian law), business meaning consistent and regular activity with the aim of profit.

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?

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.

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.

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?

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?

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 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 protection to data subject from data processor.

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

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?

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?

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?

6. 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 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?

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

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

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

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.

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?

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 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?

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 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?

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.
   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

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?

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 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 .

REGULATION AND ENFORCEMENT

1. Enforcement Models

Once the substantive obligations of a data protection law are formalised, provisions regarding enforcement must be structured so as to ensure compliance with substantive provisions. Effective enforcement requires the consideration of certain aspects of institutional design and overall approach before we can develop and align individual elements of the framework. This may be in terms of the extent of burden placed on entities covered under such framework, the structure and functions of any enforcement agency, or the tools at its disposal. Enforcement models consist of: (i) 'command and control'; (ii) self-regulation; and (iii) co-regulation.

For a fuller discussion, see page 143 above.

Questions

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

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

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

4. Are there any alternative views to this?

2. Accountability and Enforcement Tools

Accountability

A data protection law must reflect the principle of accountability. Accountability should not only be enforced for breach of data protection obligations through the adoption and implementation of standards by data controllers, but also in certain well defined circumstances, it could be extended to hold data controllers liable for the harms that they cause to individuals without further proof of violation of any other obligation. The data protection law should appropriately identify such harms for which the data controller should be held liable in this manner.

For a fuller discussion, see page 147 above.

Questions

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

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?

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

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?

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?

6. Should the data controllers be required by law to take out insurance policies to meet their liability on account of any processing which results in harm to data subjects? Should this be limited to certain data controllers or certain kinds of processing?

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

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

Enforcement Tools

A number of regulatory tools and mechanisms may be simultaneously utilised to achieve different enforcement objectives such as flexibility and rigour in compliance. It needs to be determined which regulatory tools and mechanisms will find place in a data protection law for India.

A. Codes of Practice

For a fuller discussion, see page 157 above.

Questions

1. What are your views on this?

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

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?

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

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

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

7. Are there any alternative views?

B. Personal Data Breach Notification

The aggregation of data in the hands of public and private entities leaves them vulnerable to data breaches. Data breaches can take many forms including; hackers gaining access to data through a malicious attack; lost, stolen, or temporary misplaced equipment; employee negligence; and policy and/or system failure. It is important to identify these threats and establish processes to deal with these breaches.

For a fuller discussion, see page 161 above.

Questions

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

2. How should a personal data breach be defined?

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

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

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

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

C. Categorisation of Data Controllers

Given the complexity and breadth of application of a data protection law, it may be difficult for a regulator to effectively ensure compliance on the part of all data controllers. Further, a data protection law can entail heavy compliance burdens. As a result, it may be necessary,

both for principled and practical reasons to differentiate between data controllers, depending on factors that give rise to greater risks or threats to individual data protection rights.

For a fuller discussion, see page 167 above.

Questions

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

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?

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

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?

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?

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?

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 (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?

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

5. Are there any alternative views on this?

Data Protection Audit

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

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

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

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

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

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

7. Are there any alternative views on this?

Data Protection Officer

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

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?

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

The effective enforcement of data protection law may necessitate a separate, independent regulatory authority. Such an authority may discharge the following types of functions, powers and duties: (i) Monitoring, enforcement and investigation; (ii) Standard-setting; and (iii) Awareness generation.

For a fuller discussion, see page 175 above.

Questions

1. What are your views on the above?

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

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?

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?

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?

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

3. **Adjudication Process**

Adjudication plays an integral role in enforcement of any law as it ascertains the rights and obligations of parties involved in a dispute and prescribes corrective actions and remedies. In the context of a data protection law, adjudication entails an assessment of whether and to

what extent data protection rights of an individual have been infringed by a data controller, the loss or damage suffered by the individual due to the said infringement, the remedies available to the individual as well as the penal consequences that the data controller may be liable for.

For a fuller discussion, see page 184 above.

Questions

1. What are your views in relation to an adjudication process envisaged under a data protection law in India?

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

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

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

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

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

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

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

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

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

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

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

13. Should class action suits be permitted?

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

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

4. Remedies

A. Penalties

In the context of a data protection law, civil penalties may be calculated in a manner so as to ensure that the quantum of civil penalty imposed not only acts as a sanction but also acts as a deterrence to data controllers, which have violated their obligations under a data protection law. Further, there may be three models (or a combination thereof) possible for the calculation of civil penalties, which are as follows:

(i) Per day basis;
(ii) Discretion of the adjudicating body subject to a fixed upper limit;
(iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter (such as a percentage of the total worldwide turnover of the preceding financial year of the defaulting data controller).

For a fuller discussion, see page 191 above.

Questions

1. What are your views on the above?

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

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?

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?

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?

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

B. Compensation

Awarding of compensation constitutes an important remedy where an individual has incurred a loss or damage as a result of a data controller's failure to comply with the data protection principles as set out under law.

For a fuller discussion, see page 197 above.

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?

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?

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

C. Offences

The law may treat certain actions of a data controller as an offence and impose a criminal liability. This may include instances where any person recklessly obtains or discloses, sells, offers to sell or transfers personal data to a third party without adhering to relevant principles of the data protection law, particularly without the consent of the data subject. It may be considered whether other acts should create criminal liability.

For a fuller discussion, see page 201 above.

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?

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?

****