Submission to the Committee of Experts on a Data Protection Framework for India

By **AMBER SINHA**

Inputs from **ELONNAI HICKOK** and **SUNIL ABRAHAM**

Research assistance from **ANUSHKA SINHA**, **SUNIDHI SAWHNEY** and **KANAV BURMAN**

January 31, 2018
The Centre for Internet and Society, India

Designed by **Saumyaa Naidu**

Contents

I. Preliminary

A. Introduction

This submission presents comments by the Centre for Internet and Society, India ("**CIS**") on the 'White Paper of the Committee of Experts on a Data Protection Framework for India' ("**White Paper**") released by the Ministry of Electronics and Information Technology. The White paper was drafted by a Committee of Expert ("**Committee**") constituted by the Ministry. CIS has conducted research on the issues of privacy, data protection and data security since 2010 and is thankful for the opportunity to put forth its views. The submission was made on January 31, 2018.

The submission is divided into four parts — I. Preliminary, II. Scope and Exemption, III. Grounds of Processing, Obligations of Entities and Individual Rights and IV. Regulation and Enforcement. The submission follows the same the order as adopted by the White Paper

B. About CIS

CIS is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with diverse abilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, freedom of speech and expression, intermediary liability, digital privacy, and cybersecurity.

CIS has conducted extensive research into the areas privacy, data protection, data security, and was also a member of the Committee of Experts constituted under Justice A P Shah.[1] CIS values the fundamental principles of justice, equality, freedom and economic development. This submission is consistent with CIS' commitment to these values, the safeguarding of general public interest and the protection of individuals' right to privacy and data protection. Accordingly, the comments in this submission aim to further these principles.

C. Informational Privacy

The right to data protection is currently at the center of attention globally, with the General Data Protection Regulation being enforced later this year, and Safe Harbour and Privacy Shield arrangement having undergone changes in the last few years. In India, the Puttaswamy judgment last year, emphatically upheld the right to privacy as fundamental right, and recognized the urgent need for a data protection law. The judgment is also fundamentally

1 http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

relevant to this issue for its recognition of information privacy as part of the fundamental right to privacy.

Informational privacy refers to the expectations of privacy that individuals have with respect to information about them. It is inextricably linked to the idea of control that individuals should have over their personal information.[2] In the past also, the court has held in Canara Bank,[3] that state actions to seek access to private documents must be subject to the standard of 'reasonable cause', or else it would be considered an infringement of privacy. The other important observation in this case was that, since, privacy resided in persons and not places, the disclosure of information to a third party does not stand as ground against the presumption of right to privacy.

The idea of informed consent as central to informational privacy is the key thread that runs across the different opinions in the judgment. This point is relevant to the current debates regarding the nature of data protection law that India should about. While the principles of nature and consent are essential to most data protection frameworks across the world, there have been proposals in India to move beyond it.[4] It must be remembered that this judgment has held that privacy is both a negative and a positive right, meaning that not only does it restrain the state from committing an intrusion upon the life and personal liberty of a citizen, it also imposes an obligation on the state to take all necessary measures to protect the privacy of the individual. The unequivocal endorsement of informed consent in this judgment could leave any existing or future laws governing data collection which fail to recognise the principle of informed consent susceptible to legal challenge in the future.

Without suggesting any exact recipe, we believe that an efficacious data protection system would comprise (in summary): a strong law, an assertive regulatory authority, data controllers committed to compliance, market incentives to comply, a vigilant and activist citizenry and use of privacy-enhancing technologies.[5] Through various submission made below, we suggest ways in which the data protection law can enable the above.

Data protection regimes, the world over, recognise the following broad principles, a public or private organisation that deals with PII should:

a) be accountable for all of the personal information in its possession (Accountability);

---

2 Alan Westin, *Privacy and Freedom*, New York: Atheneum, 2015.

3 *Collector* v. *Canara Bank*, (2005) 1 SCC 496.

4 Rahul Matthan, "Beyond Consent: A New Paradigm for Data Protection" Takshashila Institution (July, 2017), available at http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-DataProtection-RM-2017-03.pdf.

5 Bennett, Colin, and Charles Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, 2006.

b) identify the purposes for which the information is processed at or before the time of collection (Purpose Specification);

c) only collect personal information with the knowledge and consent of the individual, except under specified circumstances, after providing meaningful notice of data to be collected and purposes it would be used for (Notice, and Consent);

d) limit the collection of personal information to that which is necessary for pursuing the identified purposes; (Collection Limitation)

e) not use or disclose personal information for purposes other than those identified (except with the individual's consent); (Disclosure and Use Limitation)

f) retain information only as long as necessary; (Deletion)

g) ensure that personal information is kept accurate, complete and up to date; (Data Quality)

h) protect personal information with appropriate security safeguards; (Data Security)

i) be transparent about its policies and practices and maintain no secret information system; (Transparency)

j) allow data subjects access to their personal information, with an ability to amend it if it is inaccurate, incomplete or obsolete (Access and Correction)

While most of the provisional views already reflect these principles, it would be recommended to explicitly recognise a set of principles which form the basis of the recommendations of the Committee. This would be extremely useful and instructive in both holding the legislation drafted accountable to privacy principles that the Committee feels necessary, as well as guide the interpretation of and jurisprudence around the data protection law, in the future. It is also submitted that these principles should be referred to in the Statement of Object in the data protection law.

II. Scope and Exemptions

Chapter 1: Territorial Scope

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

The ubiquitous use of digital technology, cloud servers, presence of multinationations companies has resulted in easy availability of services offered by actors who may be located outside the territorial jurisdiction of the country. The data protection legislation must be applicable to whole of India and also apply to any offence or contravention thereunder committed outside India by any person, if it related to the personally identifiable information of an Indian resident. The legislation should be applicable to the following kind of data controllers:

a) Entities in India: Any public or private entity, including but not limited to individuals, societies, body corporates, partnerships, located, registered or residing in India;

b) Entities carrying out business in India: Any entity carrying out business, including any trade, commerce or manufacture or any adventure or concern in the nature of trade, commerce or manufacture, in India;

c) Providing services to Indian residents: Any entity, whether located in India or outside, either providing services to residents in India, which involves collection of personally identifiable information, or having access to personally identifiable information of Indian residents.

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?

Please refer above.

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

The data protection laws should be applicable to all entities carrying out business, including any trade, commerce or manufacture or any adventure or concern in the nature of trade, commerce or manufacture, in India, as well as all entities, whether located in India or outside, either providing services to residents in India, which involves collection of personally identifiable information, or having access to personally identifiable information of Indian residents.

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?

MLATs are binding treaties entered into between nations for seeking and providing assistance for helping each other with domestic legal processes. They are usually bilateral treaties though there exists a few multilateral treaties as well. MLATs envisage a wide range of assistance including serving of summons, taking witness testimony, execution of decrees etc.

Better transparency, efficiency and capacity building are required to ensure the MLA process is durable. There should be transparency in receiving and processing of requests for access to user data by companies and states. Countries should have transparency in terms of incoming requests including the volume of those request, the data been sought and countries that are seeking it. A higher burden should be placed on law enforcement authorities requesting information, including showing a legitimate and reasonable interest in the relevant data which is acceptable to the responding country.

Companies should provide guidelines to local law enforcement about what sorts of data requires a request for MLA and what sorts of data requests can be processed by the company directly in accordance with local law and international human rights standards (which are often employed by companies when data requests are made).[6]

Entering into more MLAs with countries that are home to massive data centres, technology companies that process data of Indian residents like Japan[7], Germany[8], China[9] will ensure that India has the capability to protect its residents data.

6 *Data Beyond Borders - Mutual Legal Assistance in the Digital Age*, available at https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf

7 *The Best (and Worst) Countries for Cloud Computing*, available at https://www.cio.com/article/2387759/government/the-best--and-worst--countries-for-cloud-computing.html, last accessed on 30-01-2018

8 *Id*

9 *The top 100 web hosting countries*, available at http://royal.pingdom.com/2013/03/14/web-hosting-countries-2013/, last accessed on 30-01-2018

Chapter 2: Other Issues of Scope

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

Natural/Juristic persons

The right to privacy is grounded in Article 21 of the Constitution, a fundamental right that is guaranteed to natural persons but not juristic persons. **As such, personal data exists only for natural persons, to apply for juristic persons it would require departing from the most international standards (under Information Technology Act, Justice AP Shah Report, EU GDPR) which is not advisable**. In cases where the data held or owned by juristic persons such as companies and body corporates are in the nature of personally identifiable information of natural persons, they would automatically be protected.

Public and private sector

As mentioned under our response in Chapter 1 of this section, the law should be made applicable to both public and private sectors, since both kinds of entities process large amounts of data. **Unlike the rule framed under Section 43A of the Information Technology Act, 2000, it is imperative that both public and private bodies are subject to the data protection law.**

Public entities, in India, now collect massive amounts of personal data for for the purpose of governance under the Digital India project and for surveillance activities, under various intelligence gathering and law enforcement projects. As a result they should follow due process and administrative law principles over and above the obligations on the private sector.

An examination of Supreme Court's jurisprudence on Article 21 clearly reveals that a person's rights under Article 21, which is the primary repository of the right to privacy, can only be limited through a law, whose procedure,[10] as well as substantive provisions, are 'fair, just and reasonable'.[11] With established administrative principles of reasonableness, procedural propriety and non-arbitrariness and due process principles of transparency, accountability and conforming to the fair, just and reasonable standard, **it is recommended that the law or its objects specify that collection of data while discharging public functions must satisfy the standards of both procedural and substantive due process under Article 21**.

Retrospective application

It is possible that a surge of personal information would be transferred immediately prior the law coming into force in a final attempt to compile databases that won't be governed by

10 *Maneka Gandhi v. Union of India,* 1978 AIR 597

11 *Sunil Batra v. Delhi Administration*, AIR 1980 SC 1579

the law.[12] Some amount of retrospective application is required to prevent undue advantage from such a situation. There doesn't need to be any distinction made with regard to the information collected before the act is implemented and that after (as is implemented in PIPEDA, the Canadian law), especially in terms of the future use and disclosure of that personal data. **The law can be retrospective in respect of the continued processing of data but not to the extent that requires re-obtaining of consent.**

An opt-out provision that provides the data subjects with a method to protect previously submitted data should be present (this will act as a safeguard for data that may have been obtained without proper consent).[13] An additional condition for the personal data already collected should be that its **retention and continued use must satisfy the conditions laid down in the legislation, otherwise it should be destroyed**.[14]

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

Refer to 1.

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?

Refer to 1.

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?

Refer to 1.

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?

The absence of any data protection guidelines necessitates that certain provisions be

12 This happened in the case of South Africa. See *POPI – Is South Africa keeping up with international trends*?, available at http://www.saflii.org/za/journals/DEREBUS/2014/84.html.

13 The South African data protection legislation provides for this. See *Id.*

14 The Canadian data protection legislation provides for this. See *Compliance with the Personal Information Protection and Electronic Documents Act*, available at http://documents.jdsupra.com/4217f03e-a265-4711-a230-103d2a5f3140.pdf.

implemented immediately. However other provisions that require higher compliances need an interim time period before they become enforceable. The table below, demarcates the provisions in terms of the time period that should be added for their compliance.

We provide below an illustrated list of how different provisions can be rolled out in a staggered fashion:

Timeline	**Rolling out of provisions**
Immediate Implementation upon enactment	Notice
	Consent
	Opt-out
	Purpose specification and use limitation
	Data Security
	Access/Rectification
	Accountability
	Transparency
	Limits on Third Party Disclosure
1 year from enactment	Anonymisation and Pseudonymisation
	Data localisation (for government data)
	Data portability
	Creation of co-regulatory bodies
	Creation of standards and methodologies on Data Protection Impact Assessments, Audits by DPA
1 Year interim Period	Punitive Enforcement - breaches of regulation in the interim period could be addressed through corrective measures for one year rather than punitive measures. The presumption for breaches within a year from enactment, and for all first reported cases of breaches should be corrective action. However in cases where there are factors to demonstrate high gravity of breach, the potential harm of the breach and the absence of mitigating factors, the judicial authority may choose to exercise punitive powers.
2 years from enactment	Creation of standards and methodologies on Data Protection Impact Assessments, Audits by Sectoral bodies
	Drafts on sectoral codes to be prepared by the industry
	Right to explanation

Chapter 3: What is Personal Data?

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

Any kind of data that can be reasonably used to identify a person has to classified as personal data.[15] In devising an approach to conceptualize PII, **the first step is to determine whether it should be defined as a rule or a standard**. A standard is an open-ended decision making yardstick, and a rule is a more prescriptive decision making tool. The definition has to be a standard based definition that inculcates these means of identification. It cannot be prescriptive or a catalogue of data categories, as the identifiability of a person is contextual and creating an exclusive definition based on particular situations will lead to the exclusion of personally identifiable data. The catalogue approach lists certain kinds of data that fall within the category of PII. The resulting attempts at a rule, however, prove either too narrow, as in the Massachusetts breach notification statute,[16] or outdated, as in the definition of sensitive personal data or information in the Information Technology Act in India.

Standards, on the other hand, permit broad discretion and allow the decision maker to take into account relevant factors. As stated by Solove and Schwartz, a "ground to prefer defining PII as a standard is the heterogeneous nature of the behavior to be regulated as the the means to track individuals and re-identify information are diverse."

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

To limit confusion from usage of multiple terms to denote the same concept, a single phrase should be used. We recommend the use of the term, *personally identifiable information*.

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

We second the opinion of the Committee that following the examples of Australia and Singapore, whether a piece of information is personal data does not depend on whether it is true or not, therefore, assessment should also be covered under this law.

In the context of opinion, the data protection law and the free speech protection under Article 19 of the Constitution refer to two different kinds of protection and both should be

15 *Justice K.S. Puttaswamy (Retd.) & Another **v/s** Union of India & Ors*, Writ Petition (Civil) No. 494 of 2012

16 *Report of the Group of Experts on Privacy by AP Shah Committee*, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

protected. The protections under Article 19 apply to free speech and expression and the ability of individuals to express opinions subject to reasonable restrictions, data protection law would only be applicable once the opinion has been expressed, and processing of that opinion as data.

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

Distinguishing information as identified, identifiable and not-identifiable is important as different levels of effort are required to identify information, and varying risks are associated with the possible identification of such data. Each category places a different burden on the data collector as to their obligations and use of the data. By distinguishing identifiable and identified, it becomes easier for the data controller to use it. Their burden is reduced, yet there is a degree of care required to ensure that the identifiable information does not become identified.

Drawing from the analysis by Solove and Schwartz, we can conclude that there is a broad continuum of identifiable information that includes different kinds of anonymous or pseudonymous information. Any dataset which involves individuals in process of data generation, has a statistical possibility of being linked back to the individuals in question. However, in a number of cases, the possibility is extremely remote. Different levels of effort will be required to identify information, and varying risks are associated with the possible identification of data. To place all such data into the same conceptual category as data that currently relate to an identified person is a blunt approach.[17]

There is a need for a model which places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other. We divide this spectrum into three categories: (1) identified, (2) identifiable, or (3) non-identifiable person.

a) Identified data: An identified person when it singles out a specific individual from others. This means a person has been identified when her identity is ascertained or as stated by the Article 29 Working group, " when, within a group of persons, he or she is distinguished from all members of the group.

b) Identifiable data: The spectrum is broader when is comes to identifiable data. There is need to draw a distinction between nominally identifiable data in which the linkability to a person has not been made but is likely, either due to the nature of the identifiable data and other data available, or due to the likely steps in processing. This ought to be treated at the same level as identified data.

17 Paul M. Shwartz and Daniel Solove, *'The PII Problem: Privacy and a New Concept of Personally Identifiable Information',* 86 NYU Law Quarterly Review 1814 (2011)

On the other hand, where identifiability is not a significantly probable event, it ought to be treated differently.

c) non-identifiable information carries only a remote risk of identification. Such data cannot be said to be relatable to a person, taking account of the means reasonably likely to be used for identification.

Matrix of applicability of the regulations on different categories of data.

Applicability of Privacy Principle	**Identified Data (includes both Unique and Direct identifiers)**	**Identifiable data (probable)** **(includes Indirect identifiers)**	**Identifiable data (improbable)**	**Non-identifiable data** **(Includes Anonymised data)**
Notice	✓	✓	✓	
Consent and Choice	✓	✓	✓	
Purpose Specification	✓	✓		
Collection Limitation	✓	✓		
Disclosure	✓	✓		
Use Limitation	✓	✓		
Deletion	✓	✓		
Data Quality	✓	✓	✓	
Data Security	✓	✓	✓	✓
Transparency	✓	✓	✓	✓
Access, Correction, Portability	✓	✓		
Accountability	✓	✓	✓	✓

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?

The key question is whether anonymised or pseudonymised data automatically be outside the purview of personal data or should they be outside the purview only when the statistically sound methods are used for such de-identification. **In order exempt data from protection, the latter approach is required, which would mean the need for a process and institutional framework to specify such methods**. Examples of such rule: HIPAA's two de-identification methods: 1) a formal determination by a qualified expert; or 2) the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual.[18]

The principles of data protection should not apply to information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not identifiable. However, pseudonymised personal that can be attributed to a natural person by the use of additional information and has to be considered as identifiable personal data.

Additionally, entities must be required to consider whether collection of personal data is necessary for specific identification or if pseudonyms are sufficient. This also adheres to the principle of data minimisation (the logic behind use limitation and purpose specification).[19] Data Controllers can be incentivised to pseudonymise data like the EU GDPR does.[20]

The standards for pseudonymisation and anonymisation and other forms of de-identification needs to be specified in codes of conduct and rules drafted under the data protection legislation based on sectoral data and the state of technology.

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

Refer to answer 4.

---

18 For the de-identification procedure, See *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, available at https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, last accessed on 30-01-2018, and *Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization,* available at https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/, last accessed on 30-01-2018

19 In Australia, Individuals have the option of not identifying themselves or using a pseudonym while dealing with entities. *Supra* note 9

20 For the incentives, See *Top 10 operational impacts of the GDPR: Part 8 - Pseudonymization*, available at https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/, last accessed on 30-01-2018

Chapter 4: Sensitive Personal Data

1. What are your views on sensitive personal data?

To categorise data as sensitive personal data it can be regarded from three overlapping perspectives of its content, purpose and impact. Thereby, when data is sensitive by content, used for purposes such as authorisation or compromise of which can have an adverse impact; it should be regarded as sensitive personal data.[21]

Data Classification

Data classification is broadly defined as the process of organizing data by relevant categories so that it may be used and protected more efficiently. The classification process not only makes data easier to locate and retrieve – data classification is of particular importance when it comes to risk management, compliance, and data security.

Data classification involves tagging data, which makes it easily searchable and trackable. It also eliminates multiple duplications of data, which can reduce storage and backup costs, as well as speed up the search process.

Data classification is carried out for a variety of purposes, one of the most common being a process that supports data security initiatives. But data may be classified for a number of reasons, including ease of access, to comply with regulatory requirements, and to meet various other business or personal objectives. In some cases, data classification is a regulatory requirement, as data must be searchable and retrievable within specified timeframes. For the purposes of data security, data classification is a useful tactic that facilitates proper security responses based on the type of data being retrieved, transmitted, or copied.

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?

Any information which reveals physical, physiological, mental, economic, cultural or social identity is characterised as sensitive personal data. These include the following categories of data should be classified as sensitive personal data:

- Racial, ethnic, religious or caste identity;
- Identifiers such as Aadhaar number, Passport Number, PAN etc.

21 *Reasonable Security Practices IT (Amendment) Act, 2008*, available at https://www.dsci.in/sites/default/files/Reasonable_Security_Practices_Under_IT_Amendment_Act2008.pdf.

- Biometric information including fingerprints, iris scans, facial records, DNA information;
- Political opinions, Membership of trade unions, political groups;
- Religious or other similar beliefs;
- Physical or mental health or condition, or related information;
- Financial information including bank account numbers, transaction history, credit related data etc.; and
- Any information pertaining to sexual life and gender identity;

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

Sensitive personal data should be subject to much stricter regulation than ordinary personal data and must only be processed when one of the following conditions have been satisfied

- The data subject has given explicit consent;
- It is needed in order to protect the vital interests of the individual or another person. For example, an individual with a medical condition has an accident at work; it would be in the individual's vital interest to disclose this condition to medical staff treating the individual.

Chapter 5: What is Processing?

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

Data processing is undertaken by any activity which requires collection of data. It is carried out using a predefined sequence of operations either manually or automatically. This data collected needs to be stored, sorted, processed and analysed.[22] As the ambit of data processing is excessively wide, the definition needs to be able to incorporate all possible activities under its ambit.

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

The definition of processing should be broadly worded to include existing operations while leaving room to incorporate new operations by way of interpretation. Hence five main activities of collection, storage, use, disclosure and deletion should be specified with broad definitions as well. The law should cover both manual and automated processing.

Suggested definition:

Data processing means any operation or set of operations involving personally identifiable information including but not limited to obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including organisation, adaptation, alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of the information or 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?

Refer to

22 *Data Processing | Meaning, Definition, Steps, Types and Methods*, available at https://planningtank.com/computer-applications/data-processing, last accessed on 30-01-2018

Chapter 6: Data Controller and Processor

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

A single organisation that has control over data, should be held accountable for protection of personal data. Rather than enforcing the law on all entities that have any correlation to personal data, it is more feasible for the state to vest responsibility of data to one unit.

However, there is a need for a staggered matrix of responsibility over the the data processors. In terms of compliance responsibility, primary data controllers should be subject to all National Privacy Principles and have the obligation to contractually enforce the same set of obligations on the all secondary data controllers contracted by it. Thus, similarly, when data controllers are in receipt of personally identifiable information from a third party, they are by law subject to the data protection principles as evident in the table below.

Administrative fines should be enforceable against both secondary and primary data controllers, however, compensatory orders should be applicable against the primary data controllers only.

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

The law should 'data controller' and 'data processor' on the lines of the GDPR. The AP Shah Committee Report states that every organization, which determines the purposes and means of processing personal information, will be considered a data controller. Data controllers will be responsible for carrying out the processing of data in accordance privacy principles. No differentiation should made between a controller and a processor and all compliance obligations should placed on the organisation that has control over data.[23]

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

An approach similar to the PIPEDA could be adopted, a data controller (as mentioned in answer 2) would have the sole responsibility to protect personal data. When personal data is transferred to a third party for processing the liability would not shift. The organization would have to protect itself by entering into third party privacy contracts, which would hold the third party accountable to the organization. Also, third party contracts could mandate adherence to the organization's privacy policy to discourage the third party from violating them.[24]

---

23 *Report of the Group of Experts on Privacy by AP Shah Committee*, *Supra* note 11

24 *Privacy Policy Not Enough, 3rd Party Privacy Contract Also Needed To Comply With*

Chapter 7: Exemptions

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

- Personal or household purpose
- Journalistic/artistic/literary purpose
- Research/historical and statistical purposes

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

None of the principles under the data protection law should be applied uniformly across all exemptions. Each exemptions need to be individually defined. For instance, the principle of purpose specification and use limitation may be difficult to mandate in the exemption under research/historical and statistical purposes, as specific research purposes can be difficult to outline before access to data. Similarly, requirements of security safeguards should not be applicable to the exemption under personal/household purposes, as that would mandate all individuals to have the infrastructure to secure data safely, which would a practical nuisance.

Therefore, all exemption needs to be carefully outlined and the data protection law should clarify which principles continue to remain applicable under each exemption.

Domestic /Household Processing

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

An exemption for personal/household purposes may be necessary to ensure that the proposed data protection law does not overregulate and encroach into the private lives of citizens. To ensure the balance between protection of privacy and privacy itself, an exemption for domestic/household purposes should be recognized.

The exemption on personal/household processing also becomes important considering the scope of activities that have the potential to fall within the exemption. Since the task of exhaustively listing all activities that should be exempted under the act is herculean, it is preferable to word the exemption of personal/household processing in a manner that encompasses a broad range of daily processing of data.

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

PIPEDA, available at http://www.carters.ca/pub/bulletin/charity/2005/chylb71.htm

Any processing that is done for personal or household purposes. This can include storage of information on phones, using CCTV cameras to secure private spaces, sharing of information with limited audience etcs, collecting personal information for local activities etc. The goal of the exemption under personal/household processing should be exempt processing of relatively small amounts of data for recreational/personal purposes.

The use of drones for personal use can be a problematic exemption under the law, as drones have the ability to infringe on the privacy of non-consenting parties with ease. Possible solutions can include industry sourced guidelines on the manufacturing and use of drones, as well as the articulation of individual rights against unauthorized collection of their private data.[25] Similarly, CCTV recordings of personal spaces such as households should only be limited to that area, and should not extend to recordings of public spaces.[26] This requirement can be relaxed when the public space is limited to the space immediately vacant to a household (such as the space right outside the door of a house). Additionally, there can be notice requirements for all technologies that invade on the privacy of others without prior consent.

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

Terms such as 'personal', 'domestic', or 'household purpose' will be difficult to define, but should be done so in a broad manner. (**See Answer 1**)

In the context of EU, the exemption for personal purposes has primarily been problematic when an individual has published the data to a wider audience.[27]A list of factors to determine when such publishing should construe to be outside or inside the scope of the exemption will be useful in delineating the scope of the exemption and for any proposed data protection authority when investigating a particular instance of processing.

4. Are there any other views on this exemption?

Due to the difficulty in defining 'personal' or 'household purposes' with precision, any proposed data protection authority should have the ability to investigate whether any instance of processing claimed under the exemption falls within the contours of the exemption or not.

---

25 *Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

26 *Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

27 *Annex 2 Proposals for Amendments regarding exemption for personal or household activities, available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf

Principles such as purpose specification and use limitation should continue to be applicable to processing under this exemption, as otherwise there is potential for the exemption to be misused. However, security safeguards should not be mandatory under this exemption, as all individuals will not have the infrastructure to safely secure data.

Journalistic/Artistic/ Literary Purpose

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

Including journalistic/artistic/literary purpose is important to balance freedom of expression and free speech with a right to privacy. Any data protection law that dilutes the role of journalism in a democracy can set a bad precedent. An exemption under journalistic/artistic/literary purpose should be carefully outlined to avoid curtailing the freedom of media in particular, as not exempting journalistic purpose would prohibit many activities of the media under the guise of data protection.

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

See Answer 1 for whether journalistic purpose be included.

Principles such as consent, notice and use specification should not be applicable to anybody claiming the exemption. However, other principles such as data quality may still be required despite the exemption. The scope under the exemption should be as wide as possible, as other legal resources such as civil and criminal defamation.[28]

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

The government may consider including 'citizens' in the definition of 'journalism', as limiting it to individuals working with established media organizations will limit the ability of interested citizens to engage in journalism for specific purposes. Therefore, the definition of 'journalism' should be broad to include private citizens as well as professional journalists.

The definition of 'journalistic purpose'' should include a loose standard to include broad range of journalistic activities that are currently practiced today. Having journalistic purpose be limited to journalism that is in public interest can severely limit the range of activities that will be considered journalism. Instead, a standard of 'newsworthiness' should be used to define journalistic purpose.[29] The US Supreme Court has defined the test of newsworthiness

28 *The "Journalism Exemption" in the Data Protection Act: Part 1, The Law – Hugh Tomlinson QC,* available at https://inforrm.org/2017/03/28/the-journalism-exemption-in-the-data-protection-act-part-1-the-law-hugh-tomlinson-qc, last accessed on 30-01-2018

29 *The relationship between journalism and data protection: Analysis of the General Data Protection Regulation and recent case law of the European Court of Human Rights,* available at https://lib.ugent.be/fulltxt/RUG01/002/349/659/RUG01-002349659_2017_0001_AC.pdf

broadly to include content that can be "fairly considered as relating to any matter of political, social, or other concern to the community" or when it "is a subject of general interest and of value and concern to the public."[30]

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

The definition of 'journalism' and 'journalistic purpose' should be wide enough to include publishing of information by non-media organization. (See Answer 3 above).

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

Any artistic or literary work that contain personal information about an individual should be included in the exemption, subject to the requirement of a notice. However, sensitive personal data should not be allowed to be reproduced unless there is explicit consent.

'Literary' or 'artistic' purpose should be defined broadly, as both the mediums constantly evolve, and a narrow definition could lead to a situation where bonafide 'literary' or 'artistic' work is not protected under the data protection law.

Research/Historical/Statistical Purpose

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

An exemption for research/historical/statistical purpose will be required to exclude some obligation unders the data protection law which will be detrimental for these purposes.

An exemption under research/historical/statistical purpose should be applicable for private and public research. Since determining research purpose can be difficult before collection of data, the principle of purpose specification should not be applicable under this exemption. Similarly, data collected for research/historical/statistical purposes can be processed in various ways for for different results, and therefore the principle of use limitation should also not be applicable. Notice, however, should still be required to give by researchers for each specific use of the data collected, unless the data has been de-identified.

As a guiding principle, researchers should be required to anonymize or pseudonymize their data to the extent that it is compatible with their research, before they are allowed to use this exemption. The data protection authority must promulgate guidelines on such de-

30 Snyder v. Phelps, 562 U.S. 443 (2011).

identification practices. Researchers should also be required to follow the various national and international ethical guidelines that are already in place for research.[31]

While this exemption may be used by both public and private bodies, it is recommended that it is subject to the test of public interest. Therefore, this exemption may only be employed for activities which may be clearly considered to be in furtherance of a public interest.

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

The data protection authority can be given the power to determine whether any processing of data under the exemption fulfills the criteria of a legitimate research/historical/statistical purpose. This can be done on the basis of how research/historical/statistical purpose will be defined under the data protection act.

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

Subsequent publication of the research should not prevent from the exemption from being applicable Since privacy interest is in the personal data collected for the research, and not the research itself, there should be not restriction on publication. In the even that data is also being published, requirements of anonymization or pseudonymization of data should be met.

Research should also be permitted to be used for commercial purposes, as long as the commercial use is in public interest. The exemption should still be applicable as long as the researchers can show that their commercial application of the research is in public interest, failing which the exemption should no longer apply. This allows the exemption to not be misused by commercial actors who may disguise purely commercial objects as 'research' objectives.

Investigation and Detection of Crime, National Security

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

Investigation of crime and national security can be recognized as separate exemptions under the Act, as their scope can considerably differ. It is imperative to balance the wide scope of these exemptions with sufficient safeguards, as otherwise it leaves open the possibility of

31 A specific example would be the *Ethical Guidelines For Biomedical Research On Human Participants* issued by the Indian Council of Medical Research, available at http://icmr.nic.in/ethical_guidelines.pdf.

the State using these exemptions to justify a wide array of surveillance measures that will infringe upon the constitutional right to privacy. These safeguards can be implemented in the review mechanism for surveillance orders, as well as a requirement for surveillance measures to have legislative (and constitutional) backing. The proportionality test, recognized by a majority in *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors*[32], should be implemented as a standard which all surveillance measure must meet.

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?

Please refer to 8.

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?

Please refer to 8.

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

Please refer to 8.

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

Please refer to 8.

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

Law enforcement agencies should not be exempt from implementing minimum safeguards to ensure that personal data in their possession in stored safely and securely. This exemption much like the others is only a limited exemption. Law enforcement and intelligence agencies would be exempt from the requirements of Consent, Purpose Specification, Use Limitation, but would still be subject to the requirements of Transparency, Accountability Data Security, Data Quality. The rights applicable to the individuals under the data protection law such as access, rectification are also not unavailable but merely suspended while the surveillance or processing activity is pending.

7. Can a data protection authority or/and a third-party challenge processing covered under this exemption?

32 WRIT PETITION (CIVIL) NO 494 OF 2012

In line with the its powers, the data protection authority as well as data controllers should be able to review judicial orders that allow for surveillance, and determine whether the orders meets the test for proportionality. This allow for an additional layer of checks and balances, and allow for the data protection authority to prevent the misappropriation of personal data.

Similarly, once notice has been issues to an individual post surveillance, the individual should be able to move a relevant authority for relief if the individual feels that his right to privacy was violated in a manner that is not consistent with the relevant law.

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

Any surveillance must comply with th International Principles on the Application of Human Rights to Communications Surveillance[33], which are reproduced below.

a. Legality: Any limitation to privacy rights must be prescribed by law and there should be no interference with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Therefore, lawful surveillance can only be carried out under procedures laid down by legislative provisions.

b. Legitimate Aim: Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

c. Necessity: Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means,it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.

d. Adequacy: Any instance of surveillance authorised by law must be appropriate to fulfil the specific Legitimate Aim identified.

e. Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations

33 *International Principles on the Application of Human Rights to Communications Surveillance*, available at https://www.eff.org/files/necessaryandproportionatefinal.pdf,

of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests. This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

i. there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out; and

ii. there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought; and

iii. other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option; and

iv. information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and

v. any excess information collected will not be retained, but instead will be promptly destroyed or returned; and

vi. information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given; and

vii. that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

f. Competent Judicial Authority: Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

i. separate and independent from the authorities conducting Communications Surveillance;

ii. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and

iii. have adequate resources in exercising the functions assigned to them.

g. Due Process: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. Insuchinstances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

h. User Notification: Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstance:

i. Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life; and

ii. Authorisation to delay notification is granted by a Competent Judicial Authority; and

iii. The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority. The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

i. Transparency: States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope,nature,and application of the laws permitting Communications Surveillance. States should not interfere with

service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance

j. Public Oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.Integrity of Communications and Systems: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, the policies should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for surveillance purposes.

k. International Co-operation: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

l. Safeguards against Illegitimate Access: States should enact legislation criminalising illegal Communications Surveillance by public or private actors.

The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.

Additional Exemptions

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

Prevention of crime should not be separately included as a ground for exemption, as it has the potential to be used to as a justification for bulk surveillance, which would in contradiction to the jurisprudence of privacy as a right laid out by the Supreme Court in various cases.

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

A limited exemption can be considered under assessment and collection of tax, and only in instances where following the provisions of the data protection law will be prejudicial to the purpose of collection i.e. assessment and collection of tax, otherwise the relevant authority must comply with the provisions.

Chapter 8: Cross-Border Flow of Data

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

Ensuring cross-boundary transfer of data with minimal restrictions is necessary in India, as many of the services and facilities available to Indian consumers require transfer of their personal data to other countries. Restrictions on cross-boundary transfer will create issues for various services that rely on the free flow of data, as well as impair trade of services in general. However, the government also has the prerogative to ensure that the data of its citizens is protected from misuse and exploitation at the hand of foreign companies and governments.

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

The data protection law should facilitate cross-boundary transfer by provisions that clarify issues relation to jurisdiction and liability that arise from such transfer.

The adequacy standard is not a helpful standard for determining where data can freely flow. Determining the adequacy of each country can be an expensive, time-consuming and restrictive process as most countries in the world are yet to implement standards and laws for data protection. Additionally, in federal countries the adequacy standard is difficult to implement as each state might have different standards of protection.[34]

Other mechanisms implemented by the EU, such as standard contract clauses and binding corporate rules might provide a better mechanism for facilitating cross-boundary 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?

The transfer of sensitive personal information should not be prohibited. Since sensitive personal information can be contextual, it should be left to the individual to determine whether his sensitive personal data can be transferred for a specific purpose.

The government can additionally mandate a higher standard of security for cross-boundary transfer of sensitive personal data.

---

34 Lingjie Kong; Data Protection and Transborder Data Flow in the European and Global Context, *European Journal of International Law*, Volume 21, Issue 2, 1 May 2010, Pages 441–456, https://doi.org/10.1093/ejil/chq025

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

Cross-boundary transfer of data are already permitted under various Mutual Legal Assistance Treaties (MLAT) signed by India. It is important to clarify how new provision relating to cross-boundary transfer of data will affect existing legal obligations under MLATs. Restrictions under cross-boundary transfer of data can also affect obligations under international trade law, such as GATS.

It is also important for India to achieve adequacy status within the EU, so that unhindered cross-border flow of data may continue between the two regions. India should not longer rely on model contract clauses for cross-border flow of data as their validity as a mechanism for data transfer with sufficient protection is currently being challenged.[35] The High Court of Ireland, on the basis of a finding by the Irish Data Protection Commissioner that standard contractual clauses do not provide sufficient protection to EU citizens, has permitted a reference to the Court of Justice of the European Union (CJEU), who may now decide on the validity of the standard contract clauses.[36] While the case and reference deal with the transfer of EU personal data to the U.S., any decision of the CJEU will have repercussions on the transfer of personal data between EU and India as well. Previous studies have estimated that getting an adequacy status could translate into an increase in annual revenue in services from from EU up to USD 50 million.

There is a need to set up a data protection authority which can engage in with different regional and international arrangements such as the APEC Cross-border Privacy Enforcement Arrangement, the ASEAN Framework on Personal Data Protection, Consultative Committee of Council of Europe Convention 108, the International Conference of Data Protection and Privacy Commissioners

35 Here We Go Again: Schrems 2 Puts the Model Clauses for Transfer of EU Personal Data in Doubt, available at https://www.lexology.com/library/detail.aspx?g=2b8e2ad4-1964-431f-9c3d-845a8278a96d, last accessed on 29-01-2018

36 *The Data Protection Commissioner v. Facebook Ireland Limited & anor,* [2017] IEHC 545

Chapter 9: Data Localisation

1. What are your views on data localisation?

Requiring local storage of the personal data of citizens can be a problematic endeavor, as it will create issues of trade, security and quality of service. India should not be overly protectionist in managing the data of its citizens, and should allow for data collectors to store data outside the country, as long as the data collectors are subject to certain rules and standards.

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

There should not be a data localisation requirement for the storage of personal data within the jurisdiction of India.

As data localization requires that all personal data relating to citizens be stored within national boundaries, it creates issues of security by making it easier for the State, or other parties, to exercise surveillance over its population or to misappropriate the data for other purposes.[37] Since all information is localized, there is repository of information that is easier to locate and available in higher volumes. If there are no data localisation requirements, personal data of citizens becomes dispersed around the globe.

Data localization requirements will also be restrictive on individual liberty, as it will severely restrict the services that Indian consumers can access.

The government should adopt an approach where data can be transferred across boundaries, subject to any mechanism that the government chooses to implement (such as standard contract clauses) that will ensure minimum security for the data, and create liability in case the data is breached or misused.

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

Please refer the answer above.

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

Requiring data localization will affect the decision of foreign companies who are willing to offer their services in India. Many such services rely on cross-boundary transfer of data, such

37 Chander, Anupam and Le, Uyen P., Data Nationalism (March 13, 2015). Emory Law Journal, Vol. 64, No. 3, 2015. Available at SSRN: https://ssrn.com/abstract=2577947

as cloud computing or IoT, and to require them to store data locally would contradict their business model and be cost ineffective for such companies. For these reasons, they will be hesitant to offer their services in India.

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

It is important to note that data localisation is not a binary issue. There are different forms of data localisation which can be implemented.

For instance, for all government data, particularly critical information infrastructure data, it should be mandatory for keeping the data within India. Similar, for all intelligence data, armed forces sensitive data and sensitive data maintained by law enforcement agencies, its is strategically imperative that such data is stored in India only.

For certain, other kinds of data, the data protection law or rules under it could mandate that a copy of the data is always maintained in India. For instance, telecommunication companies may be required to maintain a copy of their data in India.

For other kinds of data, where it relates particularly to sensitive personal data, the law could mandate that before that are exported, there are mechanisms such as standard contractual clauses or binding corporate rules or safe harbour arrangements to ensure that they are retain the same degree of protection.

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

Chapter 1: Consent

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

In the same way as medical research evolved from a researcher-subject relationship at an individual level, to one of large-scale population studies, so too have commercial relationships evolved. Collection, use and disclosure of data in the commercial context have moved from binary exchanges between buyer and seller, to complex ecosystems involving third party intermediaries who experiment in Big Data, in ways largely invisible to consumers.

In most data protection regimes world-wide, consent functions as a way for individuals to protect their privacy by exercising control over their personal information. The simplicity and elegance of this paradigm is that in one fell swoop, it seeks to ensure that consent is informed and free, and thereby also to implement an acceptable tradeoff between privacy and competing concerns. This approach is also easy to enforce for both regulators and businesses. Data collectors and processors only need to ensure that they comply with their privacy policies, and theoretically, consumers have the information required to exercise choice. The previous two drafts for privacy legislations in India also emphasised on the primacy of the notice and consent framework, as did the Report of Experts under Justice AP Shah for the Planning Commision of India which articulated nine National Privacy Principles.

The notice and consent framework is often rendered meaningless by (a) long and complicated privacy notices that provide blanket consents to the data collectors, (b) ubiquity of data collection and sharing through online services, smartphones and IoT devices, and (c) big data enabled analysis which brings together disparate data points to create an intimate picture of a data subject.

Having said the above, revisiting the principle of notice and consent needs to be a carefully calibrated exercise. While the consent framework has not worked well, proposals to discard consent are futile without a clear and viable alternative. It does mean we need to revisit how we apply consent and acknowledge that in some justifiable cases, consent may simply be impossible or impracticable. We recognize that certain data uses are sufficiently beneficial and compelling from a societal perspective to warrant finding other practical solutions.[38]

38 *Consent as A Universal Principle in Global Data Protection,* available at https://www.priv.gc.ca/en/opc-news/speeches/2017/sp-d_20170515_pk/, last accessed on 30-01-2018

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?

The criteria of valid consent as enumerated in the GDPR help in delimiting the standards of consent and help in authenticating the validity of consent and should be adopted in the data protection law.

It is necessary to mandate that consent is freely given .The GDPR now clarifies that consent will not be freely given if: the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment (Recital 42); and/or there is a clear imbalance between the data subject and the controller (Recital 4) . These provisions should be incorporated in the Indian data protection law as well

The provisions regarding consent should also be inclusive of right to withdraw and in some cases it should be mandatory to obtain explicit consent when the data in question is extremely sensitive such as biometric details.

In order to make consent meaningful, it is recommended that the following particulars are built in the language of the legislation.

Timing of the privacy notice

The privacy notice shall be provided at the time of collection from the data subject, and, where the personal data are obtained from another source, after receipt of data from such source. Further, the data protection authority must explore, incentivise and mandate evolving standards and norms for provision of privacy notices in a repetitive manner which ensure repetition of notice when the activity in question is relevant to the privacy interests of the individual.

Contents of the privacy notice

The privacy notices should include the following information:

1. What personal information is being collected;

2. Name and contact details of the entity collecting the data;

3. Purposes for which personal information is being collected;

4. Uses of collected personal information;

5. Whether or not personal information may be disclosed to third persons, and the third party recipients or categories of recipients of the personal data;

6. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

7. The manner in which it may be accessed, verified and modified;

8. The procedure for recourse in case of any grievance in relation to collection and processing of data

9. Security safeguards established by the data controller in relation to the personal information;

10. Contact details of the privacy officers and ombudsmen for filing complaints.

Form of the privacy notice

The privacy notice should be easily accessible, easy to understand, in clear, plain, intelligible, easily legible and concise language that a reasonable person without any legal or technical training can comprehend, and must follow any standards or formats that the data protection authority or the relevant sectoral regulatory bodies specify. The privacy notice ought to be a meaningful overview of the intended processing of the data collected.

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

It is recommended that the data protection authority created under the data protection legislation is given powers to take steps to ensure that the use of privacy enhancing technologies is incentivised through seals, certifications, standards and norms. While in the interest of technological neutrality, the authority ought not to prescribe the use of specific technological solutions, the authority should be proactive in endorsing and incentivising the use of approaches to the design of technology that preserve and enhance the privacy of individuals. We provide an illustrative list of such approaches below.

Sticky privacy policies[39]

Sticky privacy policies involve cryptographic solutions in which policies can stick to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information. They allow the data subject to decide on a set of conditions and constraints which unambiguously lay down how her/his PII is to be used by the party receiving the data. As the data moves across multiple parties, these policies define an allowed usage and obligations, thus enhancing the control of the data owners over their personal information. They impose prohibitions and obligations such as access of third parties and the purpose for which the data is being used. These policies also allow the data owners to blacklist certain parties from gaining access to their personal

39 This solution can aid the Notice and Consent principles.

information along with laying down rules such as a notice of disclosure and the deletion or minimization of data after a specified period of time.

Personal Data Stores[40]

A Personal Data Store or PDS helps you gather, store, manage, use and share the information. It gives the user a central point of control for their personal information (e.g. interests, contact information, affiliations, preferences, friends). For instance, openPDS can be installed on any server under the control of the individual (personal server, virtual machine, etc) or can be provided as a service (SaaS by independent software vendors or application service providers). Additionally, tools like SafeAnswers[41] can turn an algorithmically hard anonymization and application-specific problem into a more tractable security one by answering questions instead of releasing copies of raw data.

DND for the Internet Age/One Click Consent withdrawal[42]

In the case of implementing the principle of Opt Out, data subjects should be provided with options such as a.) no further collection of data, b.) erasure of all previously collected data and the results of processing of such data. In certain cases, it may not be in the public interest to allow erasures of decisions already made on the basis of data collected. This could be facilitated by a system such as a Centralised website/service/phone number/email number - where an individual can withdraw consent easily, for instance through a single SMS for which the syntax is easy to use. Services providers could be automatically informed of such choices, or they could access the details of the users who have opted out periodically (daily or bi-weekly basis) and effect changes. In order to prevent mistaken removal of users, an additional layer of confirmation through email/SMS can also be built in.

Standardized Privacy Notices[43]

The form in which notices are presented is extremely important. Therefore, summaries, infographics, highlighting relevant and actionable information can go a long way in making notices much more intelligible to laypersons. Some existing models of standardized formats for simple and easy to use privacy notices include the following: i) National Telecommunications and Information Administration (NTIA) developed a code of conduct for standardized short-form privacy notices for smartphone app.[44] ii) Private Parts is a web based service to simplify privacy notices. [45]

---

40 This solution can aid the Consent principle.

41 de Montjoye Y-A, Shmueli E, Wang SS, Pentland AS (2014) *openPDS: Protecting the Privacy of Metadata through SafeAnswers*. PLoS ONE 9(7): e98790. https://doi.org/10.1371/journal.pone.0098790.

42 This solution can aid the Opt Out principle.

43 This norm can add to the Notice principle.

44 *Short Form Notice Code Of Conduct To Promote Transparency In Mobile App Practices*, available at https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

45 *Lookout Open Sourced Its "Private Parts," You Should, Too*, available at https://blog.lookout.com/open-source-privacy-policy, last accessed on 30-01-2018

Privacy Commons[46]

The development of Privacy Commons Notices on the lines of Creative Commons Licenses can be a useful soft standard for recognised, easily understood privacy notices which are human and well machine readable. Not only will it increase awareness of key terms in privacy notices, this will also creates an incentive for service providers to improve their privacy policies if they want to claim that they use Privacy Commons Notice. Also, in the chain of big data co-controllership and information sharing, privacy preferences of the data subjects may often be neglected or not adequately considered which creates the need for automated policy definition and enforcement so that one party cannot refuse to honour the policy of another party in the chain of big data analytics. For this, the research community and the big data analytics industry needs to explore the area of privacy policy definition and to embody relevant mechanisms for automated enforcement of privacy requirements and preferences.[47] Creating a set of easily-understood Privacy Icons that "bolt on to" a privacy policy. When you add a Privacy Icon to your privacy policy it says the equivalent of "No matter what the rest of this privacy policy says, the following is true and preempts anything else in this document…". The Privacy Icon makes an iron-clad guarantee about some portion of how a company treats your data. For example, if a privacy policy includes the icon for "None of your data is sold or shared with 3rd parties", then no matter what the privacy policy says in the small print, it gets preempted by the icon and the company is legally bound to never sharing or selling your data. Of course, the set of icons still needs to be decided.[48]

Privacy Dashboards

Privacy dashboards can also be applied to manage privacy settings in the IoT environment. For example, mobile applications, such as Apple's HomeKit, that allow users to configure and control their IoT devices could also provide for a privacy dashboard to exercise user control across all such devices.132 Similarly, "companies developing 'command centers' for their connected home devices could incorporate privacy dashboards". There are moreover privacy dashboards of data brokers and more recently in the financial services sector

Privacy by Design

Privacy by design refers to the practice of technological and organisational measures to embed data protection principles in systems and services by way of implementing privacy enhancing technologies (PETs) and principles such as data minimization directly into the

46 This norm can aid the Notice principle.

47 *State of the Art Analysis of Data Protection in Big Data Architectures*, available at https://iapp.org/resources/article/state-of-the-art-analysis-of-data-protection-in-big-data-architectures/, last accessed on 30-01-2018

48 Is A Creative Commons for Privacy Possible?, available at http://www.azarask.in/blog/post/is-a-creative-commons-for-privacy-possible, last accessed on 30-01-2018

design of information technologies and systems. Effective implementation of these principles require incentives and legal obligations from the regulators so that data protection becomes an integral part of the technological design and organizational structure of services providers.

Privacy by default

Privacy by default is a principle intended to counter the wide use of privacy policies and terms of conditions by services providers to nudge users towards least privacy preserving choices by having maximum data collection and blanket consents as defaults. Implementation of privacy by default would entail that the strictest privacy settings automatically apply when a user signs up for a service. This would be done by ensuring that the default privacy settings would always lean towards privacy enhances choices and technological implementation of the data minimisation principle by automating deletion of data once the purpose has been fulfilled.

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

Inability to provide informed consent

The notice and consent principle relies on the ability of the individual to make an informed choice after reading the privacy notice. The purpose of a privacy notice is to act as a public announcement of the internal practices on collection, processing, retention and sharing of information and make the user aware of the same.[49]However, in order to do so the individual must first be able to access the privacy notices in an intelligible format and read them. Privacy notices come in various forms, ranging from documents posted as privacy policies on a website, to click through notices in a mobile app, to signs posted in public spaces informing about the presence of CCTV cameras.[50]

About 27% of India's population is still illiterate or barely literate. Most privacy policies and terms of services for web and mobile applications are in English and therefore it is only 10% of us who can actually read them before we provide our consent. Even if we can read them, we may not have the necessary legal training to understand them.

There is a need for the data protection authority to encourage the model of a Consent Broker by modifying the concept of the Account Aggregator in the Master Direction from RBI titled "Non-Banking Financial Company Account Aggregator Directions,". Like the Account Aggregator proposal, we would want a competitive set of consent brokers who will manage consent artifacts for data subjects. However, I believe there should be a 1:1 relationship

49 Florian Schaub, R. Balebako et al, *A Design Space For Effective Privacy Notices,* available at https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf.

50 Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, 2006.

between data subjects and consent brokers so that the latter compete for the business of data subjects. The consent broker must have an “arms-length distance” from data controllers and must be prohibited from making any money from them. Consent brokers could also be trusted to take proactive actions for the data subjects, such as access and correction.

Context specificity

Theory development based on context specificity is an emerging area of theory building. The word context in its Latin root means knitting together or making a connection. A more salient definition of context is given by Mowday and Sutton: “context encompasses stimuli and phenomenon that surround and thus exist in the environment external to the individual.”

Context could relate to time, location, or individual attributes. For example, examining individual behaviors before and after a major traumatic event could be a contextual study where the context variable is time (when). A comparison of individual behaviors across occupational domains such as professionals versus students could be categorized as a contextual study where the contextual variable is demographics (who). The context variable in a study of factors impacting job performance in the urban and rural settings is location (where). Context can moderate the nature and extent of relationships. People understand what is going on by understanding where and when it is happening. In order to understand a phenomenon, it is important to analyze its context, since meaning is derived from the context.

While the framework of notice and consent must serve as the basis for the omnibus data protection legislation applicable to all sectoral, it is important that sectoral codes are created based on the omnibus law, which take into context specific factors, to make rules about data sharing and processing in a given sector. For instance, use of sociological disciples such as prospecs theory to understand the how the sensitivity of context moderates the paths leading to intention to disclose private information in say, the finance sector. Thus could guide the creation of sector specific rules.

Chapter 2: Child's Consent

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

The contract law in India states that only those contracts entered into by individuals over the age of 18 year are valid. Due to the manner in which services are provided online, there may be a need for differential requirements. The digital age of consent for children can be grouped as between below 13 years (consent only by parent or legal guardian), 13 - 18 years (or possibly 16 years – with parental consent) and above 18 (consent of the user is sufficient). For guidance, we can look at the examples of COPPA in the US, which requires online services directed towards children to obtain verifiable parental consent before collecting personal information.

3. 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?

The law need not prohibit the processing of personal data relating to a child as long as parental consent is obtained by data controllers.

4. 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?

The provisions in the Australian Privacy Act rely on the judgment of the data controllers that it has determined on a case-by-case whether that individual has the capacity to provide consent. There is lack of clarity and judicial guidance over how this determination may be made. Further, in cases of automated collection of data, it is extremely difficult to meaningfully enforce this law. It is therefore, recommended that instead of following the Australian model, we rely on the US or EU model.

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

Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or

(vi) Provided that, a data controller that does not disclose children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call.

6. 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?

A piece of legislation aimed at protecting children from the influence of advertisers is the Quebec Consumer Protection Act. This Act, enacted in 1987, has banned any advertising directed at children under the age of thirteen. The regulations passed pursuant to the Act contain a rather complex scheme of exemptions. While this Act does not consider the issues of online privacy or data-management, it does provide an example of how commercial activities have been limited to protect children's interests. The general view taken by the Quebec legislature and supported by Canadian courts is that under the age of thirteen children are particularly susceptible to the manipulative content of advertising campaigns and a similar approach can be considered to be adopted under the Indian Data Protection regime.

Chapter 3: Notice

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

Yes, Please refer to the Chapter on Consent.

2. How can notices be made more comprehensible to individuals ?

Please refer to the Chapter on Consent.

Different notices for different audiences

To determine the different audiences for privacy notices, the set of all data practices specified in the privacy policy needs to be analyzed to determine which data practices affect which audience. Typical audience groups are the primary user of a system; secondary users, such as household members, having potentially less control over the system; and incidental users, such as bystanders, who may not even be aware that information about them is collected by a system. Depending on the system, other or additional

audience groups may need to be considered. There may also be regulatory requirements applying to specific audience groups, such as children, that have to be considered.

Relevant Information

A privacy notice must contain relevant information that is for each data practice, all parameters relevant for creating a notice should be gathered. For instance, for a data collection practice this may include by whom information is collected, why, how it is used, for how long it is retained, and if and how it is eventually deleted. For third party sharing practices, it is relevant with whom information is shared, why, and whether and how usage is restricted or limited in time.

Layered notices

While it may be essential to be transparent about many aspects of a system's data practices, showing everything at once in a single notice is rarely effective. Instead, all but the most simple notices should consist of multiple layers. Multilayered notices constitute a set of complementary privacy notices that are tailored to the respective audience and the prevalent contexts in which they are presented. The granularity of information provided in a specific notice layer must be appropriate for the respective context. **A good practice is to prioritize what and when notices are shown based on privacy risks associated with the respective data practice**

User testing and usability evaluation of notices can be integrated into a system's overall evaluation and quality assurance processes. Evaluating the construction of privacy notice designs on the basis of **timing , channel , modality and control**

3. Should government data controllers be obliged to post notices about how the data will be processed ?

All data controllers irrespective of being government or private must inform the data subjects of the manner in which their data will be processed . There needs to be a set of guidelines which needs to be instituted for all data controllers both government and the compliance with these guidelines must be made mandatory.

The privacy notices should include the following information:

1. What personal information is being collected;

2. Name and contact details of the entity collecting the data;

3. Purposes for which personal information is being collected;

4. Uses of collected personal information;

5. Whether or not personal information may be disclosed to third persons, and the third party recipients or categories of recipients of the personal data;

6. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

7. The manner in which it may be accessed, verified and modified;

8. The procedure for recourse in case of any grievance in relation to collection and processing of data

9. Security safeguards established by the data controller in relation to the personal information;

10. Contact details of the privacy officers and ombudsmen for filing complaints.

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

There is a multiplicity of privacy notices which exists for different kinds of transaction and for obtaining multiple categories of data , providing prescriptive provisions under a singular data protection law will standardise the notices but such standardisation is neither desirable nor possible . Even sectorally prescribing formats for every transaction is a tedious task . Therefore it is suggested that the data protection law should lay down succinct parameters for valid privacy notice such as relevant information , easy to understand and accessibility

of the notice and the effectiveness of each notice should be adjudged keeping those broad parameters in consideration.

Please refer to the technical solutions: Standaradized Privacy Notices and Privacy Commons in the Chapter on Consent. The use of such standards should be incentivized but not made mandatory.

5. How can data controllers be incentivised to make effective privacy notices?

Data trust scores is an effective method for data subjects to evaluate whether they would be comfortable with sharing their data with a particular entity and low data trust scores would mean less business for corporate bodies and hence it would act as an effective incentive for body corporates to strengthen their privacy systems .

The data protection authority would be the appropriate authority carry out the assignment of data trust scores these scores could be assigned after conducting privacy impact assessments or assessing the existing data privacy mechanisms of data controllers and also take into data leakage risks into account . Such scores must be available in the public domain for the data subjects to evaluate the standard of data privacy of the existing data controllers.

Well-designed privacy dashboards currently represent, in our view, the most feasible strategy among those existing mechanisms and promising new approaches for enhancing user controls we reviewed. Privacy dashboards are user interfaces that provide as a single point of access to information on the collection and use of personal data as well as the configuration of privacy settings by users. At the present moment privacy dashboards present a realistic scenario that is attuned to the online, mobile and platform economy and has gained traction in the market. Conceptually, privacy dashboards can be designed to meet privacy by design and usability criteria, and, via the configuration of default-settings, they can be adjusted to different legal systems. In addition to respecting applicable legal defaults, privacy dashboards should be aligned with the principles of ‘privacy by design’, ‘user centricity’ and ‘minimum asymmetry’ between those who control a technology and users. Online intermediaries and platforms are in the best position to implement privacy dashboards that offer users scalable and persistent controls in their ecosystem.

6. Are there any other alternatives other than the ones mentioned above for making notices more effective?

Please refer to the solutions listed in the Chapter on Consent.

Chapter 4: Other Grounds of Processing

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

As opposed to the EU, where the GDPR envisages six different grounds for processing, in India, the Puttaswamy judgment is clear in placing informed consent at the centre of any data protection law. As the White Paper also states "in the absence of interpretative guidelines, it may not be possible to import these grounds to the Indian context". We are of the opinion that informed consent is the primary grounds for processing of data, and any other grounds that are also articulated must be limited and also draw their legitimacy from the principle of informed consent.

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

A) Vital Interest:

This ground may be used only in very limited circumstances, such as where there is a there is a threat to the life or health of the individual. This ground must only be used to protect an interest essential to the life of the individual. As stated above, this is a limited ground and must be used only in cases where waiting to obtain consent may cause direct threat to the vital interest of either the data subject or another person.

However, this ground may not be used not in situation where the data controllers does not have the intention of seeking consent of the data subject, for instance in the case of surveillance by law enforcement agencies. It ought to be used only in situations where the data controllers, in ideal circumstances, would obtain consent, but in a given situation, waiting to obtain consent may pose a threat to a vital interest.

B) Performance of a contract:

The White Paper speaks of two kinds of situation where the ground of performance of the contract may be employed. The first case is a limited one where rocessing is necessary for the performance of a contract to which the data subject is a party. This is a strictly interpreted provision and does not cover situations where processing is not genuinely necessary for the performance of a contract, and is unilaterally imposed by the entity processing information.

The second case is however a little broader, where it is intended to cover any processing activity, which could take place prior to entering a contract. This includes pre-contractual relations, where the steps are taken at the initiative of the individual. Often upon entering into a contract, it may retrospectively cover such pre-contractual activities. The issues is in cases where the relationship may not formalise into a contract.

The basis for both kinds of processing is that of consent, where the data subject has agreed to either expressly or impliedly by entering into a contract (or demonstrating a clear intent to enter into a contract) to allow the data controller to carry out activities which may involve processing of the her data.

C) Legitimate Interest

The notion of legitimate interest was first introduced in the EU Directive 95/46/EC under Article 7 and has subsequently been adopted in the GDPR under Article 6. In both contexts, the purpose of legitimate interests is to provide an additional ground for processing of personal data which also includes consent, contractual arrangement, legal obligation or other specifically identified rationale as other grounds for processing. In brief, legitimate interests involves taking into consideration the nature and source of the legitimate interest, the impact on the interest, fundamental rights and freedom of the data subject and the nature of safeguards in a balancing test before a conclusion is reached on whether the legitimate interest can be a lawful ground for processing in that specific instance.

The Article 29 Data Protection Working Party, in its opinion on legitimate interests[51], gave detailed guidelines on the factors to take into consideration when the balancing test under legitimate interests is being done by the data controller, which are summarized below –

a. Assessing the controllers legitimate interest – taking into consideration the right of the data controller to exercise fundamental rights, the public interests or the interests of the wider community, other legitimate interests and the legal/cultural/societal recognition of the legitimacy of the interest

b. The impact on data subjects – assessment of the impact on the data subject, whether positive or negative, as well as the nature of the data, the way data is being processing, reasonable expectations of the data subject and status of the data controller and data subject

c. Safeguards – taking into consideration the nature of the safeguards being provided for the interests of the data subjects, such as measures that incorporate transparency and accountability as well as providing opt-in or opt-out consent and the right to access the data.

The Article 29 Working Party also recommended that regulations including legitimate interest as a ground implement a recital with key factors to consider when applying the test, to require the controller to document the assessment whenever

51 *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, available at http://www.dataprotection.ro/servlet/ViewDocument?id=1086.

appropriate, and to include a substantive provision for the controllers to explain to the data subject why they believe their interests would not be overridden by the data subjects' interests, fundamental rights and freedoms.[52]

Lokke Moerel and Corien Prins[53] also propose the following factors to take into consideration when balancing interests of the data controller and the data subject:

- Collective interests
- Nature of the data
- Nature of the relationship
- Informational requirements and right to access and rectification
- Accountability and transparency requirement

The Indian context – Who should do the balancing?

The Article 29 Working Party in its opinion, as well as Lokke Moeral and Corien Prins in their paper argue for the data controller to incorporate the balancing test when claiming data processing as a ground for processing of personal data. Lokke Moerel and Corien Prins specifically note that the task of the controllers would be to interpret the balancing of interests on the basis of available factors, and to make explicit the considerations in an open and public manner.[54] It would be suitable to implement the same model in India and have the data controller be responsible for determining whether his interests are legitimate enough to provide for a legal ground for processing of personal data.

The balancing test outlined above involves extremely contextual information, such as the specific interests of the data controller, the nature of the relationship between the data subject and the data controller, the safeguards implement in that specific transaction etc. Therefore, to task any other authority or party other than the data controller to conduct a balancing test on every instance where the legitimate interest ground is being invoked would be a logistical nightmare. It is useful to refer to the recommendation of the Article 29 Data Protection Working Party for guidance on how the test should be implemented. Any implementation of legitimate interest in India should be accompanied with codification of the relevant factors that should compulsorily be taken into consideration when the balancing is being

52 *Id*

53 Moerel, Lokke and Prins, Corien, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (May 25, 2016).

54 *Id*, Page 76

done by the data controller. Additionally, the balancing should be documented in a predetermined format, which should be included in the rules accompanying the data protection legislation, and which incorporate the various factors that are relevant to the balancing of interests.

For the purpose of enforcement, the data protection authority should be tasked with review of the documented assessment of interests on the basis of appeal by a data subject (or any other party). Making the data protection authority the first point of appeal rather the party responsible for assessing the interest prevents the data protection authority from being overburdened.

Processing under Legitimate Interest[55]

The data controller may process data for purposes other than those expressly consented to by the data subject in cases where it can demonstrate the existence of a legitimate interest. This legitimate interest of the data controller shall be limited by the interests of the data subject which require protection of data. Factors relevant for determining the existence of a legitimate interest shall include the the reasonable expectations of data subject, whether processing leads to an adverse impact on the data subject, overriding public interest, nature of the data that are processed (sensitive or not), the relationship between the data subject and the controller and their respective positions of power, and the measures that the controller has taken to reduce the impact on the privacy of the individuals.[56]

Right to access information regarding processing under legitimate interests

All data subjects shall have the right to access the grounds on the basis of which legitimate interest principle is being used to process data beyond the purposes to which the data subject has consented. In cases where the data subject contests the legitimate interests for the processing of data by the controller for purposes for which consent of the data subject has not been taken pending the demonstration of the legitimate interest by the data controller, the data subject has the right to restrict the processing of the data in question.

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?

Please refer to 2.

55 The legitimate principle has been a part of European jurisprudence and is also reflected in the GDPR as one of the criteria for lawful processing.

56 Lokke Morael and Corien Prins, Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016), available at http://dx.doi.org/10.2139/ssrn.2784123

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

Please refer to 2.

Chapter 5: Purpose Specification and Use Limitation

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

The purpose specification and use limitation principles have been the cornerstone of data protection law globally. The only way individual can have control over their data is by having knowledge about the purpose for which their data is being used.

The principles of purpose limitation or purpose specification seeks to ensure the following four objectives:

- Personal information collected and processed should be adequate and relevant to the purposes for which they are processed.

- The entities collect, process, disclose, make available, or otherwise use personal information only for the stated purposes.

- In case of change in purpose, the data's subject needs to be informed and their consent has to be obtained.

- After personal information has been used in accordance with the identified purpose, it has to be destroyed as per the identified procedures.

It has been argued that these principles are in direct conflict with new technology which relies on ubiquitous collection and indiscriminate uses of data. The main import of Big Data technologies on the inherent value in data which can be harvested not by the primary purposes of data collection but through various secondary purposes which involve processing of the data repeatedly. Further, instead to destroying the data when its purpose has been achieved, the intent is to retain as much data as possible for secondary uses. Importantly, as these secondary uses are of an inherently unanticipated nature, it becomes impossible to account for it at the stage of collection and providing the choice to the data subject.

Therefore, big data proponents claim that the focus of regulation should be on use, and not on collection. However, while considering these arguments, also reflected in the White Paper, it is important to carefully dissect this view, which has been termed as 'Big Data exceptionalism' by Helen Nissenbaum.

Its key assertions are that 1) characteristics inherent to digital technologies make collection inevitable and unavoidable; 2) inherent characteristics of big data make it impossible to anticipate in advance what knowledge may be extracted and what purposes served by large data aggregations; and 3) not exploiting the promise of big data to its fullest will be costly to society; 5) to address harms and risks typically associated with threats to privacy the regulation data use is sufficient.

We would dispute the above. In support of deregulating collection, proponents cite use of data for progress on the world's problems of economy, health, and security. Data available for public and public interest research is a small fraction of data held in private, commercial hands, for that matter, concentrated in the hands of a few dominant actors. These actors effectively hoard the data, obligated neither to pursue beneficial and progressive applications, nor to open their troves to third parties to do so. nor even to allow access for inspection and scrutiny of their internal practices.

We have suggested alternate grounds for processing that may extend beyond the purpose specification and use limitation principle, which could be used where data is being used for legitimate interest purposes. Such alternate grounds are better suited to address use cases in public interest rather than arguing substantial de-regulation.

Further, the big data exceptionalism proposition comprises two interdependent halves: lifting restrictions on collection counterbalanced by restrictions on use. There is a lack of viable concrete proposal on how data usage may be regulated. There is significant debate about what use regulation ought to achieve and ways to go about it. **Therefore, the principles of purpose specification need not be discarded in a hurry. Rather, we would recommended an incremental model, which would seek to build the data protection legislation around consent and purpose specification, and seek an active role by the data protection authority in exploring ways to incorporate use regulation in the codes of conduct and other subordinate processes.**

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

The Compatibility principle

The compatibility tests, as configured in the GDPR provides some guidance to allow the purpose specification principle to be retained while also accommodating new technologies. According to it, processing may be carried out for secondary purposes as long as they are not incompatible with the original purpose. This is a lower threshold keeping in mind the appetite for data that newer business models and technologies have. It must be noted that that the test is that of compatibility and not of identical purpose, while processing for secondary purposes. Or significantly, the burden on the data controllers is not to show compatibility, but merely the absence of incompatibility. **While we agree with the compatibility test, we recommend as slightly higher threshold, i.e., for data controllers to have the burden to demonstrate compatibility**.

Article 6 (4) GDPR provides that that when performing the compatibility assessment, the following criteria shall, inter alia, be taken into account:

> (i) Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(ii) The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(iii) The nature of the personal data, in particular whether special personal data are processed,

(iv) The possible consequences of the intended further processing for data subjects;

(v) The existence of appropriate safeguards, which may include encryption or anonymization.

Anonymisation of Data

Open ended Big Data applications where the analysis gives answers to questions that have not been asked before face certain limits here. In order to be in compliance with data protection rules in such cases anonymization of the data may be an option although it also needs to be said that anonymization becomes increasingly difficult in Big Data scenarios due to risks of re- identifiability.

Big Data applications that involve further processing of personal data for scientific and statistical purposes do not face considerable obstacles if appropriate safeguards for the data subject are maintained. The establishment of such safeguards is, of course, consuming resources on the side of the data controllers. Data controllers wanting to further use personal data for Big Data analysis in order to gain information about particular individuals and/or make decisions affecting them do indeed face larger obstacles to further process the personal data in compliance with the purpose limitation principle. For example, if an organization is aiming to further process the personal data of their customers in order to analyze or predict the personal preferences and behavior of individual customers in order to use such information to base decisions regarding them, then the data controller will be required to obtain the informed consent of those customers.

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?

Data Controller should be responsible for making such a determination .The data controller must consider carefully, after specifying the purpose, whether the collection and/or processing of the personal data is necessary for the aim he pursues. In order to support transparency and also to improve enforcement of the purpose limitation principle, data subjects must be informed by the data controller of the purpose of the collection.

In case the privileging rule for further processing for historical, statistical or scientific purposes does not apply, a compatibility assessment must be conducted .

The Article 29 Working Party has analyzed the legal provisions and practices in the Member States to assess the compatibility of further processing and identified key factors to be considered in the compatibility assessment:

(i) The relationship between the purposes for which the personal data have been collected and the purposes of further processing;

(ii) The context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;

(iii) The nature of the personal data and the impact of the further processing on the data subjects;

(iv) The safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

No one time consent

When the purposes for which personal data was collected are modified or expanded subsequent to its collection, consent will be be deemed to be specific only if it is obtained afresh in respect of that modification or expansion, prior to any use of that data for the modified or expanded purposes.

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?

As stated above, we would recommended an incremental model, which would seek to build the data protection legislation around consent and purpose specification, and seek an active role by the data protection authority in exploring ways to incorporate use regulation in the sectoral codes of conduct and other subordinate processes. There is a need for the data protection authority to work closely with the sectoral regulators and the other stakeholders to frame codes which explore use regulation.

Consent not a tool of coercion

If data being collected is merely incidental and not essential to the service being provided, then agreeing to a privacy policy that mandates collection of such data should not be a condition precedent.

Chapter 6: Sensitive Personal Data

1. What are your views on sensitive personal data?

To categorise data as sensitive personal data it can be regarded from three overlapping perspectives of its content, purpose and impact. Thereby, when data is sensitive by content, used for purposes such as authorisation or compromise of which can have an adverse impact; it should be regarded as sensitive personal data.[57]

Data classification is broadly defined as the process of organizing data by relevant categories so that it may be used and protected more efficiently. The classification process not only makes data easier to locate and retrieve – data classification is of particular importance when it comes to risk management, compliance, and data security.

Data classification involves tagging data, which makes it easily searchable and trackable. It also eliminates multiple duplications of data, which can reduce storage and backup costs, as well as speed up the search process.

Data classification is carried out for a variety of purposes, one of the most common being a process that supports data security initiatives. But data may be classified for a number of reasons, including ease of access, to comply with regulatory requirements, and to meet various other business or personal objectives. In some cases, data classification is a regulatory requirement, as data must be searchable and retrievable within specified timeframes. For the purposes of data security, data classification is a useful tactic that facilitates proper security responses based on the type of data being retrieved, transmitted, or copied.

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?

Any information which reveals physical, physiological, mental, economic, cultural or social identity is characterised as sensitive personal data. These include the following categories of data should be classified as sensitive personal data:

- Racial, ethnic, religious or caste identity;
- Identifications numbers such as Aadhaar number, Passport Number, PAN etc.

57 *Reasonable Security Practices IT (Amendment) Act, 2008*, available at https://www.dsci.in/sites/default/files/Reasonable_Security_Practices_Under_IT_Amendment_Act2008.pdf.

- Biometric information including fingerprints, iris scans, facial records, DNA information;
- Political opinions;
- Religious or other similar beliefs;
- Membership of trade unions, political groups;
- Physical or mental health or condition, or related information;
- Financial information including bank account numbers, transaction history, credit related data etc.
- Any information pertaining to sexual life and gender identity; and
- Convictions, proceedings and criminal acts.

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

Sensitive personal data should be subject to much stricter regulation than ordinary personal data and must only be processed when one of the following conditions have been satisfied

- The data subject has given explicit consent;
- It is needed in order to protect the vital interests of the individual or another person. For example, an individual with a medical condition has an accident at work; it would be in the individual's vital interest to disclose this condition to medical staff treating the individual.

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?

Please refer to our response to Chapter on Consent

Chapter 7: Storage Limitation and Data Quality

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

Data accuracy is one of the most important principle in any data protection regime . Even though consent is the basis of collection and the individual is responsible for providing accurate and authentic data but there are many times discrepancies with regard to the accuracy of data arise on account of lack of diligence of the data controller .Inaccurate data held by data controllers can have impact on an individual. A mis-diagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis because it is relevant for the purpose of explaining treatment given to the patient, or to additional health problems .Hence it is necessary to tether the data controllers with data accuracy compliances It is necessary for the data controller to:

- take reasonable steps to ensure the accuracy of any personal data you obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

Where the accuracy of a record has been challenged by the individual it relates to, it is good practice to mark the record as being in dispute (as in the above example). You are not legally obliged to do this – so, if you are satisfied that a record is correct, you need not flag it as having been challenged. However, in the case of credit reference agency records, it is accepted industry practice that disputed information should be flagged. In any event, the advantage of flagging a disputed record is that (as long as the other conditions are satisfied) it avoids you breaching the fourth data protection principle if the information does turn out to be inaccurate.

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

The storage limitation principle is closely connected with the purpose limitation principle so the data storage should extend upto the period of data usage for the legitimate purpose, the data should be dispensed as soon as the purpose is frustrated. The data should be anonymised or pseudonymised with proper checks so as to prevent re-identification. Setting a time period for data retention is an effective means for sensitive personal data protection. The data protection authority should set data retention limits for financial institutions which possess sensitive personal financial information and also for organisations which engage in biometric data collection. Post the retention periods the data must be destroyed. Merely

deleting a digital record or file will be insufficient to destroy the information contained therein as the underlying digital data are typically preserved in the system, and can often be “undeleted.” Specific technical methods used to dispose of the data greatly impact the likelihood that any information might be recovered.

When data are no longer needed, the destruction of the data becomes a critical, and often required, component of an effective data governance program. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).

Overwriting works by replacing your data with random text, it repeats this task many times. Each overwrite is known as a pass. It is a popular and relatively low-cost option; however the more times that the information is overwritten the more secure the deletion but also the more time consuming. A very time consuming technique is “The Gutmann Method”, which is widely considered to be the most secure method by overwriting the data thirty five times with carefully selected data patterns. However the United States Department of Defence recommends that data should be overwritten only seven times. This has a decreased level of security but is much faster than the Gutmann Method and therefore more efficient. It should be mandatory for data controllers should have a data destruction policy which is accessible to data subjects. Data subjects should also have the option to request the data controllers to destroy their data if they feel skeptical .

Further, in cases where by law or regulation, any entities, public or private are required to retain information even after the purpose of collection has been fulfilled, or for a designated period of time unrelated to the fulfilment of the purpose, aggregate details of data retention, the time period of which it is being shared should be, the respective law, regulation or orders under which such retention is being done must be part of the transparency requirements of the data controllers.

3. 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?

It is prudent to select the method based on the underlying sensitivity of the data being destroyed, or the potential harm they could cause if they are recovered or inadvertently disclosed. For very low risk information, this may mean simply deleting electronic files or using a desk shredder for paper documents. However, these types of destruction methods can be undone by means to technology, making these methods inappropriate for more sensitive data. For more sensitive data, stronger methods of destruction amay need to be employed.

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

De-identification is a tool that organizations can use to remove personal information from data that they collect, use, archive, and share with other organizations. De-identification is not a single technique, but a collection of approaches, algorithms, and tools that can be applied to different kinds of data with differing levels of effectiveness.
In general, privacy protection improves as more aggressive de-identification techniques are employed, but less utility remains in the resulting dataset. De-identification is especially important for government agencies, businesses, and other organizations that seek to make data available to outsiders.

For example, significant medical research resulting in societal benefit is made possible by the sharing of de-identified patient information under the framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the primary US regulation providing for privacy of medical records. As long as any utility remains in the data derived from personal information, there also exists the possibility, however remote, that some information might be linked back to the original individuals on whom the data are based.

When de-identified data can be re-identified the privacy protection provided by de-identification is lost. The decision of how or if to de-identify data should thus be made in conjunction with decisions of how the de-identified data will be used, shared or released, since the risk of re-identification can be difficult to estimate.

Chapter 8: Individual Participation Rights - 1

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

Implementation of access and portability

The data controllers should offer different implementation of the right to access and portability including but not limited to a direct download option and direct transmission of the data to another controller upon the request of the data subject. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.

Recommended Rights

Implementation of access and portability

The data controllers should offer different implementation of the right to access and portability including but not limited to a direct download option and direct transmission of the data to another controller upon the request of the data subject. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.

Recommended Rights

Right to Access

The data subject shall have the right to obtain from the controller access to the personal data collected and/or being processed. Additionally, the data subject can seek the the purposes of the processing, the recipients or categories of third party recipient to whom the personal data have been or will be disclosed, the intended time period of which the data would be stored, details of sources where data was not obtained directly from the data subject. The data will be made available by the controller in a structured, machine-readable as well as human-readable format. This shall include both data directly collected from the data subject as well as data observed about the data subject.

Right to portability

The data subject shall the have the right to transmit those data obtained from the controller under the right to access to another controller without hindrance from the controller to which the data was originally provided.[58]*This right will extend to all data volunteered or observed data based on the data subject's use of the services, but not to inferences made by the data controller on the basis of the data collected.*

Right to correction

The data subject shall have the right to ensure from the data controller, the rectification of inaccurate or incomplete personal data, without any undue delay, especially in cases where

58 The right to data portability has been incorporated in the new GDPR and will be explored in greater detail in subsequent briefs.

the incompleteness or inaccuracy of the data has adverse impacts on the data subjects.

Right to restrict processing

In cases where the accuracy or completeness of the data is contested by the data subject, the data subject has the right to restrict the processing of the data in question.[59]

Right to access when data indirectly obtained

All persons shall have a right to seek details as laid down in the Notice principle from any data controller about personally identifiable information about them obtained not directly from the data subject from a third party source.

Rights to access data about previous breaches

All data subjects shall have the right to seek information about the any previous instances of security breaches resulting in the theft, loss, negligence, damage or destruction of data held by the data controller or its agents, and the steps taken by the data controller to address the immediate breach as well as steps to minimise the occurrence of such breaches in the future.[60]

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

The scope of right to rectification of data should extend not only to rectify inaccurate data. It has previously been submitted that inaccurate data can have indelible impact on an individual and hence there should be some strong measures to enforce the right to rectification, the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK is an effective tool in the hands of the data subjects especially in cases where the data controllers refuse to rectify data on vague grounds or when data controllers do not respond to access requests in the stipulated time.

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

GDPR allows most requests to be made free of charge. This is a significant change and will hit the budgets of those who receive voluminous or complex requests e.g. local authority social services departments. However, a "reasonable fee" can be charged for further copies of the same information and when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information. A nominal fee on the same lines as the Right to Information Act may be imposed where information is sought from public bodies.

59 This right adds to the principle of Opt-Out and seeks to strengthen it by formulating it as a separate right available at all times to data subjects.

60 Along with transparency and openness obligations, this right may also foster market competition for services providers to address security issues.

Where information is sought from private bodies, the basis of computation of the fee should be fair and reasonable and reflective of the actual additional costs borne by the data controller.

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

Under GDPR the requested information must be provided without delay and at the latest within one month of receipt. This can be extended by a further two months where the request is complex or where there are numerous requests. If this is the case, the Data Subject must be contacted within one month of the receipt of the request and explain why the extension is necessary. All refusals must be in writing setting out the reasons and the right of the Data Subject to complain to the ICO and to seek a judicial remedy. We recommend a similar model for India.

5. 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?

We would advise against the adoption of a right to explanation analogous to the GDPR, at least until it is clear how the right may be implemented. In case such a right is adopted, we would recommend that the data protection authority along with sectoral bodies arrive at guidelines on how the data controllers may provide information to data subjects, before such a right is enforced.

However, where automated decision making is used for discharging of public functions, **the data protection law must state that such actions are subject the the constitutional standards and are 'just, fair and reasonable' and satisfy the tests for both procedural and substantive due process**.

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

The exceptions have already been dealt with in the Chapter on Exemption. We submit that no additional exemptions are required.

Chapter 9: Individual Participation Rights

1. 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?

The right to restrict processing is a progressive right which provides the data subject effective control over his / her data such a right should be introduced in the proposed data protection legislation in India subject to certain conditions . Right to restrict processing can be exercised in the following situations :

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.

- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.

- When processing is unlawful and the individual opposes erasure and requests restriction instead.

Further, we also recommend the following rights:

Right to withdraw

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

The data subject shall have a right to seek all information reasonably necessary to decide whether to withdraw his or her consent, including not limited to purposes for which their data is being processed, the manner in which such processing is being conducted, the duration which the data collector intends to process and retain the data.

Right against unfair denial of service

All persons shall have the right against unfair denial of services on the grounds that such persons do not agree to share data, not essential but merely incidental to the provision of service, being made a precondition to the provision of services.[61]

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

We recommend a right to object similar to that in the UK, and allow data subjects to ppt out to automated processing in case of evaluative decisions on the basis of automated processing. However, in cases where there is an involvement of human decisionmaking

61 This principle responds to the existing issues with the Opt-out principle where opting out is often not

as well, or a meaningful review of the automated decision by a human actor, it will not be considered a case of automated decisions.

3. 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?

We recommend that the data protection law in India does not impose any additional prohibitions or limitation on automated data processing. However, where automated processing in used for discharging public functions, it must be subject to constitutional law requirements of 'justice, fairness and reasonableness' and procedural and substantive due process.

Chapter 10: Individual Participation Rights 3 - Right to be Forgotten

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

The 'right to be forgotten' has gained prominence since a matter was referred to the Court of Justice of European Union (CJEU) in 2014 by a Spanish court.[62] In this case, Mario Costeja González had disputed the Google search of his name continuing to show results leading to an auction notice of his reposed home. The fact that Google continued to make available in its search results, an event in his past, which had long been resolved, was claimed by González as a breach of his privacy. He filed a complaint with the Spanish Data Protection Agency (AEPD in its Spanish acronym), to have the online newspaper reports about him as well as related search results appearing on Google deleted or altered. While AEPD did not agree to his demand to have newspaper reports altered, it ordered Google Spain and Google, Inc. to remove the links in question from their search results. The case was brought in appeal before the Spanish High Court, which referred the matter to CJEU. In a judgement having far reaching implications, CJEU held that where the information is 'inaccurate, inadequate, irrelevant or excessive,' individuals have the right to ask search engines to remove links with personal information about them. The court also ruled that even if the physical servers of the search engine provider are located outside the jurisdiction of the relevant Member State of EU, these rules would apply if they have branch office or subsidiary in the Member State.[63]

The 'right to be forgotten' is a misnomer, and essentially when we speak of it in the context of the proposed laws in EU, we refer to the rights of individuals to seek erasure of certain data that concerns them. In 2016, the EU released the final version of the General Data Protection Regulation. The regulation provides for a right to erasure under Article 17, which would enable a data-subject to seek deletion of data.[64] Notably, except in the heading of

62 Google Spain et al v. Mario Costeja González, available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

63 http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf.

64 Article 17 (1) states: The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

the provision, Article 17 makes no reference to the word 'forgetting.' Rather the right made available in this regulation is in the form of making possible 'erasure' and 'abstention from further dissemination.' This is significant because what the proposed regulations provide for is not an overarching framework to enable or allow 'forgetting' but a limited right which may be used to delete certain data or search results. Providing a true right to be forgotten would pose issues of interpretation as to what 'forgetting' might mean in different contexts and the extent of measures that data controllers would have to employ to ensure it. The proposed regulation attempts to provide a specific remedy which can be exercised in the defined circumstances without having to engage with the question of 'forgetting'.

Significant technical challenges remain in the effective and consistent application of Article 17 of the EU Directive. One key issue is concerned with how 'personal data' is defined and understood, and how its interpretation will impact this right in different contexts. According to Article 17 of the EU directive, the term 'personal data' includes any information relating to an individual. Some ambiguity remains about whether information which may not uniquely identify a person, but as a part of small group, could be considered within the scope of personal data. This becomes relevant, for instance, where one seeks the erasure of information which, without referring to an individual, points fingers towards a family. At the same time, often the piece of information sought to be erased by a person may contain personal information about more than one individual. There is no clarity over whether a consensus of all the individuals concerned should be required, and if not, on what parameters should the wishes of one individual prevail over the others. Another important question, which is as yet unanswered, is whether the same standards for removal of content should apply to most individuals and those in public life.

The issue of what is personal data and can therefore be erased gets further complicated in cases of derived data about individuals used in statistics and other forms of aggregated content. While, it would be difficult to argue that the right to be forgotten needs to be extended to such forms of information, not erasing such derived content poses the risk of the primary information being inferred from it. In addition, Article 17(1)(a) provides for deletion in cases where the data is no longer necessary for the purposes for which they were collected or used. The standards for circumstances which satisfy this criteria are, as yet, unclear and may only be fully understood through a consistent application of this law.

Finally, once there are reasonable grounds to seek erasure of information, it is not clear how this erasure will be enforced practically. It may not be prudent to require that all copies of the impugned data are deleted such that they may not be recovered, to the extent technologically possible. A more reasonable solution might be to permit the data to continue to remain available in encrypted forms, much like certain records are sealed and subject to the strictest confidentiality obligations. In most cases, it may be sufficient to ensure that the records of the impugned data is removed from search results and database reports without actually tampering with information as it may exist. These are some of the challenges which the practical application of this right will face, and it is necessary to take them into account in enforcing the proposed regulations.

In India, this rights should be limited to a right to seek erasure of information shared by the individual themselves or generated through their participation in a process, and not be extended to information that exist about them generated from other sources. Extending it to other kinds of information may pose significant conflicts with free speech. We also recommend that the rights should be called a right to erasure and not the right to be forgotten, as it is a more accurate description.

We recommend that the right to erasure be applicable in the following cases:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based and, where there is no other legal ground for the processing;

c) the personal data have been unlawfully processed.

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

Yes, the right to erasure should be restricted to the personal data that has been collected from the individuals, or assessments made on the basis of data shared by the individual.

IV. Regulation and Enforcement

Chapter 1: Enforcement Models

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

We welcome the Committee's deliberations on the different models of enforcement. **However, we feel that the discussion is incomplete as it focuses almost entirely on the actors responsible for regulation**– command and control involving the regulator as the key actor responsible for regulation; the self-regulation models involving the industry bodies as regulating actors; and the co-regulatory model involving a mixture of both. While this discussion is extremely important, it is also important to delve into the approach that the chosen actors (regulator, industry or a mix of the two) will adopt in governance. We provide below an overview of dominant approaches.

Two strategies that for many years dominated the debate about enforcement strategy,the question of 'regulatory style' and whether it is more appropriate for regulators to 'punish or persuade'. Regulatory agencies have considerable administrative discretion with the enforcement task. In broad terms, they can choose between (or incorporate some mixture of) two very different enforcement styles or strategies: those of deterrence and 'advise and persuade' (sometimes referred to as a 'compliance' strategy).

Deterrence:

It is an adversarial style of enforcement essentially built around sanctions for rule-breaking behaviour. I**t build on a model of economic theory that those regulated are rational actors who would respond to incentives and disincentives**. This systems believes that if offenders are detected with sufficient frequency and punished with sufficient severity, then they, and other potential violators, will be deterred from violations in the future. The deterrence strategy is adversarial. The focus of regulator is on detecting violations, establishing guilt, and penalising violators for past wrongdoing.

Proponents of deterrence assume that regulated business corporations are 'amoral calculators'[65] that will take costly measures to meet public policy goals only when: (1) specifically required to do so by law and (2) they believe that legal non-compliance is likely to be detected and harshly penalised.[66] On this view, the certainty and severity of penalties must be such that it is not economically rational to defy the law.

---

65 R. Kagan and J. Scholz (1984), *'The "Criminology of the Corporation" and Regulatory Enforcement Strategies'* in K. Hawkins and J.M. Thomas (eds) (1984), *Enforcing Regulation* (Boston, Mass: Kluwer-Nijhoff)

66 Becker, Gary S. "*Crime and punishment: An economic approach*." *The economic dimensions of crime*. Palgrave Macmillan, London, 1968. 13-68.;Stigler, George J. "*The Theory of Economic Regulation*." *The Bell Journal of Economics and Management Science*, vol. 2, no. 1, 1971, pp. 3–21. *JSTOR*, JSTOR, www.jstor.org/stable/3003160.

A distinction is made between *general deterrence* (premised on the notion that punishment of one enterprise will discourage others from engaging in similar proscribed conduct) and *specific deterrence* (premised on the notion that an enterprise that has experienced previous legal sanctions will be more inclined to make efforts to avoid future penalties). Both forms of deterrence are assumed to make a substantial positive contribution to reducing the social harm proscribed by regulation.[67]

In terms of general deterrence, the evidence shows that the perceptions of legal risk (primarily, of prosecution) play a far more important role in shaping firm behaviour than the objective likelihood of legal sanctions.[68] And even when perceptions of legal risk are high, this is not necessarily an important motivator of behaviour. For example, Braithwaite and Makkai (1991: 35) found that in the case of nursing home regulation, there was virtually no correlation between facilities' regulatory compliance rates and their perceptions of the certainty.

Yet other well constructed studies have found that 'deterrence, for all its faults, may impact more extensively on risk management and compliance activity' than applying remedial strategies after the event.[69]

Haines, in another important study,[70] suggests that deterrence, while important in influencing the behaviour of small and medium sized enterprises, may have a much smaller impact on large ones. The simpler management structures of small firms and the relative incapacity of key decision-makers within them to avoid personal liability, also make them much easier targets for prosecution.

Turning to specific deterrence, the evidence of a link between past penalty and improved future performance is stronger, and suggests that a legal penalty against a company in the past influences their future level of compliance.[71] For many companies the imposition of a first sanction produces a sea change in attitudes.' However, the literature also suggests that action falling short of prosecution (for example,inspection, followed by the issue of administrative notices or administrative penalties) can also achieve 'a re-shuffling of managerial priorities' even when those penalties are insufficient as to justify action in pure cost–benefit terms.[72]

---

67 Simpson, Sally S. *Corporate crime, law, and social control*. Cambridge University Press, 2002.

68 *Id*, Chapter 2

69 Baldwin, Robert. "*The new punitive regulation*." *The Modern Law Review* 67.3 (2004): 351-383, Page 373

70 F. Haines (1997), *Corporate Regulation: Beyond 'Punish or Persuade'* (Oxford: OUP)

71 *Supra* note 5, Page 373

72 W. Gray and T. Scholz (1991), '*Analysing the Equity and Efficiency of OSHA Enforcement*' 13 Law and Pol 185

Against the positive contribution that deterrence can make in some circumstances, must be weighed the counter-productive consequences of its over-use or indiscriminate use. For: 'if the government punishes companies in circumstances where managers believe that there has been good faith compliance, corporate officers may react by being less cooperative with regulatory agencies' (Shapiro and Rabinowitz, 1997: 718). Indeed, there is evidence that managers may refuse to do anything more than minimally comply with existing regulations (rather than seeking to go beyond compliance) and frequently resist agency enforcement efforts.

The broader message may be that the impact of deterrence is significant but uneven and that unless it is used very wisely and well, it may have negative consequences as significant as positive ones.

Compliance:

Compliance strategy emphasises cooperation rather than confrontation and conciliation rather than coercion.[73] It seeks to prevent harm rather than punish an evil. Its conception of enforcement centres upon the attainment of the broad aims of legislation, rather than sanctioning its breach. Recourse to the legal process here is rare, a matter of last resort, since compliance strategy is concerned with corrective action and not retribution.

Bargaining and negotiation characterise a compliance strategy. The threat of enforcement remains, so far as possible, in the background. It is there to be employed mainly as a tactic, as a bluff, only to be actually invoked where all else fails; in extreme cases where the regulated entity remains uncooperative and intransigent.

There is considerable evidence that cooperative approaches may actually discourage improved regulatory performance amongst better actors if agencies permit lawbreakers to go unpunished. This is because even those who are predisposed to be 'good apples' may feel at a competitive disadvantage if they invest money in compliance at a time when others are seen to be 'getting away with it.[74]

Again, the broader point is that a compliance strategy will have a different impact on differently motivated organisations. It may be entirely appropriate for corporate leaders but it will manifestly not be effective in engaging with reluctant compliers.

Responsive Regulation Theory

Given the limitations of both compliance and deterrence as stand alone strategies, most contemporary regulatory specialists now argue, on the basis of considerable evidence from

73 Hutter, Bridget M. "*Regulation: standard setting and enforcement*." (1993): 233-248.

74 Shapiro, S & Rabinowitz, R (1997), "*Punishment versus cooperation in regulatory enforcement: a case study of OSHA*", Administrative Law Review, vol 14

both Europe and the USA, that a judicious mix of compliance and deterrence is likely to be the optimal regulatory strategy.[75]

Regulated enterprises have a variety of motivations and capabilities, therefore, it is suggested that regulators must invoke enforcement strategies which successfully deter egregious offenders, while at the sametime encouraging virtuous employers to comply voluntarily and rewarding those who are going 'beyond compliance'. Thus, good regulation means invoking different responsive enforcement strategies depending upon whether one is dealing with leaders, reluctant compliers, the recalcitrant, or the incompetent. This issue is of particular relevance

The challenge is to develop enforcement strategies that punish the worst offenders, while at the same time encouraging and helping employers to comply voluntarily. The most widely applied mechanism for resolving this challenge is that proposed by Ayres and Braithwaite, namely for regulators to apply an 'enforcement pyramid' which employs advisory and persuasive measures at the bottom, mild administrative sanctions in the middle, and punitive sanctions at the top.

Central to this model are the need for the following: (i) gradual escalation up the face of the pyramid and (ii) the existence of a credible peak or tip which, if activated, will be sufficiently powerful to deter even the most egregious offender.

However, de-escalating and escalating of penalties is an extremely complex proposition. Regulators who escalate sanctions may produce unintended consequences in companies, 'which in response to threat, aim to reduce their vulnerability to scrutiny, and so, to liability. When escalation of penalty occurs, motivation for corporate compliance shifts from co-operation and trust, to confrontation and mistrust.[76]

For a country like India with an abysmal state of data protection, such a graded approach is necessary. Introduction of a robust law, which is fully necessary, will however, lead to extreme non-compliance in the beginning. We have earlier suggested an orchestrated sunrise of data protection regulation in order to accommodate the interest of data controllers allowing them sufficient time to create internal policies and capacity for compliance.

Further, risk based regulation and the enforcement pyramid are not necessarily antithetical since a pyramidal response might be applied to enterprises that had first been targeted on the basis of a risk assessment. This is of relevance to a complex subject like data protection,

75 I. Ayres and J. Braithwaite (1992), *Responsive Regulation* (Oxford: OUP) ; Kagan, R (1994), "*Regulatory Enforcement*", in Rosenbloom, D & Schwartz, R (eds), Handbook of Regulation and Administrative, Dekker, New York. ; Wright M, Marsden S and Antonelli A (2004), *Building an evidence base for the Health and Safety Commission Strategy to 2010 and Beyond: A Literature Review of Interventions to Improve Health and Safety Compliance*, HSE Books, Norwich

76 *Supra* note 6

where certain kinds of behavior, such as misuse of sensitive personal data, can have significant ramifications for data subjects. Already, there is significant discussion about use of risk based assessments in privacy impact assessments. The data regulator ought to take this into account while determining the appropriate form of intervention. This points are elaborated upon in greater detail in the chapter on Accountability and Enforcement Tools.

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

In a country like India with limited state capacity, a co-regulatory model is attractive. Such a model also allows greater participation from other actors, which would lead to greater compliance in case of a more bottom up process. However, the international experience with regard to co-regulation has been a mixed one. The White Paper does refer with approval to the articles detailing examples of collaborative governance in the Netherlands and the attempts made in the US. The experience closer home in the APEC countries has been less favorable. Such approaches have been experimented with and discarded in Australia.

In case a co-regulatory approach is adopted, it must be a carefully- calibrated one. The global experience with self-regulation in particular suggests that it is ineffective. Industry driven self regulatory practices on privacy in the United States have arisen in response to the incentives and interventions from regulators such as Federal Trade Commission (FTC), and legislative actions. These efforts have been perceived, in retrospect, as a means to circumvent any real regulation from FTC or Congress, by demonstrating a desire and ability of self-govern. In this section we briefly look at a few self regulation initiatives and how they fared.

In 1997, the Individual Reference Services Group," or "IRSG Group was announced at a public workshop organised by the FTC. The IRSG Group developed and agreed to a set of principles that regulates the availability of information obtained from non-public sources through individual reference services by implementing the voluntary restrictions. The FTC Report notes that the "principles show particular promise because they include a compliance assurance mechanism and are likely to influence virtually the entire individual reference services industry" and "should substantially lessen the risk that information held by these services will be misused, and they should address consumers' concerns about the privacy of non-public information about them in the services' databases."[77] The regulatory tools included an annual assurance review of compliance with principles, and summaries of reports to be made publicly available. While the IRSG portal does indicate that some members did conduct reviews, the reports were not made public. In 2001, the IRSG was terminated purportedly in response to the Gramm-Leach-Bliley Act. Curiously, the IRSG companies were in fact not even regulated by the operative parts of the Gramm-Leach-Bliley Act. Gellman and Dixon opine that "IRSG members lost interest in supporting an expensive

77 *Individual Reference Services- A Report to Congress*, available at https://www.ftc.gov/reports/individual-reference-services-report-congress

self-regulatory organisation because they no longer felt threatened by legislation or regulatory activities."[78]

This example is representative of dozens of self-regulatory privacy governing initiatives undertaken by the industry in the United States, and the lax regulatory view of such initiatives by the FTC,[79] which involved the introduction of self-regulation as a political response to threats of privacy regulations from the Executive or the Legislature, and fizzling out with diminished threat of regulation or transitioning into other projects as dictated by the political expediency. Notable examples of such initiatives include the Privacy Leadership Initiative,[80] the Online Privacy Alliance,[81] the Network Advertising Initiative[82] and the BBBOnline Privacy Programme.[83]

Therefore, **its is necessary to have proper oversight and accountability of the self regulating organisations**. The codes of conduct drawn up with the approval of the data protection authority must be for the purpose of specifying regulation to further the objects of the legislation. Associations and other bodies which intend to prepare a code of conduct or to amend or extend an existing code should submit the draft code, amendment or extension to the the data protection authority or other supervisory authority created by it which is competent. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards. In no circumstance should the code be in contravention of any provisions of the legislation and must be in furtherance of the statement of objects in the legislation.

Further, the data protection authority must establish clear procedures for the monitoring and evaluation of the codes of conduct. It should be done by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the data protection authority. For the monitoring bodies to be efficient, the law must prescribe conditions such as:

- demonstrating its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

- establishing procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

78

79 While FTC reports acknowledges the limitations of the self regulatory measures such as the IRSG initiatives, it has taken no steps, nor made concrete recommendations to alleviate these issues. See *Supra* note 14

80

81

82

83

- establishing procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

- demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

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?

Please refer to 1 and 2.

Chapter 2: Accountability

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

We second the reference made in the White Paper to the description of Accountability as first, the need of a data controller should take appropriate measures to implement data protection principles and second, a data controller must be in a position to demonstrate, when asked by a supervisory authority, that such measures have been adopted.

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?

On the lines of the GDPR, the data controllers should be subject to the following obligations:

- Obligation to assess the risks and implement security measures to mitigate those risks.

- These risks are of varying likelihood and severity for the rights of individuals, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

- Obligation to train staff having access to personal data on the steps to follow in case of a data breach (adopt an incident response plan).

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

The obligations listed above must be linked to liabilities for the data controllers. It is suggested that a staggered approach is adopted the same obligations are not implemented for all data controllers. Data controllers who process data of larger number of individuals, or process sensitive personal data must be subject to more onerous obligations. The data protection law could identify categories of material and non-material harm. If such harm is occasioned, it could trigger liability only on proof of failure to to take appropriate measures. In cases where the nature of processing is inherently risky, the data controllers could become strictly liable, subject to the exceptions that the harm was caused by an act of God or the data subject herself contributed to the harm. This option should be exercised only in circumstances where the proposed use could lead to significant harms.

4. 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?

Strict liability should be used only in circumstances where there is evidence of harms that can be caused as result of the proposed data processing, and it is clearly recognised by the data protection authority, for instance, any breach caused to the security of biometric databases despite the presence of security protocols.

5. 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?

In our opinion, the primary data protection legislation should be so prescriptive so as to specify that need for insurance by a group of data controllers. We recommend that this issues should not be dealt with in the legislation but be decided in sectoral codes based on inputs from the industry, sectoral regulators, civil society and academia.

Chapter 3: Enforcement Tools

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

The codes of conduct drawn up with the approval of the data protection authority must be for the purpose of specifying regulation to further the objects of the legislation. Associations and other bodies which intend to prepare a code of conduct or to amend or extend an existing code should submit the draft code, amendment or extension to the the data protection authority or other supervisory authority created by it which is competent. As mentioned in the GDPR, some of the subject matters that the codes can address are:

- fair and transparent processing;
- the legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the exercise of the rights of data subjects;
- technical and organizational measures, measures introducing data protection by design and by default, and safeguards for the security of processing;
- the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; or
- the transfer of personal data to third countries or international organisations.

2. 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?

The most suitable bodies to prepare such codes are industry bodies, particularly sectoral industry bodies. There are sectors where such bodies may not be fully evolved in India, therefore, a group of companies which intend to come together and frame the code may also lead the process of preparing such codes of conduct. While the intent of such a regulatory model is that they must evolve through a bottom-up process, thus, ensuring that codes are framed by active participation of those who would be governed by it, In cases, where the industry bodies are reluctant or slow to take initiative, the data protection authority may encourage and incentivise the creation of such codes. In some cases, drawing from the example in UK, the data protection authority may itself also prepare and disseminate codes of practice –for guidance as to good practice after carrying out consultations. In some cases, the data protection authority may set up a task force with representation from different stakeholders to do preliminary research or provide recommendations for the codes.

For such steps to be fully inclusive and thereby efficient, it is important that they process of drafting the codes is a multi-stakeholders one involving not just the industry and the regulator, but also civil society and academia.

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

As stated earlier, Associations and other bodies which intend to prepare a code of conduct or to amend or extend an existing code should submit the draft code, amendment or extension to the the data protection authority or other supervisory authority created by it which is competent. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards. In no circumstance should the code be in contravention of any provisions of the legislation and must be in furtherance of the statement of objects in the legislation.

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

The data protection authority must establish clear procedures for the monitoring and evaluation of the codes of conduct. It should be done by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the data protection authority. For the monitoring bodies to be efficient, the law must prescribe conditions such as:

- demonstrating its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

- establishing procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

- establishing procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

- demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

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

The codes should also engage in detail with the consequences for the violations. The consequences will depend on the nature of the violation, enforcement tools are dealt with later in the chapter on data protection authorities.

Chapter 4: Personal Data Breach Notifications

1. How should a personal data breach be defined?

As stated in the White Paper, the definition of personal data breach must take into account both the cause and effect of of security incident and its impact on personal data. We second the Committee's view of the three broad kinds of personal data breaches:

- Confidentiality breach: Where there is an unauthorised or accidental disclosure of, or access to personal data.

- Integrity breach: Where there is an unauthorised or accidental alteration of personal data.

- Availability breach: Where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

The definition used in the GDPR is most comprehensive, and must be adopted for personal data breach: "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."

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

The RBI guidelines in India state that all Non Banking Financial Companies shall immediately notify RBI in the event of any breach of security and leakage of confidential customer related information.[84] Thus, we see a clear recognition of the need to inform the regulator immediately after a security incident.

We recommend that all personal data breaches should be reported immediately to the data protection authority and sectoral regulator, if any.

In case of individual notification, we strongly recommended against the matrix approach to deal differentially with data controllers based on size of the actor in the primary legislation. This will significantly complicate the law, and pose numerous issues of interpretation. Alternately, we suggest a graded approach with respect to nature of breach, in line with the HIPAA code in the US.

84 *Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs*, available at https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT87_091117658624E4F2D041A699F73068D55BF6C5.PDF

- Notification to the regulator (DPA and sectoral regulator) immediately upon detection of the breach. The DPA and sectoral regulator must create an easy and secure electronic mechanism to receive these notifications;

- Notification to the press within three business days of the detection of the breach where personal data of more than 500 persons is compromised in the breach;

- Notifications to individual affected by the personal data breach at the earliest but not later than 30 days of the detection of the breach;

- Requirement to publish details all security incidents, including the personal data breaches on a quarterly basis, under transparency obligations.

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

All personal data breaches must be informed to the individuals affected, or suspected to be affected at the earliest and not later than 30 days from the detection of the breach.

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

We second the views of the Committee that the personal data breach notification should mention; the type of personal data breach, the estimated date of the breach, general description of the security incident in language that is comprehensible for an individual with average technical and legal knowledge. The notification must also inform the individual of his or her rights with respect to the breach and the contact information of the person or office in

charge of addressing related grievances. The notification could be done by way of postal mail or electronic mail, as long as the notification is communicated to the affected individual in the stipulated time. A standard format for notification could be drafted by the data protection authority or the sectoral bodies for administrative ease.

Chapter 5: Categorisation of Data Controllers

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

The White Paper notes the Australian Privacy Act where small businesses (with an annual turnover AUD 3 million or less) are exempt from obligations under the Privacy Act, though they may, nonetheless, have such duties in certain circumstances such as when the business discloses personal information about another individual for a benefit, service or advantage. However, this effectively excludes about 95% of Australian data controllers from the purview of the legislation. We strongly argue against such a system. Any differentiated system, if created must apply only to specific onerous obligations on the data controllers.

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

Instead of creating a general classification of data controllers, the focus should be on creating differentiating factors for specific obligations. We will address classifications for specific obligation in subsequent sections.

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

Please refer to 2.

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

Please refer to 2.

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

Please refer to 2.

Chapter 6: 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?

The technology industry comprises actors from across the spectrum – there are the larger multinationals with resources at their disposal, but there are also the smaller startups. A system of registration for data controllers would suffocate and stunt this mushrooming sector due to the unnecessary addition of bureaucracy and regulatory processes. We strongly recommend against instituting any specific registration obligations under the general data protection law. Such obligations may be introduced in sectoral codes and rules where deemed necessary by the sectoral regulators. In regulated industries such as the medical, telecommunications and banking industry, there are already a set of registrations / compliances for a data controller to meet.

Chapter 7: Data Protection Impact Assessment

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

There is clear need for greater accountability in the practices of the data controllers. The resistance of legal mandates for accountability measures such as data protection impact assessments is antithetical to the view of big data exceptionalism that the focus should from collection regulation to use regulation. Unless there are clear steps taken to institute use regulation through identification of use cases that are harmful, it is difficult to evaluate the efficacy of such steps. The data protection impact assessments are an excellent measure in this regard.

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

Periodic DPIAs should be made mandatory through sectoral codes. We list some illustrative thresholds that could be used:

- For large companies with an annual turnover above INR 1 crore or annual profits over INR 50 lakhs.
- For data controllers processing the personally identifiable data of more than 500 people.
- For use of a new untested technology for data processing which may pose risks to identifiability or security
- For examples of data processing which may show a prima facie likelihood of harm to the data subjects.

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

The Data Protection Impact Assessment should be carried out by the data controller, or an external professional qualified to do so. The data protection authority must provide guidelines on standards and methodologies for conducting the assessments.

The data protection authority should not be obligated to conduct the DPIAs as it will put considerable burden on them. In the course of audits, inspection and investigations, the data protection authority may choose to examine the DPIA conducted.

<once in two years>

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

The key findings of a DPIA must be made public periodically along with the other transparency requirements of data controller.

Chapter 8: Data Protection Audits

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

Data protection audits are both an important tool for data protection authority, as well as a key compliance requirement for data controllers. We recommend following the model in the GDPR which allows for data protection audits within controller-processor contracts, as a responsibility of a data protection officer, as well as part of the investigative powers of a supervisory authority.

Chapter 9: Data Protection Officers

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

Under the Information technology Act, a body corporate is required to designate a grievance officer for grievance redressal purposes with certain details of the same posted on the body corporate‘s website. This role ought to be expanded in the data protection law to play an advisory role in relation to the data controller but must also be its external face in relation to complaints, requests and the requirements of a data protection authority.

Chapter 10: Data Protection Authority

1. What are your views on the above?

Please refer to 2, 3 and 4.

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

An independent supervisory body for the purposes of data protection is an essential criteria for any country regulating data.

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

No, we strongly recommend that a separate independent body with a focussed mandate on data protection is created.

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

The Data Protection Authority must consist of the Privacy Commission, and a Secretariat.

The Privacy Commission would consist of the Chief Privacy Commissioner and not more than six other Privacy Commissioners, to be appointed by the President. The Chief Privacy Commissioner shall be a person who has been a Judge of the Supreme Court of India. One Privacy Commissioner shall be a person who is or has been a Judge of a High Court. One Privacy Commissioner shall be a person of ability, integrity and standing who has a special knowledge of, and professional experience of not less than ten years in privacy law and policy.

The other Privacy Commissioners shall be persons with technical expertise and knowledge in the fields of data collection and storage practices, or data protection and ethics, or big data analytics and technologies or information technology.

The office of the Privacy Commission shall be autonomous, independent, and free from external interference. The Office shall be provided with sufficient operational resources including human, technical, and financial for the effective discharge of its duties and exercise of its powers. Such powers shall be subject to audit by the Comptroller and Auditor General of India.

In order to prevent bureaucratic hurdles, the Privacy Commissioners must be permitted to function unilaterally and not require the vote of the entire Commission unless specifically prohibited in the legislation. It is also recommended that the Privacy Commissioners must be given charge of specific sectors, based on their area of expertise, and the Commision should be able hire officers and consultants to assist with the regulation of specific sectors.

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?

The Central Government shall appoint a Secretary to the Privacy Commission to exercise and perform, under the control of the Chief Privacy Commissioner such powers and duties as may be prescribed or as may be specified by the Chief Privacy Commissioner. The Secretary shall head the Secretariat and it shall comprise other officers and employees as may be necessary for the efficient performance of the functions of the Data Protection Authority.

The salaries and allowances payable to the Chief Privacy Commissioner and Privacy Commissioners and the administrative expenses, including salaries, allowances and pension, payable to or in respect of the officers and other employees of the of the Privacy Commission shall be defrayed out of the Consolidated Fund of India.

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

The Central Government shall issue a public advertisement inviting applications to fill all vacancies in the Privacy Commission. The selection committee for the appointment of the members of the Privacy Commission shall comprise the Chief Justice of India, the Law Minister, the Leader of the Opposition from Lok Sabha or of the single largest Opposition party being one with the greatest numerical strength in the Lok Sabha, one eminent person representing the private sector and one eminent person representing the civil society. All proceedings of the selection committee will constitute a public record.

Before appointing any person as the Chief Privacy Commissioner or Privacy Commissioner, the President shall satisfy himself or herself that the person does not, and will not, have any such financial or other interest as is likely to affect prejudicially their functions as such Privacy.

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?

The state level Privacy Commissions should be set up under the data protection law. The jurisdiction of the state level data protection authorities would be co-extensive with the jurisdiction of the state high courts.

It must be remembered that the regulated entities in the case of data protection law, often do not function within specified geographical boundaries. Therefore, a division of on the basis of state may not be the most efficient way of organise the authority. It may be more beneficial to set up sectoral organs of the data protection authority.

However, it would be beneficial to have a state level entity which could assist in performing the supporting as well sanctioning functions of the data protection authority at the state level, and work with state governments and regional bodies.

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

Please refer to 4 and 6.

Further, Independence', from international sources, most commonly involves the following ten attributes:[85]

- Establishment by legislation rather than any executive order or delegated legislation;
- Ability to investigate and report free of direction or permission from any other political or governmental authority;
- A fixed term of office, so as to avoid a Commissioner being at the whim of executive dismissal (including remuneration also independent of the executive);
- Removal from office only for defined reasons (inability, neglect of duty or serious misconduct), and with procedural safeguards;
- Powers and duties to report directly on issues to either the Parliament and/or the public;
- Resources of the DPA determined independently of the Executive;
- Positive qualification requirements for Commissioners;

85 Greenleaf, Graham, *Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience* (December 13, 2011). Computer Law & Security Review, Vol. 28, Issues 1 & 2, 2012; U. of Edinburgh School of Law Working Paper No. 2011/42. Available at SSRN: https://ssrn.com/abstract=1971627 or http://dx.doi.org/10.2139/ssrn.1971627.

- Prohibition of Commissioners undertaking other concurrent positions;

- Prohibition of appointment of Commissioner from specified backgrounds which could cause conflicts of interests, or requirement of the disclosure of interests.

9. Can the data protection authority retain a proportion of the income from penalties/fines?

The incomes from fines and penalties imposed by the Data Protection Authority must flow into the Consolidated Fund of India. Retaining incomes from fines and penalties would create a conflict of interest and must be avoided.

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

The Privacy Commission may, through decisions arrived at by a simple majority of its members present and voting authorise, review, investigate, make an inquiry, and/or monitor, suo moto or on a petition presented to it by any person or by someone acting on his behalf, the implementation and application of the data protection law and give such directions or pass such orders as are necessary for reasons to be recorded in writing.

The Privacy Commission shall perform all or any of the following functions, namely –

a) review the safeguards provided under the data protection law and under other laws for the time being in force for the protection of personal data and recommend measures for their effective implementation or amendment, as may be necessary from time to time;

(b) authorise, review, investigate, make an inquiry, and/or monitor any measures taken by any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity for the protection of privacy and take such further action is it deems fit;

(c) authorise, review, investigate, make an inquiry, and/or monitor any action, code, certification, policy or procedure of any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to ensure compliance;

(d) Investigate and direct data controllers and processors to do or cease to do any act in order to address activity which is in contravention of the provisions of the data protection law

(e) formulate through public consultation with experts, other stakeholders, and the general public, norms for the effective protection of privacy by competent organisations, police forces, armed forces, intelligence organisations, public authorities, companies, persons or other entities;

(f) promote awareness and knowledge of personal data protection through any means necessary and to all stakeholders including providing information to any data subject regarding their rights under this Act as requested ;

(g) undertake and promote research in the field of protection of personal data and privacy;

(h) encourage the efforts of non-governmental organisations and institutions working in the field of personal data protection and privacy;

(i) publish periodic reports concerning the incidence of compliance including violations of this Act and data breaches as reported, collection, processing, storage, disclosure and other handling of personal data, interception of communications and surveillance;

(j) hear and decide applications for interception and surveillance;

(k) exercise its powers to ensure the speedy and efficient redressal of all complaints whose cause of action arises from the data protection legislation;

As stated above, Responsive regulation describes the complexity of relationships between achievement of objectives and the provision and use of appropriate enforcement mechanisms. At its centre are both a hierarchy of sanctions and a hierarchy of regulatory strategies (proactive sanctions and reactive sanctions). It comprises of multiple levels of sanctions with escalating seriousness, which lead to effective regulation. These are in a pyramid from so that the sanctions at the top get utilised the least. However, all sanctions should be used to retain credibility. It requires visibility of sanctions to consumers and those regulated. The higher levels serve, as a deterrent and most non-compliance are restricted to the lower levels.

We suggest the use of an additional support pyramid that aims to provide education and incentives for compliance, to the point of prioritising it, as it's the cheapest way to achieve large-scale compliance. This entire procedure requires high levels of transparency and visibility. All these pyramids (there are possibilities of overlap in the three pyramids) combined should provide a sufficient range of practices that makes responsive regulation possible.

Based on Graham Greenleaf's research into Asian Data Privacy Laws and mode of reactive and proactive measures, we have listed the following measures for India. For reactive and proactive sanctions constitution of a Data Protection Authority (DPA) or similar authority that has adequate powers of enforcement and regulation (as listed in the table below) is found to be most effective. The table below lists proactive and reactive measures taken by countries in Asia to ensure data protection. The hierarchy of the elements in this list as well as the support list is highly contextual and each jurisdiction needs to independently determine what serves as a higher sanction (or requires higher cost for support).

Proactive Measures	Description	Reactive Measures	Description
Audits and inspections	These include periodic inspections, publication of results and informal compliance checks	Administrative penalties	The issuance of fines for non-compliance. The range of fines will differ based graveness of the breach
Appointment of data protection officer	There should be defined qualifications for appointees and a defined independence of action	Compensation	DPA empowered to order payment of compensation
Registration systems	Data controllers with higher risk could be mandated to register, with potential cancellation serving as punitive threat. This should be formalised under the sectoral codes.	Mediation	DPA mediate to find mutually acceptable solutions to complaints
Design/default requirements	Data protection in information systems through mandated and predefined requirements	Name and shame publication	Parties in breach are named in public reports and press releases
Accountability requirements of data processor	Compliance with a code of conduct which has legal effect	Appeal	Appeal from decisions of DPAs on various grounds
Openness of data processing procedure	Follows from OECD openness principles and serves as a deterrent against non-compliance. Information of processing activities can be given to any person enquiring about it	Compensation for data subjects	Right to seek compensation through court.
Monitoring	Issue of notices like enforcement, information, assessment notice to check compliance		
Advisory power	DPA can advise the state and other institutions on the possible legislative and administrative measures to protect data subjects		
	Examining proposed legislations that may have any impact on data and privacy		

The types of support mechanism adopted by various countries in Asia to ensure compliance:[86]

Support Mechanisms	Descriptions
Training courses (Awareness generation)	Assisting data controller and data subject to understand their obligations and rights.
Freely accessible training	Educating both adults and children through educational materials, and other media outlets about privacy.
Voluntary audits and PIAs	Performing Privacy impact assessment to help determine if the entity is processing data in a lawful manner
Guidelines	Investing to develop non-compulsory guidelines and to apply them in industry sectors
Standards setting	Issuing code of conduct (can be prepared by DPA, trade associations, etc.), certification mechanisms and compliance seals and marks
Compliance advisory services	Advise controllers to ensure that no influential actions that risk protection are taken, incentivising compliance through awards and prizes
Research	Monitoring developments in information processing and technology to minimise any adverse impact on protection of personal data

Receiving and investigating complaints

Complaints are a double-edged sword. On the one hand, a rising number of complaints shows that people are increasingly aware of their privacy. On the other hand, that rising number consumes more time from the data protection authorities. It would be regrettable if data protection authorities were obliged to deal with all complaints and requests for assistance without the possibility to exercise a reasonable discretion as to whether and how to deal with the matter. This may be a common approach for courts, and understandable from the point of view of general administrative law, but for data protection authorities with wide responsibilities and limited resources, it only means that individual cases will dominate the agenda at the expense of other matters.

The appropriate remedy for these problems should thus be twofold: first, encourage alternative courses of action for enforcement of data protection rights and, second, make sure that data protection authorities are able to set priorities and develop more flexible methods of dealing with individual complaints, including simple procedures and using them in support of ex officio inquiries against responsible parties.

86 Graham Greenleaf, See *Id*

Guidance and codes of practice

Data Protection Authority should offer guidance and codes of practice on, especially, sensitive or difficult issues. For example, the UK Information Commissioner's Office (ICO) has issued a data sharing code of practice providing practical advice to organisations that share personal data. Some subjects on which the DPA must provide guidance are practice for surveillance (or CCTV) cameras, on subject access for organisations dealing with requests from individuals for personal information, on privacy impact assessment, on assessment notices, employment practices, big data and international data transfers.

Notices and Warnings

A regulator may require an organisation to provide it with whatever information it needs to carry out its functions. This is sometimes described as an **"information notice"**. It differs from an "enforcement notice", whereby the regulator may require a data controller or data processor to take whatever steps it considers appropriate to comply with data protection legislation. Such steps could include correcting data, blocking data from use for certain purposes, or erasing data altogether.

In Ireland, the Office of the Data Protection Commissioner (ODPC) may prohibit the transfer of personal data from the state to a place outside the European Economic Area. The ODPC can exercise this power by providing a written notice, called a **"prohibition notice"**, to the data controller or data processor. In considering whether to exercise this power, the ODPC considers the need to facilitate international transfers of information. A prohibition notice may be absolute, or may prohibit the transfer of personal data until the person concerned takes certain steps to protect the interests of the individuals affected.

An **enforcement notice** has the potential to have a far greater influence on a controller than even the heftiest fine: an order to cease processing personal data altogether. Whether the order only relates to certain types of data, or is confined to a limited period (for example, until the controller improves its compliance more generally), it has the potential to shut down a business for the duration of the notice. Consequently, this power is often regarded as the strongest weapon that a DPA has in its arsenal. Failure to comply with an enforcement notice is punishable by a fine, and constitutes a criminal offence. This means that any subsequent fine is potentially unlimited, but would have to be the subject of formal proceedings before a criminal court (entailing, amongst other things, that the offence be proved beyond reasonable doubt).

Naming and Shaming

When a DPA makes public the names of organisations that have seriously contravened data protection legislation, this is a practice known as "naming and shaming". The UK ICO and other DPAs recognise the power of publicity, as evidenced by their willingness to co-operate with the media. The ICO does not simply post monetary penalty notices (MPNs or fines) on its website for journalists to find, but frequently issues press releases, briefs journalists and uses social media. The ICO's public policy statement on communicating enforcement

activities states that “the ICO aims to get media coverage for enforcement activities”.

Mandatory DPIAs

While some DPAs encourage organisations in their jurisdictions to undertake pri- vacy impact assessments (PIAs), few have made PIAs mandatory. They are manda- tory for government departments and agencies in the UK, the US and Canada. PIAs (or data protection impact assessments) will be mandatory in the European Union when the new Data Protection Regulation comes into force where the processing of personal data poses “high risks” to data subjects. PIAs could be a formidable arrow in the regulatory quiver depending on how the European Commission implements the DPIA provision in practice

Inspections, investigations and audits

Most DPAs are able to conduct inspections, investigations and audits, in some cases only in response to a complaint, in other cases, on the DPA’s own initiative. For example, the Australian DPA has the power to conduct investigations on its own initiative (not just in response to a complaint).

Monetary penalties (fines)

The strong sanction powers in the form fines in the European General Data Protection Regulation (GDPR) suggests a growing faith in the efficacy of fines as deterrents in the governance of privacy in Europe. Sanctions, have so far not been a big part of the data protection frameworks across the world with a few notable exceptions. The UK Information Commissioner’s Office (ICO) is among the data regulators which relies heavily on monetary penal sanctions.

The statutory basis for fines in the European Union so far has been Article 24 of the Data Protection Directive (95/46/EC). It states that that Member States shall “lay down the sanctions to be imposed in cases of infringement”. The fines regime in the UK is laid down in 55A to 55E of the UK Data Protection Act, 1998. Under this scheme, the ICO can impose Monetary Penalty Notices (MPN) which may range up to GBP 500,000 for serious offences.[87] Due to some confusion about whether the fines amounted to civil or criminal sanctions, but it was decided by the tribunal that the rules intended a civil standard of proof. Aside from MPNs, there are also other fines which can be imposed, for unlawfully obtaining or disclosing information, failure to register as a data controller etc. However, these fines are for acts designated as criminal offences, and therefore require a public prosecution and higher burden of proof. These offences can potentially result in an unlimited fine. [88]

87 Regulation 2, The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010

88 *Unlimited fines for serious offences*, available at https://www.gov.uk/government/news/unlimited-fines-for-serious-offences, last accessed on 30-01-2018

Fines have traditionally played a deterrent role, especially for repeat offences. The ICO has adopted a strategy of wide media coverage of its actions, so that the fines act a deterrent not only against the offending parties but for the ecosystem, as a whole. The other impact of wide coverage is to increase consumer awareness. The introduction of a penalty regimes has also enhanced the importance of legal counsels and information officers within organisations, thus, making it easier for them to impress upon these organisation and their employees the significance of data protection. Similarly, it has also increased the standing of the ICO, and it has been invested in raising public awareness of its work.[89] Much like the Spanish regime, the presence of mitigating factors play an important role in encouraging good behavior in the form of swift remedial actions, voluntary self-reporting, informing affected individuals and committing to future improvements. Finally, the proceeds of a monetary penalty regime can be used to fund other privacy enhancing projects, or compensate affected individuals, though this approach has not been adopted anywhere.

The other question is how fines should be computed, and when they should be enforced. The ICO can imposes monetary sanctions for cases where the data controller has committed a "serious contravention" likely to cause "substantial damage or substantial distress" and the controller was aware or ought to have aware of this outcome. This means that there is no real impact on minor breaches which are numerous, and the sanctions regime does not address these incidents in any way. The ICO also look as the previous and subsequent behavior of the data controllers brought to its attention. Another important ingredient of decision-making by the ICO to impose fines, is to evaluate the 'impact on the data controller' as a potential mitigating or aggravating factors. This is extremely relevant in terms of criticisms of regimes with strict enforcement that they impeded innovation or place too heavy a burden on burgeoning business models.

Ensuring fines are used effectively means the courts and/or DPAs must consider a variety of factors in determining, first, whether to issue a fine in any given instance and, second, how much that fine should be. In this respect, the considerations are not dissimilar to those faced by regulators in any other body of law: fines should be sufficiently high to act as a deterrent without causing undue hardship, should be proportionate to the breach and should reflect the regulator's view of the severity of the misconduct. Some of these factors are state below:

- The nature of the incident;
- The antecedent behaviour of the data controller;
- The subsequent behaviour of the data controller post the incident;
- The circumstances of the data controller;
- Factors external to the data controller;
- Whether fines are being combined with other measures

89 For instance, ICO keeps a record of all the enforcement action it takes. Available at https://ico.org.uk/action-weve-taken/enforcement/, last accessed on 30-01-2018

Undertakings

The ICO has leveraged the threat of fines into an alternative enforcement mechanism: seeking contractual undertakings from data controllers to take certain remedial steps. Although the practice began before fines were initially introduced, the regulator can encourage data controllers to take steps to avoid a fine and the resulting negative media coverage. Undertakings have significant advantages for the regulator. Since an undertaking is a more "co-operative" solution, it is less likely that a data controller will challenge it. An undertaking is simpler and easier to put in place. Furthermore, the ICO can put an undertaking in place quickly.

Privacy seals and trustmarks

Some DPAs, notably the CNIL and the ICO, have developed or are developing trustmarks. The first DPA-inspired privacy seal was the EuroPriSe seal, developed by the DPA from Schleswig-Holstein. Privacy seals are voluntary. To be able to use a privacy seal or trustmark, the applicant must meet and adhere to certain standards.

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

The data protection authority should have the power to: (a) issue codes of conduct/practice; (b) lay down standards for security safeguards; (c) lay down standards for data protection impact assessment. Where the standards relate also to matters beyond data protection, the data protection authority must work with sectoral regulators whose jurisdiction the additional matters may fall within. The data protection authority, working with the Bureau of Indian Standards, must designate sectoral supervisory bodies for the purpose of standards setting.

Chapter 11: Adjudication Process

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

It is imperative that the data protection authority has the power to receive complaints, carry out investigations and adjudicate complaints from individuals and other entities where the provisions of the data protection law have been breached.

2. 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?

The complaints must be heard by the Privacy Commission, the constitution of which is discussed in the last chapter.

The Privacy Commission shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying suits in respect of the following matters, namely –

(a) the summoning and enforcing the attendance of any person from any part of India and examining him on oath;

(b) the discovery and production of any document or other material object producible as evidence;

(c) the reception of evidence on affidavit;

(d) the requisitioning of any public record from any court or office;

(e) the issuing of any commission for the examination of witnesses.

The Privacy Commission shall have power to require any person, subject to any privilege which may be claimed by that person under any law for the time being in force, to furnish information on such points or matters as, in the opinion of the Privacy Commission, may be useful for, or relevant to, the subject matter of an inquiry and any person so required shall be deemed to be legally bound to furnish such information within the meaning of section 176 and section 177 of the Indian Penal Code, 1860 (45 of 1860).

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

As stated in the White Paper, given that the Appellate Tribunal has already been provided with the mandate to hear appeals from adjudicating officers under the IT Act, it may be

worthwhile to propose the Appellate Tribunal as an appellate forum for any decision passed by a data protection authority.

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

The data protection authority must have the power to impose both administrative fines and compensatory orders against breaching parties. Administrative fines should be discretionary rather than mandatory; they must be imposed on a case by case basis and must be "effective, proportionate and dissuasive". In the case of a minor infringement, or where a fine would impose a disproportionate burden on an organisation, a reprimand may be issued instead of a fine.

Compensatory orders must take into account the nature of data impacted by breach. We state below an illustrative list of factors relevant in determining the penalty:

- the nature, gravity and duration of the infringement having regard to the nature, scope or purpose of the processing concerned as well as the number of data subjects and level of
- damage suffered by them;
- whether the infringement is intentional or negligent;
- actions taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor;
- any relevant previous infringements;
- the degree of co-operation with the supervisory authority;
- categories of personal data affected;
- whether the infringement was notified by the controller or processor to the supervisory authority;
- any previous history of enforcement action;
- adherence to approved codes of conduct or approved certification mechanisms pursuant; and
- any other aggravating or mitigating factors applicable in the circumstances e.g. financial benefits gained, losses avoided, directly or indirectly, from the infringement

Chapter 12: Remedies

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

A civil penalty may be imposed for the following breaches:

a) Breach of any of the four grounds of processing

b) Failure to respect the nine National Privacy Principles

c) Failure to provide data subjects (in particular for any information addressed specifically to a child) with transparent information in a concise, transparent, intelligible and easily accessible form, using clear and plain language

d) Failure to comply with a right of access by the data subject for data concerning him or her.

e) Failure to comply with a right to rectification in relation to inaccurate data held about a data subject

f) Failure to comply with a right to erasure without undue delay

g) Failure to comply with a right to data portability in relation to data which he or she has supplied to a controller.

h) Failing to implement appropriate technical and organisational measures, prescribed by the DPA

i) Failure to co-operate with the data protection supervisory authority

j) Failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk

k) Failure to notify supervisory authority of data breaches within stipulated timelines or failure to provide reasonable explanation for the delay

l) Failure to notify data subjects of a data breach without undue delay

m) Failure to complete a data protection impact assessment in relation to high risk processing of personal data

n) Failure to appoint an independent and fully supported data protection officer

o) Transfer of data following a court or tribunal order to a third country without an international agreement, such as a mutual legal assistance treaty being in place

2. 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?

A strict liability standards must only be employed in case of breach of provisions where sensitive personal data is involved. In other cases, the the data protection authority must take into account factors mentioned above in Q. 4 of Chapter 11.