PART IV
REGULATION AND ENFORCEMENT

CHAPTER 1: ENFORCEMENT MODELS

1.1 Introduction

As a result of the nature and complexity of the legal provisions commonly constituting a data protection law, a broad range of questions arise regarding how these provisions can best be enforced. So as to develop a sound legal and regulatory framework, we must consider certain aspects of institutional design and overall approach before we can develop and align individual elements of the framework. This may be in terms of the extent of burden placed on entities covered under such framework, the structure and functions of any enforcement agency, or the tools at its disposal.

The enforcement of data protection norms is complicated by two factors primarily: first, the application of the norms across different fields, sectors, industries and contexts and, second, the rapid pace of development and change in data processing technologies.[656] These factors produce unique enforcement problems not found in other regulatory fields.

For instance, while many laws apply across different sectors, it has been observed that norms regarding information can be very contextual.[657] It could be quite problematic for a data protection law to run slip-shod over requirements in distinct walks of life that individuals desire to differentiate. Similarly, privacy norms have always been catching up to changes in technology that modify the playing field on which information is shared. The original conception of the right to privacy by Warren & Brandeis was driven by technological changes that permitted easier dissemination of information.[658] Similarly, the rise of computers and the internet have posed profound challenges for informational privacy.[659]

If anything, the rate of change of technology has only increased with time and appropriate legal responses are called for with greater rapidity. To add to this, different technologies with similar effects often come to be assessed according to various criteria including their prevalence and acceptability in society.[660] These concerns may not be capable of being addressed even where the substantive provisions of the law are technology-neutral. Instead, they additionally raise issues regarding the capacity of a data protection authority, if such an authority has been envisaged.

---

[656] Report of the Justice AP Shah Committee, 75 (October 16, 2012).
[657] Helen Nissenbaum, 'Privacy as Contextual Integrity,' 79 Washington Law Review 119, 137-41 (2004).
[658] Samuel Warren and Louis Brandeis, 'The Right to Privacy,' 4(5) Harvard Law Review 193 (15 December 1890).
[659] Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 Stanford Law Review 1193, 1202-03 (April 1998).
[660] For example, in determining whether there had been a 'search' under the Fourth Amendment, the US Supreme Court has differentiated aerial surveillance from thermal imaging of homes on the basis of how common each practice was. See, *Florida v. Riley*, 488 U.S. 445, 447, 452 (1989) and *Kyllo v. United States*, 533 U.S. 27, 34, 40 (2001).

1.2 Types of Enforcement Models

There have been concerns in the past regarding the strength and effectiveness of enforcement mechanisms in the Indian context, especially when it comes to technology-related laws.[661] Appropriate consideration must thus be given to the enforcement model that is to be employed. Generally, one may consider three different variations:[662]

(i) 'Command and control' regulation

This approach requires the State to provide legal rules or clear prescriptions for regulated entities, with no room for discretion. If these prescriptions are not followed, the State exercises its power to sanction. Where elements of a 'command and control' system are adopted, necessary features include the involvement of some governmental authority or the other, whether this involvement is through the establishment of a single, specialized agency or the creation of a federated, sectoral framework.

A number of issues are raised on this point, including whether the state machinery involved should be unified, how independent it should be from governmental control and industry influence, whether it should have regional spread, what regulatory tools and forms of sanction it should have at its disposal etc. Most jurisdictions do not have data protection frameworks that are purely 'command and control' in nature and create some room for industry involvement.

(ii) Self-regulation

This approach involves private organisations complying with standards they set for themselves without any enforcement by the State.[663] In a self-regulatory framework, norms become established either through market forces (such as demand for privacy from consumers), through industry standard-setting or through some limited facilitation of market transactions in the form of choice-enhancing legal rules such as information disclosure norms.

Legal obligations that enhance the fairness of transactions such as notice and privacy policy requirements may require governmental enforcement machinery and do not always fit comfortably in the self-regulation rubric. The US is a good example of a jurisdiction with largely self-regulatory elements, though a few sector-specific and state-specific laws are also in place. As these rules are a threshold requirement for achieving regulatory effectiveness,

[661] Deborah Roach Gaut and Barbara Crutchfield George, 'Offshore Outsourcing to India by U.S. and E.U. Companies Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing', 6 UC Davis Business Law Journal 13 (2006).
[662] Dennis D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' 34 Seattle University Law Review 439, 440-41 (2011).
[663] Reuben Binns, 'Data Protection Impact Assessments: A meta-regulatory approach,' 7(1) International Data Privacy Law 22, 25-29 (2017); Cary Coglienese and Evan Mendelson, 'Meta-regulation and Self-Regulation' in Oxford Handbook of Regulation, 146, 147-148 (Robert Baldwin *et al eds*., 2010).

they form core, substantive elements of a data protection framework and are not, appropriately, to be considered as part of the enforcement mechanism.

(iii) Co-regulation

This typically involves elements of both 'command and control' regulation and self-regulation. Co-regulation may be described as "initiatives in which government and industry share responsibility for drafting and enforcing regulatory standards."[664] This model advocates the formulation of a general data protection statute with broad provisions complemented by "codes of practices or conduct" formulated by the industry and approved by the government or the relevant data protection authority.

Once these codes are approved, compliance with the detailed requirements of the code is treated as compliance with or evidence of compliance with the general provisions of the statute, thus promoting legal certainty within an otherwise uncertain regulatory scheme through the creation of 'safe harbours'.[665] The reason for the uncertainty that would otherwise prevail is the inherent generality of a broad statute that is unable to capture the multitude of situations that can arise in data processing. Such a co-regulatory approach would therefore appear useful in promoting compliance while also making room for innovation within the digital economy which may otherwise come to be severely restricted, especially for small businesses and start-ups.

In the context of privacy law in India, it may be noted that a co-regulatory model was suggested by the Justice AP Shah Committee.[666] A 'command and control' regulatory mechanism may be too rigid and may lag behind rapid technological changes which are prevalent in today's day and age. On the other hand, a pure self-regulation approach may lack enforcement and may lead to a situation where the objectives sought to be achieved by a data protection law are, effectively, not met.[667] Co-regulation may seem like an appropriate middle path that combines the flexibility of self-regulation with the rigour of government rule-making.[668]

---

[664] Dennis D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' 34 Seattle University Law Review 439, 441 (2011) (describing co-regulation as "initiatives in which government and industry share responsibility for drafting and enforcing regulatory standards"); Hans-Bredow-Institut and Institute of European Media Law, 'Final Report: Study on Co-Regulation Measures in the Media Sector', 17 (June 2006).

[665] Dennis D. Hirsch, 'Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law,' 2013 Michigan State Law Review 83, 86-87, 96 (2013); Ira S. Rubinstein, 'Regulating Privacy by Design,' 26 (3) Berkeley Technology Law Journal 1410, 1451-53 (2011).

[666] Report of the Justice AP Shah Committee, 75 (October 16, 2012).

[667] S. Pearson and A. Charlesworth, 'Accountability as a Way Forward for Privacy Protection in the Cloud', in 5931 Cloud Computing, Lecture Notes in Computer Science 131, 133 (M.G. Jaatun *et al eds*., 2009).

[668] However, the processes by which rule-making and enforcing powers are shared can raise concerns regarding undue benefits to industry with public interest being sidelined; Neil Gunningham and Darren Sinclair, 'Leaders & Laggards: Next Generation Environmental Regulation', 105-06 (Greenleaf, 2002); regarding the scope for abuse, *see* Bradyn Fairclough, 'Privacy Piracy: The Shortcomings of the United States Data Privacy Regime and How to Fix It,' 42 (2) The Journal of Corporation Law 461, 476-77 (2016).

1.3 Provisional Views

Given that a co-regulation model envisages a spectrum of frameworks involving varying levels of government involvement and industry participation, it may be appropriate to pursue such a model that may be moulded to meet the circumstances as they emerge in the Indian context. It is also relevant to note that the co-regulation model is being adopted in most modern data protection systems to respond to the peculiar characteristics of this field of law.

1.4 Questions

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

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

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

4. Are there any alternative views to this?

CHAPTER 2: ACCOUNTABILITY AND ENFORCEMENT TOOLS

ACCOUNTABILITY

2.1 Introduction

The processing of personal data entails an increase of power (in terms of knowledge and its consequent insights) of the data controller vis-à-vis the individual. Data protection regulations are a means to help protect individuals from abuses of power resulting from the processing of their personal data. The method by which this protection was traditionally sought to be achieved was using notice and consent, offering the individual the autonomy to decide whether or not to allow her data to be processed after providing her full knowledge of what was going to be done with that data. As we have seen, that model has begun to come under pressure. Owing to the abundance of services, the complexity of data processing requirements and the multiplicity of purposes to which data can be put, notices have become too complex to understand. As a result, the concept of privacy self-management is coming under pressure given the complexity of the trade-offs between the benefits and the harms of modern technology.

To offset the flaws of the notice and choice model, a key principle that has emerged is of accountability as articulated in the EU GDPR. Central to accountability are the concepts of 'privacy by design' and 'privacy by default' which oblige businesses to consider data privacy at the initial design stages of a project as well as throughout the life cycle of the relevant data processing.[669] In this sense, accountability does not redefine data protection, nor does it replace existing law or regulation, since accountable organisations must comply with existing applicable law. Instead, accountability shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified privacy objectives.[670] A recent paper has suggested a much more aggressive use of accountability by holding data controllers responsible for all data under its control so much so that if a data subject suffers any harm as a result of a security breach or from the manner in which the data is processed, the data controller will be held liable for these harms.[671]

The essential elements of the principle of accountability in the EU are two-fold. First, a data controller should take appropriate measures to implement data protection principles. Second,

[669] Andrew Dunlop, Burges Salmon LLP, 'GDPR: The Accountability Principle', Lexology (10 November 2016), available at: https://www.lexology.com/library/detail.aspx?g=5454293d-7fea-4963-afc4-7e4310ed0a1e, (last accessed 23 November 2017).
[670] Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements A Document for Discussion', Hunton & Williams LLP (October 2009), available at: https://www.hunton.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf, (last accessed 21 November 2017).
[671] Rahul Matthan, 'Beyond Consent: A New Paradigm for Data Protection- Discussion Document 2017-03', Takshashila Institution (19 July 2017), available at: http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf, (last accessed 24 October 2017).

a data controller must be in a position to demonstrate, when asked by a supervisory authority, that such measures have been adopted.[672]

The principle of accountability emphasises that standards prescribed externally either by the law or by the industry must be implemented internally by organisations.[673] The onus of proving that such measures have been complied with is placed on the organisation. This in many ways paves the way for effective implementation of data protection principles.

A more expansive use of accountability may hold the data controller strictly liable for any harm caused as a consequence of processing by it, irrespective of whether appropriate measures to implement data protection principles are put in place and implemented. This principle may be considered for processing that is inherently risky, in consonance with the strict liability principle as developed in traditional tort law.[674]

To illustrate the working of the general principle of accountability, consider a data controller embarking on a new process that involves personal data processing. The data controller, before commencing such processing, must consider the relevant standards in the law which apply to the processing. The standards may include requirements relating to grounds of processing, notice, consent, data quality, security of collected data, questions of access to data when data is to be handled by a data processor, etc. The data controller must draw up a procedure or policy as to how it intends to meet these standards. In drawing up this policy or procedure, it must have regard to any binding code of practice, industry practices and any other external binding standard. The data controller may also take into account any voluntary standard beyond the baseline norm which it abides by. If harm is caused to an individual owing to such processing, the data controller will bear the burden of proof to demonstrate that it had a policy to prevent such harm and implemented such policy. If such a policy does not exist, or was not implemented strictly, the data controller would be liable for damages. If however it does exist and it has been implemented, there is still a strong case that the data subject should not be left without recourse. One way in which a situation like this can be met is for data controllers to insure against such contingency to adequately compensate the data subject.

In addition, or as an alternative, if the nature of data processing is inherently risky, then any harm caused to an individual that can be traced back to the processing, would result in liability of the data controller.[675] Simply demonstrating that certain organisational measures

---

[672] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability', European Commission (13 July 2010), 9, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf, (last accessed 2 November 2017).

[673] Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements A Document for Discussion', Hunton & Williams LLP (October 2009), available at: https://www.hunton.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf, (last accessed 21 November 2017).

[674] *Rylands v. Fletcher*, 1868 UKHL 1.

[675] *See* Baker Mckenzie, 'Accountability Obligations under the GDPR', available at: http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Accountability%20Obligations%20under%20the%20GDPR.pdf, (last accessed 23 November 2017).

have been taken or that the data subject consented to such use may not, by itself, be sufficient to disclaim liability.

The operation of this principle would mean that the processing of personal data by a data controller for its business needs commences and continues only in a manner which is in accord with the data protection principles. This approach, to some extent, shifts the burden away from the individual from having to constantly monitor whether his or her data is being processed as per law and ensures greater accountability for data controllers.

2.2 Issues

(i) Harm and Liability

The principle of accountability bears a close link to the liability to be cast on the data controller. In order to determine the contours of such liability, it may be important to establish what constitutes harm. For instance, if as a result of the manner in which the data is processed, the reputation of the individual is impaired so as to result in a loss in reputation or social standing of the individual, this could could have serious repercussions for the individual. Similarly, as a consequence of processing the data, the individual suffers any direct or indirect financial loss this could be easily identified as a harm that the data controller should be held accountable for. If the data controller uses the personal data about the individual in order to limit the choice available to the individual whether in terms of the information that she can access or any products or services that she is allowed to avail of, this too could be a harmful restriction of the options available to the individual. However, this kind of harm is of a qualitatively different nature as compared to the first two examples, constituting a denial of access or fair treatment, rather than material loss.

From amongst these, 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. Alternatively, if 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. A third alternative is for data controllers, or a certain class of data controllers to compulsorily take out insurance to cover certain types of harms caused to data subjects due to processing activities, even in a situation where the data controller has taken all reasonable measures according to law and established practices and standards.

(ii) Joint Controllers and Remoteness of Liability

Modern data processing is complex and often involves multiple service providers who process the individual's data simultaneously or sequentially. Primary data collected directly from the individual is often made available through application programming interfaces (APIs) that can be accessed by various secondary data controllers who either process this data themselves or make the data available for further processing down the line. If any harm

results from this chain of processing it will be difficult to adequately allocate responsibility. While the principle of joint and several liability may be applied, it could be unfair to data controllers who have genuinely taken all care and diligence to safeguard the individual from harm. On the other hand, having such a stringent norm could be what is required to ensure that the data controllers take adequate efforts to ensure that anyone down the chain who is given access to the data takes care to ensure that it does not result in any harm. This may be effectuated by data controllers taking indemnities against harm being caused to the data subject owing to any processing in this chain. This is consonant with the baseline principle that harm suffered by an individual should not remain unredressed.

(iii) Audit

Harms that result from improper processing of data are not always immediately evident. For instance, in many cases, the bias inherent in the decision making algorithms is not immediately discernible. It is only after a large number of people suffer from improper processing that we come to realise the harm that is being caused. This could well be too late and in order to appropriately protect the individual the law must suggest proactive measures that detect these harms early enough. Thus, in addition to requiring that personal data processing beyond certain scales must be commenced only after having in place a policy or prescribed organisational procedure, there could be provisions for audits (both internal and external). This would be critical in implementing the second limb of accountability, i.e. maintaining the burden of proof of compliance on the data controller. A requirement of audit would mean that the data controller must maintain records of measures and processes which could provide proof of compliance of data protection principles.

(iv) Security Safeguard Obligations

Appropriate technical and organisational measures to ensure security of personal data are central to the principle of accountability. These measures should be in-tune with the cyber threats of today. At the same time, these security obligations should keep in mind the costs of implementation of such measures which have to be kept operational constantly as security and privacy breach protection require constant assessment and reporting.

The EU GDPR provides general security obligations that the data controller and the processer must follow. These are summarised below:

a. Obligation to assess the risks and implement security measures to mitigate those risks.
b. 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.
c. 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).

The EU GDPR focuses on a "risk based approach" for continual assessment and adoption of mitigation measures. It does not mention whether the organisation should adopt a specific risk assessment industry standard (eg. ISO 27001, ISO 31000 etc). The only security practice it recommends is the use of pseudonymisation of personal data.

Accountability demands proactive actions from organisations including continuing investments to ensure that security safeguards are up to date. Organisations are expected to empower customers with tools and technologies to protect their data.

Under the existing privacy framework in India, Rule 8 of the SPDI Rules, mentions security practices that a body corporate should have in place for the purpose of protecting sensitive personal data. These security practices and standards should be supplemented by a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[676] It also mentions making use of international Information Technology Security Standards such as ISO 27001 and the use of code of best practices created by self-regulatory bodies, once approved and duly notified by the government.[677] The use of empanelled auditors to ensure compliance was these practices was also mandated.

Security safeguards obligations should provide adequate protection to the personal data of the individuals while taking into account the financial and organisational capabilities of data controller. A risk-based approach of dealing with potential security and associated privacy incidents could be the general norm. The approach should define the risk criteria, the mitigation measures and mechanisms to ensure reporting and continual improvement.

2.3 International Practices

European Union

The EU GDPR provides that a data controller would be responsible for, and must be able to demonstrate compliance with principles relating to the processing of personal data (these include the purpose limitation principle, data accuracy principle, storage limitation principle etc.).[678] The obligation requires data controllers to implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing activities are performed in accordance with the data protection obligations set out under the EU GDPR.[679]

Data controllers must also review and update such technical and organisational measures whenever necessary.[680] The measures incorporated would take into account the nature and

[676] Rule 8(1), SPDI Rules.
[677] Rule 8(3), SPDI Rules.
[678] Article 5(2), EU GDPR.
[679] Article 24, EU GDPR.
[680] Article 24(2), EU GDPR.

scope of the processing activity, as well as the risks posed to the individual by processing her personal information.[681] Risks could include physical, material, or non-material damage. Non-material damage could include: discrimination, fraud, and reputational damage.

In order to demonstrate that a data controller has complied with its obligations under the EU GDPR, it could implement internal data protection policies; maintain relevant documentation of processing activities; and use data protection impact assessments where appropriate.[682]

South Africa

The POPI Act sets out that a "responsible party" must ensure that certain conditions for lawful processing of personal data are satisfied at the time of processing.[683] The conditions for lawful processing of personal data are: accountability[684], processing limitation[685], purpose specification[686], further processing limitation,[687] information quality,[688] openness,[689] security safeguards,[690] and data subject participation.[691]

As part of the accountability principle, a responsible party must ensure that it secures the integrity and confidentiality of personal information in its possession by taking appropriate and reasonable technical and organisational measures in order to prevent loss, damage, or unauthorised destruction of personal information. The responsible party must also prevent unlawful access to, and unlawful processing of personal information. [692]

In order to ensure this, the POPI Act provides that a responsible party must take reasonable measures to identify all reasonably foreseeable internal and external risks to the personal information in its control, establish and maintain appropriate safeguards against these identified risks, verify that these safeguards are implemented and also to ensure that the safeguards are updated in order to respond to any new risks or to plug-in deficiencies found in the previous safeguard measures.[693]

The POPI Act has an additional obligation on third parties that process personal data on behalf of a responsible party. It provides that such third parties may process personal data only with the knowledge or authorisation of the responsible party and must treat personal information as confidential.[694] Additionally, the POPI Act provides that where an operator (a

[681] Article 25, EU GDPR, read with Recitals 74 and 75 of the EU GDPR.
[682] ICO, 'Accountability and Governance', available at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/, (last accessed 20 November 2017).
[683] Section 8, POPI Act.
[684] Section 8, POPI Act.
[685] Sections 9, 10, 11 and 12, POPI Act.
[686] Sections 13 and 14, POPI Act.
[687] Section 15, POPI Act.
[688] Section 16, POPI Act.
[689] Sections 17 and 18, POPI Act.
[690] Sections 19, 20, 21 and 22, POPI Act.
[691] Sections 23, 24 and 25, POPI Act.
[692] Sections 19(1)(a) and (b), POPI Act.
[693] Section 19(2), POPI Act.
[694] Section 20, POPI Act.

person who processes personal information for a responsible party on the basis of a contract) processes personal data, such operator is also bound to establish and maintain adequate security measures.[695]

Finally, in the event that the responsible party believes that the personal data of an individual has been accessed or acquired by an unauthorised party, then the responsible party must inform the Information Regulator. The responsible party must also notify the individual as soon as reasonably possible after the discovery of the data breach, and also take steps to restore the integrity of the responsible party's information system.[696]

Australia

Although the Privacy Act does not have a specific provision relating to accountability principle, the Privacy Act addresses this topic by way of the APPs under the said Act. For instance, APP 1 mandates open and transparent management of personal information. As per this principle, an APP entity must take reasonable steps to ensure the implementation of privacy practices and systems within the entity, which would ensure compliance with other data protection obligations under the Privacy Act.[697] Additionally, the said principles also provide that any entity holding personal information relating to an individual, must also take reasonable steps to protect this information from misuse, interference, loss, unauthorised access, modification or disclosure.[698]

Entities which come under the scope of the Privacy Act also have an additional obligation to destroy or de-identify personal information which is no longer required by an entity for any purpose.[699] The Privacy Act additionally mandates certain obligations on entities transferring personal information to overseas recipients. APP 8 provides that these entities must take reasonable steps to ensure that cross-border transfers do not breach any of the obligations set out under the Privacy Act and the APPs.[700] A breach of a privacy principle is said to occur when any activity of an entity is contrary to or inconsistent with the provisions set out under any of the APPs.[701]

Further, the OAIC has issued a "Guide to securing personal information", which provides some guidance as to the reasonable steps which entities are required to take in order to protect personal information in their control from misuse, interference, loss, unauthorised access, modification or disclosure. It also provides guidance on the reasonable steps which entities

[695] Section 21(1), POPI Act.
[696] Section 22, POPI Act.
[697] APP 1, Privacy Act.
[698] APP 11, Privacy Act.
[699] APP 11, Privacy Act.
[700] APP 8, Privacy Act.
[701] Section 6A, Privacy Act.

may take once personal information in their possession is no longer required.[702] However, this guide is not legally binding in nature.

Canada

Accountability in relation to privacy is the acceptance of responsibility for personal information protection. An organisation which is accountable to individuals must have in place appropriate policies and procedures that promote good privacy practices.[703] The model code for protection of personal information contained in Schedule 1 of PIPEDA sets out that an organisation is responsible for any personal information that is under its control. The organisation must also designate certain individuals who must be accountable for the organisation's compliance with the data protection obligations as set out under PIPEDA.[704]

PIPEDA also provides that an organisation is not only responsible for any personal information that is under its control, but is also responsible for any information transferred to a third party for processing. In such situations, an organisation must ensure that the third party also provides a comparable level of protection while processing personal information. This is usually ensured by contractual means.[705]

Additionally, organisations must implement policies and practices to protect personal information; establish procedures to receive and respond to complaints; train its staff about its data protection policies and practices.[706] PIPEDA provides that personal information must be protected by security safeguards appropriate to the sensitivity of the information. Security safeguards are intended to protect personal information against loss, theft, unauthorised access, disclosure, copying, use or modification.[707] The nature of safeguards, which an organisation is expected to implement, will be in accordance with the nature and sensitivity of the personal information in its possession.[708] Therefore, it follows that information of a more sensitive nature will be safeguarded by a higher level of protection. PIPEDA also prescriptively suggests some methods of protection that may be incorporated by an organisation. For instance, an organisation could utilise physical, organisational and technological measures to protect information in its possession.[709] Organisations must ensure that adequate care must be taken while disposing or destroying personal information, in order to prevent unauthorised parties from gaining access to the information.[710] The Office of the Privacy Commissioner has issued a guidance document to provide organisations assistance

[702] OAIC, 'Guide to Securing Personal Information: 'Reasonable steps' to protect personal information' (January 2015), available at: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf, (last accessed 20 November 2017).
[703] Office of the Privacy Commissioner of Canada, 'Getting Accountability Right with a Privacy Management Program', available at: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf, (last accessed 20 November 2017).
[704] Principle 1 of Schedule 1, PIPEDA.
[705] Clause 4.1.3, Principle 1 of Schedule 1, PIPEDA.
[706] Clause 4.1.4, Principle 1 of Schedule 1, PIPEDA.
[707] Clause 4.7.1, Principle 1 of Schedule 1, PIPEDA.
[708] Clause 4.7.2, Principle 1 of Schedule 1, PIPEDA.
[709] Clause 4.7.3, Principle 1 of Schedule 1, PIPEDA.
[710] Clause 4.7.5, Principle 1 of Schedule 1, PIPEDA.

with developing certain baseline accountability principles which would help develop a comprehensive privacy management program.[711]

As is clear from the above, jurisdictions across the world have implemented the principle of accountability in varied forms. At their core, however, these practices require data controllers to adopt processes and procedures which are consistent with data protection principles. In the Indian context, as mentioned above, it may be worth exploring whether a statutory requirement to adopt such measures can be linked to liability in cases of clearly defined harms.

2.4 Provisional Views

Accountability, as a principle of data protection, has existed for some time and has found mention in various privacy laws around the world. It is imperative that the data protection law reflects the principle of accountability. Accountability should not only be enforced for breach of data protection obligations through the adoption and implementation of standards by data controllers, but also in certain well defined circumstances, it could be extended to hold data controllers liable for the harms that they cause to individuals without further proof of violation of any other obligation. The data protection law should appropriately identify such harms for which the data controller should be held liable in this manner.

2.5 Questions

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

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

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

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

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

[711] Office of the Privacy Commissioner of Canada, 'Getting Accountability Right with a Privacy Management Program', available at: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf, (last accessed 20 November 2017).

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

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

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

ENFORCEMENT TOOLS

2.6 Introduction

A number of regulatory tools and mechanisms may be simultaneously utilized to achieve different enforcement objectives. Some of these may be based on a co-regulatory model whereas others may be based on a 'command and control' approach. These are discussed below.

A. CODES OF PRACTICE

2.7 Issues

A code of practice or conduct is considered an important element in establishing a workable co-regulatory data protection scheme. As has been discussed in Part IV, Chapter 1 of the White Paper, a co-regulatory framework is one that integrates elements of self-regulation with elements of governmental regulation. Codes of conduct originate in ordinary industry practices where associations engage in standard-setting for better service provision or manufacturing. They thus naturally form part of some self-regulatory systems in the form of voluntary codes with no force of law.

However, in a co-regulatory system, a code of conduct or practice is integrated into the broader regulatory scheme through recognition of different types in the general statute. While adoption of a code remains voluntary and its formulation still involves industry participation, co-regulation may involve encouraging their creation or allowing compliance with them to serve as evidence of compliance with the data protection statute. Issuance of such codes by a regulator or other forms of legal recognition allows for such standard-setting practices to be formalised and anchored to statutory processes. This would also improve the transparency of the processes by which such codes are formulated while codes themselves create transparency regarding how information is being processed in practice.[712]

Codes of conduct suffer from some issues when conceived of as purely self-regulatory.[713] However, when such codes are viewed as part of a co-regulatory framework, their true potential can be exploited. The manner in which co-regulation can introduce government oversight and other elements of accountability is illustrated in international practices below.

---

[712] OAIC, 'Guidelines for developing codes – issued under Part IIIB of the Privacy Act 1988' (September 2013), 2, available at: https://www.oaic.gov.au/resources/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes.pdf, (last accessed 28 October 2017).

[713] Margot Priest, 'The Privatization of Regulation: Five Models of Self-Regulation', 29(2) Ottawa Law Review 233, 242 (1998) (Codes of conduct only create accountability towards each other and not to the government; they engage in purely consensual rule-making; there is no real adjudication of violations or dispute resolution; there are very limited sanctions for violation apart from trade association dismissal; there is only limited coverage of the code across the industry due to its voluntary nature; and there is only rarely any involvement of the public or stakeholders external to the industry, no matter how large their stake).

2.8 International Practices

European Union

Under the EU GDPR, codes of conduct are recognised as compliance-signalling or demonstrating tools in a number of provisions.[714] Further provisions deal with the codes themselves stipulating that they can be formulated for subject matters like:[715]

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

After drafts of these codes of conduct are prepared by representative bodies and submitted to it, the supervisory authority must provide an opinion on the same and where it finds the code in compliance with the EU GDPR, it must approve, register and publish the same.[716]

United Kingdom

Section 51(3) of UK DPA states that at the direction of the Secretary of State or the discretion of the Information Commissioner, the Information Commissioner may himself prepare and disseminate codes of practice "for guidance as to good practice" after carrying out consultations. As per Section 51(4) of the UK DPA, the Information Commissioner is also required to encourage the preparation of such codes by trade associations. When such a draft code is submitted, the Information Commissioner must consider the draft and carry out consultations after which he may "notify the trade association whether in his opinion the code promotes the following of good practice."[717]

Canada

Section 24(c) of PIPEDA requires the Privacy Commissioner to encourage organizations to develop detailed policies and practices, including organizational codes of practice, towards compliance with processing obligations.[718]

---

[714] Articles 24(3), 28(5), 32(3), and 35(8), EU GDPR.
[715] Article 40, EU GDPR.
[716] Article 40, GDPR.
[717] Section 52(3), UK DPA further requires the Information Commissioner to lay before each House of Parliament any code of practice prepared on the direction of the Secretary of State but does not place this requirement for codes prepared by trade associations under Section 51(4).
[718] Codes may be developed for compliance with Sections 5 to 10, PIPEDA which deal with general obligations on the protection of personal information.

Australia

The Privacy Act makes extensive use of privacy codes as part of its overall framework through what are called APPs codes and Credit Reporting codes. These are envisaged to be developed by an entity, a group of entities, or a representative body or association of such entities. Under Part III B of the Privacy Act, the OAIC can approve and register enforceable codes developed by entities on their own initiative or on the request of the OAIC. These can be developed by the OAIC directly as well. These codes are envisaged to apply over and above the Privacy Act's provisions and detail how the Privacy Act's relevant provisions are to be complied with as well as who is bound by the code.[719] Entities bound by codes are required by law not to breach them[720] and such breach is deemed "an interference with the privacy of an individual".[721]

South Africa

Chapter 7 of the POPI Act lays down detailed provisions for codes of conduct, including for their issuance, notification, commencement, complaint mechanism, amendment, revocation, registration, review and compliance. A failure in compliance with an applicable code is deemed to be a breach of lawful processing conditions.[722] The Information Regulator issues such codes on its own initiative or on application by a representative body.[723]

2.9 Provisional Views

1. It may be important to incorporate and make provision for codes of practice within a data protection framework.

2. Such codes of conduct or practices may be issued by a data protection authority after appropriate consultations with the industry and individuals.

3. A data protection law may set out the various matters on which codes may be issued, which may include matters such as the best practices for privacy policies, data quality obligations or more core obligations on processing.

2.10 Questions

1. What are your views on this?

---

[719] OAIC, 'Guidelines for developing codes – issued under Part IIIB of the Privacy Act 1988' (September 2013), 2, available at: https://www.oaic.gov.au/resources/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes.pdf, (last accessed 28 October 2017).
[720] Sections 26A and 26L, Privacy Act.
[721] Section 13, Privacy Act; the Privacy Act further includes a number of detailed provisions regarding the form of any such code, how it is to be prepared and registered, and how it is to be monitored and governed. These include complaint and investigation provisions as well as provisions for reviewing, varying and removing codes.
[722] Section 68, POPI Act.
[723] Sections 60 and 61, POPI Act.

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

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

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

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

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

7. Are there any alternative views?

B. PERSONAL DATA BREACH NOTIFICATION

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

2.11 Issues and International Practices

(i) Defining Data Breaches

While data breaches may occur in various forms, these breaches can be classified using the fundamental principles of information security, i.e. confidentially, integrity and availability. So, a personal data breach may be categorised as the following:

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

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

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

Based on the circumstances, a breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these. Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. Carefully defining personal data breach is thus imperative.

The EU GDPR defines a "personal data breach" as *"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".*[724] Article 29 Working Party guidance on personal data breach notification notes that there is a difference between a security incident and a personal data breach.[725] A personal data breach is essentially a subset of a security incident. All personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. So, only a security incident that hampers the security, confidentiality or integrity of personal data would result in a 'personal data breach'.

[724] Article 4(12), EU GDPR.
[725] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679', European Commission (3 October 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741, (last accessed 10 November 2017).

In the US, personal data breaches are defined under sector-specific statutes or specific state laws. Under HIPAA Privacy Rule[726], a breach is, generally, an impermissible use or disclosure that compromises the security or privacy of the protected health information.[727] Privacy Technical Assistance Center (PTAC), established by the US department of education defines a data breach as any instance in which there is an unauthorized release or access of PII or other information not suitable for public release.[728]

Further, the California Security Breach Notification Act, 2016 defines a security breach as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the entity. Good-faith acquisition of personal information by an employee or agent of an entity for the purposes of the entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.[729]

North Dakota Century Code, Chapter 51-30 Notice of Security Breach for Personal Information defines a security breach as unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.[730]

It is important to note that although worded differently, US sector specific laws and a comprehensive privacy legislation like the EU GDPR, both recognise the cause and effect relationship between a security incident and a breach that may hamper personal data.

(ii) Data Breach Notifications

Data breach notification refers to the practice of alerting and informing stakeholders including data subjects that a personal data breach has occurred. The nature of notification required depends on the nature of data involved in the breach.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The EU GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to

[726] The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
[727] Office for Civil Rights (OCR), 'Breach Notification Rule', US Department of Health & Human Services (26 July 2013), available at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, (last accessed 20 November 2017).
[728] Privacy Technical Assistance Center, 'Data Breach Response Checklist' (September 2012), available at: http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf (last accessed 10 November 2017).
[729] Section 1(d), California Security Breach Notification Act, 2016.
[730] North Dakota Century Code, Chapter 51-30 Notice of Security Breach for Personal Information.

reputation, and loss of confidentiality of personal data protected by professional secrecy.[731] It can also include any other significant economic or social disadvantage to those individuals.

In general, the more sensitive the information involved, the more consequences there may be for the data subject. It is important to take note of this relationship between the degree of harm and the sensitivity of the data. Breach of sensitive personal data could have an immediate impact on the individual, which may lead to reputational or monetary damage.

Where there is a likely high risk of these adverse effects occurring, the EU GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible.[732] There needs to be an open line of communication between the organisation and its supervisory authority for the purpose of consultation with respect to the risk associated with the category of personal data the organisation is handling and the security safeguards, technical and policy, it has in place to tackle a breach associated with that category of personal data. The supervisory authority may advise the organisation based on the degree of harm for the individual, if and when the individual needs to be notified.

(iii) Breach Detection and Notification Duration

The EU GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.[733] There has been a great debate around whether the stipulated time frame for notification is too short and what does it mean to become "aware" of a personal data breach.

Becoming aware of a breach implies the detection of a security incident that has consequences for personal data of individuals by the organisation. The process of breach detection is very complex in nature, especially if the organisation has many allied business entities and the engages third party processors.

It is important to specify where this period of becoming aware of the breach begins. Is it when the allied business entities or third parties discover the breach or when the same is notified to the organisation acting as the data controller? It could take months, or even years to find and assess if the breach is in relation to personal data of an individual. The primary issue in relation to detection of breach is the large quantity of data that an organization has to comb through to find anomalies.

[731] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679', European Commission (3 October 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741, (last accessed 10 November 2017).
[732] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679', European Commission (3 October 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741, (last accessed 10 November 2017).
[733] Article 33(1), EU GDPR.

A research conducted by Ponemon Institute, sponsored by Arbor Networks and found that the average security breach (in North America and EMEA regions) in the retail services sector takes 197 days to detect and 98 days in the financial service sector.[734]

Under Section 6 of the New Mexico Data Breach Notification Act, 2017 (New Mexico Data Breach Act), a person that owns or licenses elements that include personal identifying information of a New Mexico resident shall provide notification to each New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach. Notification shall be made in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach**.**

The New Mexico Data Breach Act uses a time frame for notifying the individual in case of breach. It provides that the notification should happen as soon as possible but also provides an upper limit of 45 days for the purpose of notification to the affected individual. This legislation solely provides for one time notification of the individual affected by the breach in the manner prescribed under Section 7 of the said legislation.

This time frame allows the organisation to provide the individual with the information that would help her/him understanding how the incident took place, what is being done in this regard and the person or office to contact in case for following up. An argument in favour of this manner of notification would be that it doesn't create a situation of panic, which might happen if the individual is informed right at the time of initial detection. At the stage of initial detection, the organisation itself is many times in the dark and won't have enough information to answer the individual's queries and may result in an atmosphere of panic and mistrust. This point needs to be deliberated upon further in the Indian context, where the average individual's privacy awareness is at a very different level from what it is in the EU or the US.

While fixing a time period for breach notification it is also important to take into consideration the magnitude of the leak. If the number of individuals affected is in millions then would it be prudent to put in a place a notification requirement like we see in the EU GDPR where the data controller has only 72 hours to notify the individuals? It might be within the ability of a large organisation to put automated reporting and breach notification mechanisms in place. But that might not be the case with respect to SME and start-ups across sectors. Building a notification matrix based on the size of the organisations could be a way to tackle this problem, providing different time limits for notifying individuals. This could solve this particular problem but at the risk of complicating the notification mechanism greatly.

[734] Ponemon Institute LLC, 'Advanced Threats in Retail – A Study of North America & EMEA', ARBOR Networks, available at: https://pages.arbornetworks.com/Global_Ponemon_Retail.html?utm_source=Ponemon&utm_medium=blog_post&utm_term=AT&utm_content=whitepaper&utm_campaign=Ponemon_Retail, (last accessed 21 November 2017); Ponemon Institute LLC, 'Advanced Threats in Financial Services – A Study of North America & EMEA', ARBOR Networks, available at: https://pages.arbornetworks.com/Global_Ponemon_Financial_Services.html?utm_source=Ponemon&utm_medium=blog_post&utm_term=AT&utm_content=whitepaper&utm_campaign=Ponemon_FinServ, (last accessed 21 November 2017).

There is a need to put in place a notification time line that keeps in mind all the above-mentioned factors.

(iv) Notification Requirements

Once a personal data breach is established the organisation must notify the competent authority. In US, the HIPAA demands notification of breach to the affected individuals, and in certain circumstances, to the media. A media notification is required only if a breach affects more than 500 residents of a state or jurisdiction. Reporting to media might put significant burdens on small companies. This option should be carefully weighed. Depending upon the nature of the breach, magnitude of the breach and to whom the notification is addressed, the format of the notification has to be adapted.

(v) Individual Notification

As a best practice, a personal data breach notification should mention; the type of personal data breach, the estimated date of the breach (could be in the form of a range), 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 for administrative ease. But the content should reflect type of personal data breach, , the estimated date of the breach (could be in the form of a range), general description of the security incident, the estimated number of individuals affected by the breach, the steps being taken to minimise the impact of the breach and future resolution.

2.12 Provisional Views

1. The law may require that individuals be notified of data breaches where there is a liklelihood that they will suffer privacy harms as a result of data breaches.

2. The law may also require that the data protection authority or any authority be notified immediately on detention of data breaches.

3. Fixing too short a time period for individual notifications may be too onerous on smaller organisations and entities. This may prove to be counter productive as well as an organisation may not have the necessary information about the breach and its likely consequences.

4. The data protection authority may issue codes of practice which prescribe the formats for such notifications.

2.13 Questions

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

2. How should a personal data breach be defined?

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

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

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

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

C. CATEGORISATION OF DATA CONTROLLERS

2.14 Issues

Due to the breadth of a data protection law, its effectiveness can come to depend on the ability of a regulatory body to have adequate awareness and monitoring capacity of actual data protection practices so that it can identify and effectively address data protection risks. Not all processing activities pose risks of similar gravity and the nature or volume of the data being processed or the form of the processing operations themselves may require greater scrutiny and oversight. Such differentiation can be seen, for example, in banking regulation where "systemically important financial institutions" seem to require additional forms of regulation.[735]

An example of a general exemption on the basis of the nature of the entity may be found under the (Australian) Privacy Act,[736] 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. Other instances of differentiated regulation within the data protection laws of other jurisdictions are outlined in specific points below regarding the additional obligations for these different entities. Different jurisdictions have categorised data controllers for the purposes of certain additional obligations and have made this categorization on varying criteria.

2.15 Additional Obligations on Data Controllers

(i) Registration

In the context of data protection, there is a need for prior identification and availability for monitoring of data controllers. As a result of this, data protection laws can create a registration requirement for data controllers. However, given the sheer multitude of such entities, it may actually be counterproductive for the requirement to be placed on all of them.

International Practices

In the UK, as per Section 17 of the UK DPA, no processing of personal data can be done by any data controller unless an entry on that entity is included in the register maintained by the Information Commissioner. However, it allows for an exemption from registration for processing that is not harmful, through notification by the Secretary of State and for processing for the sole purpose of maintaining a public register.[737]

---

[735] Financial Stability Board, 'Reducing the moral hazard posed by systemically important financial institutions: FSB Recommendations and Time Lines' (20 October 2010), available at: http://www.fsb.org/wp-content/uploads/r_101111a.pdf, (last accessed 28 October 2017).
[736] Sections 6C, 6D and 6E Privacy Act.
[737] More than 400,000 organisations are currently registered: *See* ICO, 'Register (notify) under the Data Protection Act,' available at https://ico.org.uk/for-organisations/register/ (last accessed 28 October 2017).

(ii) Data Protection Impact Assessment

A data protection impact assessment (DPIA) is a process centred on evaluating activities that involve high risks to the data protection rights of individuals. The process can become necessary whenever a new project is taken up or a new policy is adopted by a data controller which may involve the use of a new technology or may have a significant impact on the data protection rights of individuals. A DPIA is aimed at describing the details regarding the processing activity, assessing the necessity and proportionality of such an activity, and helping manage the risks that are identified in relation to this activity.[738] The DPIA is carried out before the proposed processing activity is initiated so that the relevant data controller can plan the processing at the outset itself.

International Practices

European Union

Under Article 35 of the EU GDPR, there is a requirement to undertake a compulsory data protection impact assessment prior to data processing where a type of processing is likely to result in a high risk for the rights and freedoms of individuals. Certain kinds of processing activities are identified under the EU GDPR that would require such an assessment[739] and a supervisory authority is permitted to specify certain further activities that would trigger similar obligations.[740] Certain details regarding the contents of the assessment are also laid down. Recital 84 of the EU GDPR makes it clear that the outcome of the DPIA must be taken into account during the actual processing to demonstrate compliance and that where a DPIA indicates risks that cannot be mitigated, a consultation with the supervisory authority should be undertaken.[741]

Australia

Section 33D of the Privacy Act empowers the OAIC to direct an agency to carry out and submit a privacy impact assessment if the relevant activity or function might have a significant impact on the privacy of individuals. The provision also provides a non-exhaustive list of contents of the assessment.

Canada

Further, EU, Canada, Australia and South Africa do not appear to place any requirements for the registration of processing entities.

[738] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', European Commission (4 April 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, (last accessed 20 November 2017).

[739] Article 35(3), EU GDPR. A DPIA would be required for "a systematic and extensive evaluation of personal aspects" through automated processing, large scale processing of special categories of data, and processing of data related to criminal convictions and offences.

[740] Articles 35 (4) and (5), EU GDPR.

[741] It may be noted that the UK DPA and South Africa's POPI Act do not make DPIAs mandatory.

The Treasury Board of Canada Secretariat has released a directive making privacy impact assessments mandatory for all governmental bodies covered under Section 3 of the Canada Privacy Act.[742]

(iii) Data Protection Audit

Data protection audits are processes that can be undertaken by a regulated entity by itself, through an external auditor, or through the regulator to assess whether the entity's processing activities and overall policies are in line with applicable data protection law and good practice. The development of data protection auditing practices in an industry could well give rise to the establishment of specialised auditing agencies for this purpose and their empanelment under a data protection law may also be considered.

International Practices

European Union

The EU GDPR envisages a role for data protection audits within controller-processor contracts,[743] as a responsibility of a data protection officer,[744] as a mechanism for verification of compliance with binding corporate rules[745] as well as part of the investigative powers of a supervisory authority.[746]

United Kingdom

Under the UK DPA, the Information Commissioner is permitted to conduct audits with the consent of the data controller.[747]

Canada

Section 18 of the PIPEDA enables the Privacy Commissioner to carry out an audit of the "personal information management practices of an organisation" after giving reasonable notice and at a reasonable time.[748]

---

[742] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', European Commission (4 April 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, (last accessed 20 November 2017).
[743] Article 28(3)(h), EU GDPR.
[744] Article 39(1)(b), EU GDPR.
[745] Article 47(1)(j), EU GDPR.
[746] Article 58(1)(b), EU GDPR.
[747] Section 51(7), UK DPA specifically states that the Information Commissioner would 'assess any processing of personal data for the following of good practice' and then 'inform the data controller of the results of the assessment.'
[748] The provision also lays down extensive powers for the purposes of auditing including summoning and enforcing appearance, administering oath, receiving and accepting evidence, entering premises etc. that are along the lines of investigative powers.

Australia

The Privacy Act requires credit rating bodies to ensure that regular audits are carried out by an independent person to ensure that certain agreements with credit providers are being complied with.[749]

South Africa

Under Section 89 of the POPI Act, the Information Regulator is required to assess "whether an instance of processing of personal information complies with the provisions of [the] Act" in the prescribed manner. It may do so on its own initiative or on request by or on behalf of the responsible party, data subject or any other person. The provision clarifies the mandatory nature of such assessment, stating that it must be carried out by the Information Regulator "if it appears to be appropriate" though it may not make the assessment if, on a request, it is unable to identify the requester or the action that must be assessed.[750] Information notices are sent to the relevant organisation towards initiating an assessment.[751] A provision is also made regarding the assessment report resulting from the assessment process.[752] The report is to be given to the responsible party and the Information Regulator may also make any aspect of the assessment public if it is in public interest to do so.

(iv) Data Protection Officer

The designation of a specific individual or officer by a data controller to facilitate compliance through monitoring and advising as well as to act as a point of contact with a data protection authority is a crucial element of data protection laws. These individuals are often called data protection officers (DPOs).[753] It is relevant to note that in the present Indian legal framework, 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.[754]

International Practices

European Union

[749] Sections 20N (3)(b) and 20Q(2)(b), Privacy Act.
[750] Section 89(2), POPI Act. The criteria that the Information Regulator is to keep in mind when determining when it is 'appropriate' to make the assessment is also laid down. *See* Section 89(3), POPI Act.
[751] Section 90, POPI Act.
[752] Section 91, POPI Act.
[753] For example, as part of EU GDPR's accountability-based compliance framework, DPOs will be at the heart of the regulatory scheme, facilitating compliance with the provisions of the EU GDPR as key players: *See* Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')', European Commission (13 December 2016), 4-5, available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=43823, (last accessed 20 November 2017).
[754] Rule 5(9), SPDI Rules.

Under the EU GDPR, only certain data controllers are required to designate a DPO.[755] Some provision is also made to maintain the independence and effectiveness of this officer.[756] The tasks of the DPO include informing and advising on as well as monitoring compliance, advising on and monitoring the performance of DPIAs, cooperating with the supervisory authority and acting as the authorities' contact point on all relevant issues.[757]

Canada

Under the PIPEDA, an accountability framework is built around certain individuals who have been designated by an organisation for compliance with accountability provisions[758] and for receiving challenges/complaints regarding compliance.[759] The PIPEDA also states that the designation of such individuals does not relieve organisations of their duty to comply with obligations.[760]

South Africa

The POPI Act adopts the designation of an information officer from the Promotion of Access to Information Act, 2000.[761] Further, it provides for certain additional obligations for the information officer such as encouraging organisational compliance with the relevant law, dealing with requests made to the body under that law, and working with the Information Regulator in relation to investigations.[762]

2.16 Provisional Views

1. The effective enforcement of a data protection law may require some form of differentiated obligations so that certain entities covered under the framework whose processing activities create higher degrees of risk or may cause significant harm can be more readily engaged with and guided in ensuring compliance with relevant obligations.

---

[755] Article 37, EU GDPR. (The provision outlines three situations in which the obligation to appoint a DPO arises: first, for a public authority or body (except a court) carrying out processing; second, where the controller core activities require regular, systematic and large scale monitoring of persons; and third, where such core activities require large scale monitoring of certain special categories of data).

[756] Article 38, EU GDPR. (The DPO may be a staff member or may be on a service contract. It is further mandated that the DPO is to receive adequate support and should not be instructed on his data protection tasks or dismissed or penalised for performing them. Any other tasks he is asked to fulfil should not create any conflict of interest).

[757] Article 39, EU GDPR. Further, there is no provision in the UK DPA for the appointment of a DPO: *See* Anita Bapat and Adam Smith, 'United Kingdom: Data Protection 2017,' International Comparative Legal Guides (ICLG) (15 May 2017), available at: https://iclg.com/practice-areas/data-protection/data-protection-2017/united-kingdom, (last accessed 6 November 2017).

[758] Principle 1 of Schedule 1, PIPEDA (Accountability).

[759] Principle 10 of Schedule 1, PIPEDA (Challenging Compliance).

[760] Section 6, PIPEDA. Further, there is no provision in the Australian (Privacy Act) for for the appointment of a DPO: *See* Melissa Fai and Alex Borowsky, 'Australia: Data Protection 2017', International Comparative Legal Guides (ICLG) (15 May 2017), available at: https://iclg.com/practice-areas/data-protection/data-protection-2017/australia, (last accessed 6 November 2017).

[761] Section 1, POPI Act.

[762] Section 55, POPI Act.

2. The following additional obligations mentioned below may find place within the mechanism as appropriate:

(i) Registration

Registration obligations may be placed only for certain kinds of data controllers categorised on the basis of a specified criteria.

(ii) Data protection impact assessment

DPIAs may be required for certain categories of data controllers. Such DPIAs may, however, be undertaken in only specific instances, such as, where processing involves the use of new technology or likelihood of harm to any individual whose data is being processed.

(iii) Data audits

It would be beneficial for data protection law to provide for data protection audits in a regular manner for data controllers whose activities pose higher risks to the protection of personal data. A useful framework need not require the regulator to always carry out such audits itself and the law may provide for the registration of independent external auditing agencies. It may also contain some indication as to what an audit should cover in light of the technical nature of the compliance with certain obligations.

(iv) Data protection officer

There may be a substantial need for designating individuals who are made centres of accountability through their position in the data controller's organisation. Such officer may not only 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.

2.17 Questions

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

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

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

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

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

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

Registration

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

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

Data Protection Impact Assessment

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

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

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

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

5. Are there any alternative views on this?

Data Protection Audit

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

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

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

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

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

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

7. Are there any alternative views on this?

Data Protection Officer

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

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

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

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

5. Are there any alternative views?

D. DATA PROTECTION AUTHORITY

2.18 Issues

With rapid technological growth, there has been a surge in the processing of individuals' personal data for multiple purposes. The potential for harms to individuals has risen. While a data protection law may be enacted to protect individuals, the implementation and efficacy of such a law may be contingent on the establishment of a robust, independent and technically sound supervisory authority. This is all the more so since issues pertaining to data protection may be highly specialised and may require expertise in several areas such as data analytics, data science, law and associated issues.

Currently, in India, there is no separate authority to ensure compliance with data protection obligations required to be followed by data controllers. The IT Act is limited in its scope and provides for the appointment of adjudicating officers[763] and an appellate mechanism,[764] whose primary mandate is restricted to adjudication of disputes arising under the IT Act. Therefore, a stronger mechanism in the form of a central, oversight authority may be required in India in order to effectuate the effective protection of personal data.

While there is divergence regarding the structure of enforcement and oversight mechanisms in relation to data protection in various jurisdictions, there appears to be strong support for establishing a single centralised regulatory authority when possible.[765] Several countries have moved from a complex multi-agency regulatory structure to a simpler national agency structure.[766] The benefits of a single, centralised regulatory authority, especially in the context of international trade opportunities, appear to be considerable since multinational companies may have a single point of contact and such an authority can ensure consistency by issuing a single set of rules, guidelines or standards. Moreover, it is easier for individuals to seek guidance and direct queries and complaints in relation to a data protection violation from a single, centralised regulatory authority.

2.19 International Practices

(i) Composition and terms of service

European Union

[763] Section 46, IT Act.
[764] Section 48, IT Act.
[765] *See* United Nations Conference on Trade & Development (UNCTAD), 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (2016) available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf, (last accessed 25 October 2017).
[766] For example, Japan has moved from 30 regulators to just one. *See* United Nations Conference on Trade & Development (UNCTAD), 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (2016) available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf, (last accessed 25 October 2017).

The EU GDPR envisages the establishment of one or more supervisory authorities in each Member State of the EU to ensure compliance with the provisions of the EU GDPR.[767] The EU GDPR provides that Member States shall have the flexibility to choose the qualifications, the eligibility conditions and the rules and procedures for appointment of the members of the supervisory authority.[768] The EU GDPR also prescribes that the duration of service of each member must not be less than four years.[769] The EU GDPR lays down specific provisions for ensuring the independence of the members of the supervisory authorities.[770] Moreover, a member may be dismissed only in cases of serious misconduct if the member no longer fulfills the conditions required for the performance of her duties.[771]

United Kingdom

The UK DPA mandates the establishment of an Information Commissioner responsible for enforcement of the obligations set out under the UK DPA.[772] The Information Commissioner is appointed by Her Majesty by Letters Patent[773] for a maximum term of seven years.[774] To aid in the discharge of her duties, the Information Commissioner can appoint a deputy commissioner and as many officers and staff as she may determine.[775] Removal of the Information Commissioner may happen if she fails to discharge the functions of the office for a continuous period of at least three months, fails to comply with the terms of appointment, is convicted of a criminal offence, declares bankruptcy, or is otherwise unfit to hold office and unable to carry out her functions.[776] The Information Commissioner may be removed from office by Her Majesty with recommendation from both Houses of the Parliament.[777]

Canada

The Privacy Commissioner is responsible for enforcing the provisions of the PIPEDA. The Canada Privacy Act sets out the provisions for appointment, tenure and duties of the Privacy Commissioner. The Privacy Commissioner is appointed by the Governor in Council after consultation with the leader of every recognised party in the Senate and House of Commons

[767] Article 51, EU GDPR.
[768] Article 54, EU GDPR. Further, Article 53, EU GDPR specifies that each Member State shall provide that the appointment of each member of the supervisory authority shall be by means of a transparent procedure by their parliament, their government, their head of State or an independent body entrusted with such appointment.
[769] Article 54, EU GDPR.
[770] Article 52, EU GDPR provides that each member of the supervisory authority shall remain free from external influence, not take instructions from anyone, shall not undertake any action which is incompatible with their duties and not engage in any incompatible occupation during the term of their office. The supervisory authority must have its own staff which shall be subject to the exclusive direction of the members of the supervisory authority. Moreover, each Member State is required to ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has a separate public annual budget, which may be part of the overall state or national budget.
[771] Article 53, EU GDPR.
[772] Section 6 read with Schedule 5, UK DPA.
[773] Section 6(2), UK DPA.
[774] Rule 2(1) of Part I, Schedule 5, UK DPA.
[775] Rule 4(1) of Part I, Schedule 5, UK DPA.
[776] Rule 3A of Part I, Schedule 5, UK DPA.
[777] Rule 2(3) of Part I, Schedule 5, UK DPA.

and approval of the appointment by a resolution in the Senate and House of Commons.[778] The Privacy Commissioner holds office for a term of seven years but may be removed for cause by the Governor in Council at any time on address of the Senate and House of Commons.[779] The Canada Privacy Act also lays down specific provisions for ensuring the independence of the Privacy Commissioner.[780]

South Africa

The POPI Act establishes an independent Information Regulator which is tasked with governing the protection of personal information.[781] The Information Regulator is composed of a Chairperson and four members.[782] The POPI Act specifically includes strict instructions on the composition of the Information Regulator, i.e., at least one member of the Information Regulator must be appointed on account of experience as an advocate, attorney, or professor of law.[783] The remainder of the members may be appointed based on any other relevant qualifications.[784] The Chairperson and two regular members must be full-time employees whereas, the other two members may be there in a full-time or part-time capacity.[785] To be appointed within this body an applicant must be a citizen, a public servant, a member of some government body, employee of a political party, mentally fit, without criminal record, and must be chosen by the President on recommendation bythe National Assembly.[786] A committee is created within the National Assembly that nominates a member, who must then be approved by a majority of the Assembly.[787] The members may not be appointed for a period longer than five years, but will be eligible for reappointment at the the end of the term.[788] To ensure the lawful enactment of the duties of the Information Regulator, the POPI Act explicitly states that the Information Regulator must be impartial and perform its functions without fear, favour or prejudice.[789] The members are not permitted to undertake any other remunerative work while they hold office.[790]

Australia

[778] Section 53(1) of the Canada Privacy Act.
[779] Section 53(2) of the Canada Privacy Act.
[780] Section 54 of the Canada Privacy Act stipulates that the Privacy Commissioner shall engage exclusively in the duties of the office of the Privacy Commissioner and shall not engage in any other employment for reward. Further, the Privacy Commissioner shall be paid a salary equal to that of a judge of the Federal Court and shall also be entitled to a pension equivalent of that received by others in public service.
[781] Section 39, POPI Act.
[782] Section 41, POPI Act.
[783] Section 41, POPI Act.
[784] Section 41, POPI Act.
[785] Section 41, POPI Act.
[786] Section 41, POPI Act.
[787] Section 41, POPI Act.
[788] Section 41, POPI Act.
[789] Section 39(b), POPI Act.
[790] Section 41, POPI Act.

The OAIC is mandated to ensure enforcement of the provisions of the Privacy Act.[791] The OAIC is appointed by the Governor‑General by a written instrument[792] for a duration of no more than five years.[793] To ensure the lawful enactment of his/her duties by the OAIC, she may not engage in paid employment outside the duties of his or her office without the Minister's approval.[794]

(ii) Functions, powers and duties of data protection authorities

European Union

The functions, duties and powers of the supervisory authority under EU GDPR include the following:[795]

a. Monitoring, enforcement and investigation

The supervisory authority must monitor and enforce the application of the EU GDPR. It also has the power to handle complaints lodged by a data subject, duty to investigate the complaint (including obtaining from the data controller access to all personal data as required) and inform the complainant of the progress and outcome of the investigation within a reasonable period. The supervisory authority has the power to order the rectification or erasure of personal data, issue warnings and reprimands, and impose administrative fines on a data controller in case of breach of data protection obligations. The supervisory authority also has the power to carry out data protection audits and impact assessments.

b. Advisory powers

The supervisory authority can advise the Member States and other institutions on legislative and administrative measures relating to protection of natural persons' rights and freedoms about processing.

c. Standard setting powers

The supervisory authority can establish codes of conduct, encourage the establishment of data protection certification mechanisms, data protection seals and marks, and undertake periodic review of issued certifications.

d. Awareness generation

[791] The OAIC is established under Section 5, Australian Information Commissioner Act, 2010 (Australian Information Commissioner Act).
[792] Section 14, Australian Information Commissioner Act.
[793] Section 15, Australian Information Commissioner Act. Per Section 16, Australian Information Commissioner Act, the OAIC is not permitted to engage in paid employment outside the duties of her office without the Minister's approval.
[794] Section 16, Australian Information Commissioner Act.
[795] *See* Articles 35, 57, 58, 77 and 83, EU GDPR.

The supervisory authority shall promote awareness of data controllers and processors of their obligations under the EU GDPR and promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing.

United Kingdom

The functions, duties and powers of the Information Commissioner of UK include the following:[796]

a. Monitoring and enforcement

The Information Commissioner has the power to issue an 'enforcement notice', 'assessment notice' and 'information notice' in order to determine whether the data controller has complied with the provisions of the UK DPA.[797]

b. Standard setting powers

The Information Commissioner may encourage trade associations to prepare and to disseminate to their members codes of practices, and where any trade association submits a code of practice to the Information Commissioner for her consideration, notify the trade association whether in her opinion the code promotes the following of good practice.

c. Awareness generation

The Information Commissioner must also provide educational materials to the public so that individuals are aware of their data protection rights. In order to ensure that data controllers are aware of their obligations in relation to processing operations of personal data, the Information Commissioner can disseminate information to data controllers that pertains to the same.

Canada

The functions, duties and powers of the Privacy Commissioner include the following:

a. Monitoring, enforcement and investigation

The Privacy Commissioner's investigative powers predominantly include the handling of all complaints filed under PIPEDA.[798] While conducting an investigation, the Privacy Commissioner may review evidence, collect relevant records, and enter any premises and prepare a report within one year of filing of the complaint that contains all the findings and recommendations.[799] Where the Privacy Commissioner deems a complaint resolvable without

[796] Section 51, UK DPA.
[797] Sections 40, 41A and 43, UK DPA.
[798] Section 11(1), PIPEDA.
[799] Section 13(1), PIPEDA.

extensive investigation, she may resolve such complaint through dispute resolution mechanisms, such as, mediation and conciliation.[800]

b. Awareness generation

The Privacy Commissioner is required to promote research activities relating to the privacy of individuals and processing of personal information by persons other than by government institutions. [801]

South Africa

The functions, duties and powers of the Information Regulator of South Africa include the following:[802]

a. Awareness generation

This includes advising public and private entities on data protection matters and ensuring no influential actions are taken that risk the protection of personal information.

b. Monitoring, enforcement and investigation

This includes investigation and resolving of complaints arising under the POPI Act. It also includes monitoring developments in information processing and computer technology. Further, the Information Regulator is also required to conduct an assessment of a public or private body in respect of processing of personal information.

c. Laying down codes of conduct and facilitating cross-border cooperation

This includes assisting bodies to develop codes of conduct regarding protection of personal information. Further, it also includes consulting with national and international bodies that are concerned with data protection or information processing.

Australia

The functions, duties and powers of the OAIC include the following:[803]

a. Guidance related functions

It includes making guidelines to adopt best practices in relation to data protection. The OAIC should promote an understanding of APPs.

[800] Section 12.1(2), PIPEDA.
[801] Section 60(1), Canada Privacy Act.
[802] Section 40, POPI Act.
[803] Section 28, 28A, 28B, Privacy Act.

b. Advisory

The functions of the OAIC include providing advice to a Minister or entity regarding data protection. The OAIC must provide reports and recommendations to the Minister regarding protection of the privacy of individuals.

c. Monitoring, enforcement and investigation

The OAIC is required to monitor the accuracy of information held by the entity. It must also ensure no entity is using information for unauthorised purposes. The investigative powers of the OAIC include the power to conduct investigation, obtain information and documents and the power to examine witnesses.[804]

2.20 Provisional Views

1. Based on the above, it follows that a separate and independent data protection authority may be set up in India for enforcement of a data protection legal framework.

2. There are three broad categories of functions, powers and duties which may be performed by a data protection authority: monitoring, enforcement and investigation; standard-setting; and awareness generation.

3. Specifically, the above functions may include:

(i) Monitoring, enforcement and investigation

This may include the power to (a) ensure compliance and enforcement with the provisions of a data protection law; (b) conduct inspection, investigations and collect documents as may be required; (c) adjudicate disputes arising between individuals and data controllers; (d) monitor cross-border transfer of data; (e) monitor security breaches; (f) issue directions to all relevant entities; (g) impose civil penalties for non-compliance; and (h) issue regulations in order to facilitate the enforcement of data protection principles and other ancillary matters relating to data protection.[805]

(ii) Awareness generation

This may include: (a) the ability to conduct research and promote public awareness of data protection; and (b) the power to educate public and private entities.

(iii) Standard setting

[804] *See* Part V, Privacy Act.
[805] The power to issue regulations are standard provisions which are there in the TRAI Act, Securities and Exchange Board of India Act, 2002 (SEBI Act), and the Insurance Regulatory and Development Authority Act, 1999.

This may include 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; and (d) lay down standards for registration for data controllers as may be required and maintain a database in this regard. Some of these standards relate to data protection issues, e.g., standards for data protection impact assessments; others such as standards for security safeguards are not *per se* related to data protection. The role of the central government in relation to setting of standards for the latter and such analogous categories and organisational measures should be ensured.

2.21 Questions

1. What are your views on the above?

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

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

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

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

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

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

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

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

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

11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of

standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

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

CHAPTER 3: ADJUDICATION PROCESS

3.1 Introduction

Adjudication plays an integral role in the enforcement of any law as it ascertains the rights and obligations of parties involved in a dispute and prescribes the corrective actions and remedies. In the context of a data protection law, adjudication entails an assessment of whether and to what extent data protection rights of an individual have been infringed by a data controller, the loss or damage suffered by the individual due to the said infringement, the remedies available to the individual as well as the penal consequences that the data controller may be liable for. Given the technical and specialised nature of the issues that may arise while adjudicating under a data protection law, it is imperative to evaluate the shortcomings of existing adjudicatory mechanisms in India in this field and propose an adjudicatory framework along with the remedies that may be available (the substantive issues relating to 'Remedies' is dealt with in Part IV, Chapter 4 of the White Paper).

3.2 Issues

Under the extant Indian legal framework, specifically the IT Act, a special class of officers called 'adjudicating officers' are appointed for hearing and adjudicating cases pertaining to violations of the provisions of the IT Act or of any rule, regulation, direction or order made thereunder.[806] The IT Act also specifies certain disputes in relation to which the adjudicating officer has the power to adjudicate.[807]

An adjudicating officer is an officer not below the rank of a 'Director' to the Government of India or an equivalent officer of a State Government and is required to have such experience in the field of information technology and legal or judicial experience as may be prescribed.[808] Further, an adjudicating officer is required to adjudicate matters in which the claim for injury or damage does not exceed Rs. 5 crores.[809] Moreover, while adjudicating, an adjudicating officer shall have the powers of a civil court.[810]

It is relevant to note that the adjudicatory functions discharged by adjudicating officers primarily relate to fraudulent transactions from bank accounts on account of failure to

[806] Section 46(1), IT Act.
[807] Sections 43 (Penalty and compensation for damage to computer, computer system, etc.), 43A (Compensation for failure to protect data), 44 (Penalty for failure to furnish information, return, etc.) and 45 (Residuary penalty), IT Act.
[808] Section 46(1) and (3), IT Act.
[809] Section 46(1A), IT Act. Please note that jurisdiction in respect of a claim for injury or damage exceeding Rs. 5 crores shall vest with the competent court.
[810] Section 46(5), IT Act. All proceedings before an adjudicating officer shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228, IPC, shall be deemed to be a civil court for the purposes of Section 345 and 346, CrPC and shall be deemed to be a civil court for the purposes of Order XXI, Civil Procedure Code, 1908 (CPC).

maintain reasonable security practices[811] and as such, it appears that such orders may not *per se* relate to other aspects of data protection violation.

So far as the appellate mechanism under the IT Act is concerned, prior to the enactment of the Finance Act, 2017 (Finance Act), appeals from decisions of adjudicating officers lay before the CyAT set up under Section 48 of the IT Act. The CyAT, which started functioning in 2006, was set up with a specific mandate to hear appeals on matters where the jurisdiction of civil courts was barred, i.e. where the claim for injury or damage does not exceed Rs. 5 crores.[812] However, the CyAT has, as of 31 March 2017, passed merely 17 judgments and has passed no judgement after 30 June 2011.[813] Moreover, the chairman's position for the CyAT has been lying vacant since July 2011 and consequently, though appointment of members has been carried on, a bench to hear the matters has not been constituted in the absence of a chairman.

In order to bring about rationalisation of tribunals, uniformity in service, efficiency and cost optimisation[814], the IT Act was amended by the Finance Act to confer the powers of the CyAT to hear appeals from the decisions of the adjudicating officers to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT or Appellate Tribunal)[815]. There are concerns on whether the current resources, capacity and infrastructure of the Appellate Tribunal can take on the additional mandate of discharging the functions of the CyAT[816].

Upon adjudication, the adjudicating officer under the IT Act has the power to give remedies in the form of either a civil penalty imposed upon the defaulter or grant compensation to the aggrieved individual. Section 43A of the IT Act stipulate that any person who commits the acts specified under the said provision shall be liable to pay damages by way of compensation to the person so affected.[817] Given that there does not appear to be any specific limit on the amount of compensation payable under this provision, it follows that a person affected by an infringement may assess the damages on her own so long as the amount assessed does not

---

[811] Sreenidhi Srinivasan and Namrata Mukherjee, 'Building An Effective Data Protection Regime', Vidhi Centre For Legal Policy 19 (January 2017). *Also see Ram Techno Park v. State Bank of India*, Complaint No. 9 of 2012, Adjudicating Officer (Maharashtra) Order dated 22 February 2013, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudication_RamTechno_Vs_SBI-22022013.pdf, (last accessed 23 October 2017) and *M/s Shreenivas Signs Pvt. Ltd. v. IDBI Bank Ltd.*, Complaint No. 12 of 2013, Adjudicating Officer (Maharashtra) Order dated 18 February 2014, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudication_SreenivasSigns_Vs_IDBI-18022014.PDF, (last accessed 23 October 2017).

[812] Section 61, IT Act.

[813] *See* 'Judgments', Cyber Appellate Tribunal, available at http://cyatindia.gov.in/Judgement.aspx (last accessed 22 October 2017).

[814] Radhika Merwin, 'Merger of tribunals to rationalize working', Hindu Business Line (23 March 2017), available at: http://www.thehindubusinessline.com/economy/policy/merger-of-tribunals-to-rationalise-working/article9598534.ece, (last accessed 22 October 2017).

[815] The TDSAT is established under Section 14 of the TRAI Act. An appeal from the TDSAT lies with the Supreme Court of India (as per Section 18, TRAI Act).

[816] It is relevant to note that in 2004, the TDSAT's jurisdiction was extended to cover broadcasting services. Moreover, per the Finance Act, the mandate of the Airports Economic Regulatory Authority Appellate Tribunal has also been transferred to the TDSAT (in addition to that of the CyAT).

[817] Similar provision is contained in Section 43, IT Act.

exceed Rs. 5 crores.[818] Furthermore, in case of a contravention of the provisions of the IT Act for which no penalty has been prescribed separately, the defaulting person shall be liable to pay a penalty not exceeding Rs. 25,000 or compensation not exceeding Rs. 25,000.[819]

Compensation, as a remedy under Section 43A of the IT Act is extremely limited and is applicable where a body corporate fails to maintain and implement reasonable security practices and procedures. Moreover, for any other violation of the provisions of the IT Act (for which no separate penalty is prescribed), the amount of compensation that may be claimed is limited to Rs. 25,000. In the context of adjudication of disputes pertaining to data protection violation, it may be relevant to consider the extent to which adjudicatory bodies may grant compensation to an aggrieved party and consequently, determine the jurisdiction and powers of adjudicatory bodies in this regard.

3.3 International Practices

European Union

Under the EU GDPR, the supervisory authority set up in every Member State has the power to investigate complaints relating to the breach of any of the rights of the data subject.[820] The supervisory authority has a wide range of investigative powers[821] and corrective powers.[822] A data subject may file a complaint with the supervisory authority where she considers that the processing of personal data related to her infringes the EU GDPR.[823] The supervisory authority has the power to impose an administrative penalty on the data controller where the latter has breached the provisions of the EU GDPR.[824] The data subject, however, also has the right to bring an appeal or seek a remedy from the competent courts of the Member States where the supervisory authority is established where the said authority does not handle the complaint or does not inform the data subject about the progress or outcome of the complaint within the prescribed time limit.[825]

United Kingdom

Under the UK DPA, the Information Commissioner has several powers including the power to issue 'enforcement notices' to data controllers in case of contravention of the provisions of the UK DPA.[826] The Information Commissioner also has the power to issue 'assessment

[818] Please note that for a claim above Rs. 5 crores, the claim will be filed with a civil court having competent territorial and pecuniary jurisdiction. In other words, when such a claim is filed with a civil court, then the special adjudicatory mechanism of the IT Act will no longer be the procedural law and the process will be governed by the provisions of the CPC. *See* Apar Gupta, 'Commentary on Information Technology Act', 184 (Lexis Nexis, 2013).
[819] Section 45, IT Act. Section 44, IT Act only prescribes a penalty for failure to furnish information, return, etc.
[820] Article 57(1)(f), EU GDPR.
[821] Article 58(1), EU GDPR.
[822] Article 58(2), EU GDPR.
[823] Article 77(1), EU GDPR.
[824] Article 83, EU GDPR.
[825] Article 78, EU GDPR.
[826] Section 40, UK DPA.

notices'[827] and 'information notices' in order to determine whether the data controller has complied with the provisions of the UK DPA.[828] Where a data controller fails to comply with any of the notices, then it may be considered as an offence under the UK DPA.[829] The Information Commissioner may impose a monetary penalty upon the data controller for contravention of data protection principles.[830] A data controller on whom any type of notice under the UK DPA has been served by the Information Commissioner, has the right to file an appeal with the First-tier Tribunal.[831]

Australia

Under the Privacy Act, in case of a breach of the privacy principles, an individual can file a complaint with the OAIC.[832] Where it is not feasible to conciliate between the parties, the OAIC may undertake an investigation and upon finding of a substantiated complaint, can direct the respondent to not repeat such a conduct or perform a reasonable act to redress the loss suffered by the individual.[833] On an application by the OAIC, if the prescribed court is satisfied that the respondent has contravened the provisions of the Privacy Act, it may order the respondent to pay a penalty.[834] The OAIC may also undertake the above on the basis of a *suo moto* action.[835] Moreover, an application for review of an order made by the OAIC lies with the Administrative Appeals Tribunal.[836]

Canada

In Canada, under the PIPEDA, the Privacy Commissioner may take cognizance of a complaint filed by an individual or on its own.[837] Upon filing of a complaint, the Privacy Commissioner may conduct an investigation.[838] Upon completion of investigation, the Privacy Commissioner is required to prepare a report consisting of its findings and recommendations.[839] On receiving the report, the individual may apply to the court for a hearing in respect of the matter in relation to which the complaint was made or that is referred to in the Privacy Commissioner's report.[840] The court may direct the organization to correct its practices and award damages to the complainant.[841]

---

[827] Sections 41A, 41B, 41C and 42, UK DPA.
[828] Section 43, UK DPA.
[829] Section 47, UK DPA.
[830] Sections 55A-55E, UK DPA.
[831] Section 48, UK DPA read with ICO, "Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998", 3 (December 2015), available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf, (last accessed 20 October 2017).
[832] Section 36, Privacy Act.
[833] Section 52, Privacy Act.
[834] Section 80W, Privacy Act.
[835] Section 52(1A) read with Section 40(2), Privacy Act.
[836] Section 96, Privacy Act.
[837] Section 11, PIPEDA.
[838] Section 12, PIPEDA.
[839] Section 13, PIPEDA.
[840] Section 14, PIPEDA.
[841] Section 16, PIPEDA.

Under the POPI Act, the Information Regulator may undertake investigation into a complaint submitted by a person for, *inter alia*, breach of the conditions of lawful processing of personal information.[842] The Information Regulator may also, on its own initiative, commence investigation.[843] On receipt of a complaint, the Information Regulator may conduct a pre-investigation[844], act as a conciliator, conduct a full investigation or refer the complaint to its enforcement committee[845]. Where the Information Regulator is satisfied with the organization has interfered with the protection of personal information of the complainant, the Information Regulator may issue a notice directing the organization to take corrective steps accordingly.[846] A penalty may also be imposed on the organization.[847] A right of appeal against the direction/notice of the Information Commissioner lies with the High Court having the requisite jurisdiction.[848]

3.4 Provisional Views

1. Given that under a data protection legal regime, government bodies and public authorities may be considered as data controllers, an adjudicating officer appointed under the IT Act, who is an officer of the government, may not be the appropriate body to adjudicate disputes which involve violation of data protection obligations by such government bodies and public authorities. Therefore, it may be appropriate for a separate, independent body, such as, a data protection authority to adjudicate on disputes arising between an individual and a data controller due to breach of any data protection obligation.

2. It follows that an individual whose data protection rights have been violated may, at the outset, first approach the data controller or a specific grievance redressal officer of the data controller identified in this regard.

3. Where the data controller fails to resolve the complaint of the individual in a satisfactory and expeditious manner, the individual may be given the right to file a complaint with the data protection authority. Moreover, where the data protection authority observes any violation by a data controller of any of the provisions of a data protection law, it may initiate action against such data controller on a *suo motu* basis.

4. The data protection authority may be conferred with the power to appoint an adjudicating officer who may have the requisite qualifications and expertise to inquire into the facts of the complaint and adjudicate accordingly.

[842] Sections 73 and 74, POPI Act.
[843] Section 76(3), POPI Act.
[844] Section 79, POPI Act.
[845] Section 92, POPI Act.
[846] Section 95, POPI Act.
[847] Section 109, POPI Act.
[848] Section 97, POPI Act.

5. 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. This, of course, will be subject to suitable amendments to the TRAI Act along with the constitution of specialised benches having the requisite technical knowledge and expertise as required to achieve this purpose.

6. In addition to the powers described in the previous section on 'Data Protection Authority' (Part IV, Chapter 2 of the White Paper), the data protection authority may be given the power to impose civil penalties as well as order the defaulting party to pay compensation.

7. Specifically, in case of compensation claims, the consumer fora set up under the Consumer Protection Act, 1986 (COPRA) typically act as avenues for filing such claims. However, it is relevant to note that given the vast number of data controllers operating in the Indian market and the number of potential data protection violation claims that may be brought by individuals, the consumer fora, especially at the district and state levels, may not have the requisite capacity as well as the technical knowledge and expertise to adjudicate on compensation claims arising from such violations. Moreover, if all compensation claims lie with the consumer fora, it may not incentivise individuals to file complaints with the data protection authority for enforcement and instead file claims relating to compensation with the consumer fora.

8. Consequently, it may be proposed that matters in which compensation claims for injury or damage does not exceed a prescribed threshold, may lie with the data protection authority. Further, an appeal from an order of the data protection authority granting such compensation and matters in which compensation claims for injury or damage exceeds such threshold may lie with the National Commission Disputes Redressal Commission (National Commission). This may be undertaken pursuant to requisite amendments to the COPRA and by setting up benches with the requisite technical skills and expertise.

3.5 Questions

1. What are your views on the above?

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

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

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

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

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

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

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

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

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

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

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

13. Should class action suits be permitted?

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

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

CHAPTER 4: REMEDIES

A. PENALTIES

In the context of a data protection law, civil penalties may be calculated in a manner to ensure that the quantum of civil penalty imposed not only acts as a sanction but also acts as a deterrence to data controllers, which have violated their obligations under a data protection law.

4.1 Issues

The IT Act does not appear to prescribe civil penalty provisions specifically for violation of data protection obligations.[849] The provisions of the IT Act are limited in their applicability and do not appear to take into account the wide range of instances of data protection violation which may occur due to advancement in technology used towards processing of personal data. Moreover, the quantum of penalty prescribed under the provisions of the IT Act appear to be inadequate and may not act as a deterrence to emerging e-commerce and other technology based players in India. Therefore, the critical issue in relation to civil penalties under a data protection legal framework pertains to the manner in which such penalties may be determined or calculated and the quantum of such penalties which may act as adequate deterrence.

4.2 International Practices

European Union

The EU GDPR mandates that the administrative fines imposed by a supervisory authority in each individual case must be effective, proportionate and dissuasive.[850] For specific violations, the EU GDPR prescribes an administrative fine of up to EUR 20,000,000, or in the case of an undertaking, up to four percent of the total worldwide turnover of the preceding financial year, whichever is higher. [851] In other words, administrative penalty that may be imposed on a data controller under the EU GDPR is linked to the total worldwide turnover of the preceding financial year of the defaulting data controller.

[849] Under the IT Act, civil penalty provisions are limited to instances where any person fails to furnish any document, return or report, or fails to maintain books of accounts or records as may be prescribed (Section 44, IT Act). Moreover, there is a residuary penalty clause which is applicable to instances for which no separate penalty is prescribed and limits the amount of penalty leviable to a maximum of Rs.25,000 (Section 45, IT Act). It may be noted that the IT Act prescribes fines (along with imprisonment) for offences involving breach of privacy and confidentiality under Section 72 and disclosure without consent or in breach of lawful contract under Section 72A.

[850] Article 83(1), EU GDPR.

[851] Per Article 83(5), EU GDPR, this includes instances where the data controller or data processor has infringed the basic principles for processing (including conditions for consent), data subjects' rights, and transfer of personal data to a recipient in a third country or an international organization pursuant to Articles 44-49, EU GDPR. Similar administrative fine is also prescribed where the data controller or data processor does not comply with an order of the supervisory authority. Moreover, for certain other types of infringements, Article 83(4) of the EU GDPR prescribes an administrative fine of up to EUR 10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Given that only an upper limit is prescribed in relation to the quantum of administrative penalty that may be imposed on a data controller or data processor, the EU GDPR further stipulates the criteria that a supervisory authority may consider while determining the quantum of such administrative penalties. These factors include[852]:

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

(ii) the intentional or negligent character of the infringement;

(iii) any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects;

(iv) the degree of responsibility of the data controller or data processor taking into account the technical and organizational measures implemented by them; and

(v) any relevant previous infringement by the data controller or data processor.

It is pertinent to note that the obligations set out under the EU GDPR are also applicable where public authorities/government bodies are acting as data controllers or data processors. However, the EU GDPR mandates each Member State to lay down rules on whether and to what extent administrative fines may be imposed on such public authorities and bodies.[853]

United Kingdom

Under the UK DPA, the Information Commissioner has the power to impose monetary penalty up to the prescribed amount upon the data controller in case of a serious contravention of the data protection principles set out under the UK DPA.[854] The Information Commissioner must be satisfied that the contravention was of a kind likely to cause substantial damage or substantial distress, and either (i) the contravention was deliberate or (ii) the data controller knew or ought to have known that there was a risk that the contravention would occur and that such a contravention would be of a kind likely to cause substantial damage or substantial distress but failed to take reasonable steps to prevent the contravention.[855] The Information Commissioner is also required to take into account the

[852] Article 83(2), EU GDPR.
[853] Article 83(7), EU GDPR.
[854] Sections 55A-55E, UK DPA. The amount of the monetary penalty determined by the Information Commissioner cannot exceed GBP 500,000. The monetary penalty imposed must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others. *See* ICO, "Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998", 3 (December 2015), available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf, (last accessed 20 October 2017).
[855] Section 55A, UK DPA.

sector, size, financial and other resources of a data controller as the purpose of a monetary penalty is not to impose undue financial hardship on an otherwise responsible entity.[856]

Australia

As per the Privacy Act, the OAIC may apply to the prescribed court for an order that an entity which has infringed any provisions of the Privacy Act shall be liable to pay a pecuniary penalty.[857] If the court is satisfied that the entity has contravened certain provisions of the Privacy Act, then it may order the entity to pay a pecuniary penalty as it determines.[858]

South Africa

Under the POPI Act[859], an administrative fine not exceeding R10 million may be imposed on the defaulting organization. Moreover, while determining an appropriate fine, the Information Regulator may consider the following factors:

(i) nature of personal information involved;

(ii) duration and extent of contravention;

(iii) number of data subjects affected or potentially affected by such contravention;

(iv) likelihood of substantial distress or damage, including injury to feelings or anxiety suffered by data subjects;

(v) whether the responsible party could have prevented the contravention from occurring; and

(vi) failure to carry out risk assessment or a failure to operate good policies, procedures and practices to protect personal information.

4.3 Provisional Views

1. Based on a review of the extant Indian legal and regulatory framework as well as the international best practices set out above, the following models for calculation of civil penalties may be possible:

[856] ICO, "Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998", 3 (December 2015), available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf, (last accessed 20 October 2017).
[857] Section 80W, Part VIB, Privacy Act.
[858] From a reading of Section 80W(5), Privacy Act, it appears that the pecuniary penalty is capped at five times the amount stipulated for violation of a specific provision under the Privacy Act, in case of a body corporate and otherwise, it is the amount of pecuniary penalty contemplated for violation of a specific provision under the Privacy Act.
[859] Section 109, POPI Act.

(i) Per day basis

A data protection law may stipulate that for a violation of a data protection obligation, a civil penalty of a specific amount may be imposed on the data controller for each day such violation continues, which may or may not be subject to an upper limit.[860] An upper limit may be a fixed amount or may be linked to a variable parameter, such as, a percentage of the annual turnover of the defaulting data controller.

(ii) Discretion of adjudicating body subject to a fixed upper limit

A data protection law may stipulate that for a violation of a data protection obligation, an adjudicating authority may decide the quantum of civil penalty leviable subject always to a fixed upper limit as prescribed under applicable law. This model of penalty determination is common to the Indian context[861] and appears to be so from an international perspective as well.

(iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter

A data protection law may stipulate that for a violation of a data protection obligation, an adjudicating authority may decide the quantum of civil penalty leviable subject always to an upper limit which is linked to a variable parameter. There are instances in Indian law where such a standard has been adopted.[862] In the context of a data protection law, the EU GDPR adopts a similar standard and sets the upper limit of a civil penalty that may be imposed on a defaulting data controller as a percentage of the total worldwide turnover of the preceding financial year of the defaulting data controller.

2. In relation to the penalty models set out above, it may be relevant to note that while civil penalty leviable on a daily basis (i.e., model (i)) may act as a deterrent, it may lead

[860] In the Indian context, typically, per day civil penalty that may be leviable is capped to an upper limit. For instance, Section 91(2), Companies Act, 2013 provides that civil penalty for closure of register of members or debenture holders without prescribed notice is Rs. 5,000 for every day of such violation subject to a maximum of Rs. 1 lakh. Similarly, per Section 15C, SEBI Act, if any listed company or any registered intermediary fails to redress grievances of investors within the prescribed time, then such company or intermediary shall be liable to penalty which not be less than Rs. 1 lakh but which may extend to Rs. 1 lakh for each day during which such failure continues subject to a maximum of Rs. 1 crore. However, there are instances in the IT Act, such as, Section 44(b) (as cited above) which prescribes a per day civil penalty of Rs. 5,000 which is not capped.

[861] For instance, per Section 105, Insurance Act, 1938, if any director, managing director, manager or other officer or employee of an insurer wrongfully obtains possession of any property or wrongfully applies to any purposes of the said Act, then such person shall be liable to a penalty not exceeding Rs. 1 crore. Further, per Section 50, Food Safety and Standards Act, 2006, any person who sells to the purchaser's prejudice any food which is not in compliance with the provisions of the FSSA or of the nature, substance or quality demanded by the purchaser shall be liable to a penalty not exceeding Rs. 5 lakhs.

[862] For instance, per Section 15G, SEBI Act, the penalty for insider trading is provided as a minimum of Rs. 10 lakhs which may extend to Rs. 25 crores or three times the amounts of profit made out of insider trading, whichever is higher. Similarly, under Section 27, Competition Act, 2002, where after any enquiry, it is found that any agreement or action of an enterprise in a dominant position is in contravention of Sections 3 or 4, as the case may be, a penalty may be imposed which shall not be more than 10% of the average of the turnover for the last three preceding financial years upon each of such person or enterprise which are parties to such agreement or abuse.

to an overly adverse impact on small data controllers/ start-up entities who are in the process of setting up businesses or may be in their teething period. In such a case, a per day civil penalty may not be feasible and the quantum of penalty that may be imposed may be left to the discretion of an adjudicating body subject to an upper limit, where such an upper limit may be a fixed amount or may be linked to a variable parameter, such as, a percentage of the annual turnover of the defaulting data controller

3. Where models (ii) or (iii) are proposed to be adopted, it may leave sufficient room for discretion on the part of the adjudicating authority. Consequently, it may be necessary to set out the factors that an adjudicating authority may consider while determining the appropriate quantum of civil penalty that may be imposed. This may include, nature and extent of violation of the data protection obligation, nature of personal information involved, number of individuals affected, whether infringement was intentional or negligent, measures taken by data controller to mitigate the damage suffered and previous track record of the data controller in this regard.

4. To ensure that civil penalty imposed constitutes adequate deterrence, any of the above models or a combination thereof may be adopted. An upper limit of civil penalty which may be linked to the total worldwide turnover of the defaulting party, as is the case under the EU GDPR, brings within its ambit those data controllers which handle large volumes of personal data, or who have a high turnover due to their data processing operations, or whose operations involve the use of new technology for processing and therefore may have a higher likelihood of causing harms to individuals.

5. Consequently, the highest form of deterrence in relation to civil penalties may be where a per day civil penalty is imposed subject to a fixed upper limit or a percentage of the total worldwide turnover of the defaulting data controller of the previous financial year, whichever is higher.

4.4 Questions

1. What are your views on the above?

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

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

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

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

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

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

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

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

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

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

B. COMPENSATION

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

4.5 Issues

The IT Act, albeit in a limited manner, in Section 43A, recognizes the right of an individual to claim compensation in case of a failure to protect sensitive personal data. Section 43A of the IT Act specifically stipulates that where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates is negligent in implementing and maintaining reasonable security practices and procedures[863] and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.[864]

Moreover, while adjudging the quantum of compensation payable under the IT Act, the adjudicating officer shall have due regard to the following factors, namely:[865]

(i) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(ii) the amount of loss caused to any person as a result of the default; and

(iii) the repetitive nature of the default.

From a plain reading of the above, it follows that Section 43A of the IT Act is triggered in cases of negligence in maintaining and implementing reasonable security practices and procedures and that such negligence has caused a wrongful loss or wrongful gain[866] to any person.

---

[863] As per Section 43A, IT Act, 'reasonable security practices and procedures' may be specified in an agreement between the parties or may be specified under law or in the absence of such agreement or any law, such reasonable security practices and procedures as may be prescribed by the central government in consultation with such professional bodies or associations as it may deem fit.

[864] It is relevant to note that under Section 43, IT Act, if any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network accesses or secures access to such computer, computer system or computer network, downloads, copies or extracts any data or information from the same, or provides any assistance to any person to facilitate access to the same in contravention to the provisions of the IT Act shall be liable to pay damages by way of compensation to the person so affected.

[865] Section 47, IT Act.

[866] While there is no specific definition of the terms 'wrongful loss' or 'wrongful gain' under the IT Act, reliance may be placed on Section 23, IPC which states as follows:
"*"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled. "Wrongful loss".—"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.*"

Compensation as a remedy as stipulated under Section 43A of the IT Act appears to be rather limited in its nature and scope.[867] In this regard, it is relevant to note that first, this provision is applicable only where a body corporate[868] fails to maintain and implement reasonable security practices and procedures. Consequently, Section 43A of the IT Act does not appear to impose any liability to pay compensation on a government body/public authority in case of breach of data protection obligations by such entities.

Second, Section 43A of the IT Act appears to be applicable only when a body corporate has failed to maintain reasonable security practices and procedures as provided in an agreement between the parties concerned or as may be specified under any law for the time being in force, i.e., the SPDI Rules. It is unclear whether "reasonable security practices and procedures" referred to in Section 43A of the IT Act includes the various obligations under the SPDI Rules or only the security practices and procedures specified in Rule 8 of the SPDI Rules.[869] Concomitantly, even where one or more other obligations under the IT Act is breached but there is no gain or loss in financial terms, Section 43A of the IT Act would not be attracted.[870]

4.6 International Practices

European Union

Under the EU GDPR[871], an individual who has suffered "material or non-material" damage as a result of the infringement of the EU GDPR shall have the right to receive compensation from the data controller or data processor for the damage suffered. It has been specified that a data controller shall be liable for the damage caused by processing which infringes the EU GDPR and that a data processor shall only be liable where it has acted in violation of any obligation specifically applicable to data processors or has acted outside or contrary to any lawful instruction provided by the data controller. Further, court proceedings for exercising the right to receive compensation shall be brought before the competent courts in the Member States.

---

[867] The use of Section 43A, IT Act appears to be rather limited. A majority of the jurisprudence in this regard appears to stem from orders passed by adjudicating officer in Maharashtra where cases pertain to fraudulent transactions from bank accounts on account of failure to maintain reasonable security practices and compensation may range from Rs. 5,000 to Rs. 40 lakhs. *See* Sreenidhi Srinivasan and Namrata Mukherjee, 'Building An Effective Data Protection Regime', Vidhi Centre For Legal Policy 19 (January 2017) and *also see Chander Kalani & Anr. v. State Bank of India & Ors.*, Complaint No. 1 of 2014, Adjudicating Officer (Maharashtra) Order dated 12 January 2015, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudication_Chander%20Kalani_Vs_SBI_Ors-12012015.PDF, (last accessed 21 November 2017) and *Amit Dilip Patwardhan v. Bank of Baroda*, Complaint No. 15 of 2013, Adjudicating Officer (Maharashtra) Order dated 30 December 2013, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudicaton_AmitPatwardhan_Vs_BankOfBaroda-30122013.PDF, (last accessed 21 November 2017).

[868] Explanation (i) to Section 43A, IT Act defines "body corporate" as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

[869] Sreenidhi Srinivasan and Namrata Mukherjee, 'Building An Effective Data Protection Regime', Vidhi Centre For Legal Policy 19 (January 2017).

[870] Sreenidhi Srinivasan and Namrata Mukherjee, 'Building An Effective Data Protection Regime', Vidhi Centre For Legal Policy 19 (January 2017).

[871] Article 82, EU GDPR.

United Kingdom

As per the guidance[872] issued by the ICO, if an individual suffers damage where a data controller has breached the provisions of the UK DPA, the individual is entitled to claim compensation from the data controller. If an individual claims a certain amount as compensation, she will be required to demonstrate how the data controller's failure to comply with the UK DPA has resulted in her incurring that amount of damage or loss. This right can only be enforced through the courts. Moreover, a claim for compensation may be defended on the basis that the data controller took reasonable care in the circumstances to avoid breach. However, there are no guidelines on the level of compensation to be payable in this regard.

Australia

Under the Privacy Act, if the OAIC, upon investigation makes a finding of substantiated complaint that the organization has engaged in conduct that amounts to an interference with privacy, then the OAIC may, *inter alia*, declare that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice which forms the subject matter of the complaint.[873] Further, any loss or damage as referred above includes injury to the feelings of the individual and humiliation suffered by the individual.[874] However, a determination made by the OAIC above is not binding or conclusive between the parties to the determination and separate proceedings are required to be initiated by the individual or the OAIC to enforce the latter's determination.[875]

Canada

Under PIPEDA, the court (to which the complainant has applied for hearing in respect of any matter in respect of which complaint was made to the Privacy Commissioner) may, *inter alia*, award damages to the complainant including damages for any humiliation that the complainant has suffered.[876]

South Africa

Under the POPI Act, a data subject or on the request of the data subject, the Information Regulator may institute a civil action for damages in a court having jurisdiction against the responsible organization for breach of the provisions of the POPI Act, whether or not there was intent or negligence on the part of the responsible party. The court may award payment which is just and equitable, including payment of damages as compensation for patrimonial

[872] ICO, 'Compensation' available at https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/compensation/ (last accessed 20 October 2017).
[873] Section 52, Privacy Act.
[874] Section 52(1AB), Privacy Act.
[875] Section 52(IB), Privacy Act.
[876] Section 16(c), PIPEDA.

and non-patrimonial loss suffered by the data subject, aggravated damages, interest and cost of suit on such scale as may be determined by the court.[877]

4.7 Provisional Views

1. An individual may be given the right to seek compensation from a data controller in case she has suffered any loss or damage due to a violation of the data controller's obligations under a data protection legal framework.

2. A claim for compensation may be filed in accordance with the provisions set out in the previous chapter on 'Adjudication Process' (Part IV, Chapter 3 of the White Paper).

3. It may be considered whether an obligation should be cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to violation of data protection rules by such data controller (without the individual taking recourse to the adjudicatory mechanism).

4.8 Questions

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

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

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

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

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

[877] Section 99, POPI Act.

C. OFFENCES

There are certain types of breaches of data protection obligations, which, by their very nature and the impact they create, are extremely serious and may cause significant harm to individuals. In these instances, it may be imperative to prescribe criminal sanctions in the form of punishment and severe fines on the data controller.

4.9 Issues

The IT Act deals extensively with several types of offences or cybercrimes and prescribes penalty in the form of fines or imprisonment or both.[878] Specifically in the context of data protection, Sections 72[879] and 72A[880] of the IT Act offer some redress. Section 72 of the IT Act is limited in scope as it prescribes a penalty only against those persons who have been given the power under the IT Act or the rules and regulations made thereunder to access any electronic resource. As such, it may be limited to functionaries who have been granted specific powers under the provisions of the IT Act.[881] Section 72A of the IT Act is broader in scope as it imposes a penalty on any person, whether a private or public entity, for the disclosure of personal information without the consent of the person concerned. However, Section 72A of the IT Act is triggered only in those instances where the person (who has disclosed the personal information) has secured access to such personal information while providing services under the terms of a lawful contract.

Rapid growth of technological advancements which may be utilised towards processing of personal information increases the risk of data protection violations. Consequently, provisions in a data protection legal framework may be required to carefully set out criminal liability in cases of data protection violation. Moreover, criminal sanction in the form of imprisonment and fines may be prescribed to ensure that it adversely affects the data controller financially and reputationally thereby serving some deterrent value.

---

[878] This includes Section 65 (tampering with computer source documents), Section 66 (computer related offences), Section 66B (punishment for dishonestly receiving stolen computer resource or communication device), Section 66C (punishment for identity theft), Section 66D (punishment for cheating by personation by using computer resource), Section 66E (punishment for violation of privacy), Section 66F (punishment for cyber terrorism) and Section 67 (punishment for publishing or transmitting obscene material in electronic form).

[879] Section 72, IT Act provides as follows:

"*Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*"

[880] Section 72A, IT Act provides as follows:

"*Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.*"

[881] Apar Gupta, Commentary on Information Technology Act, 269 (Lexis Nexis, 2013).

4.10 International Practices

European Union

Under the EU GDPR, it appears that Member States shall have the discretion to decide rules in relation to criminal sanctions for infringements of the EU GDPR.[882]

United Kingdom

The UK DPA makes it an offence for a person who either knowingly or recklessly without the consent of the data controller obtains or discloses personal data or the information contained in the personal data, or procures the disclosure to another person of the information contained in the personal data.[883]

Australia

Under the Privacy Act, a person commits an offence if personal information (that relates to another individual) is disclosed to her and such person subsequently discloses the personal information.[884]

Canada

Under PIPEDA[885], every person who knowingly contravenes, *inter alia*, Section 8(8)[886] of the PIPEDA is guilty of an offence punishable on summary conviction and liable to a fine not exceeding CAD10,000, or an indictable offence and liable to a fine not exceeding CAD100,000.

South Africa

Under the POPI Act, fine or imprisonment (for a period not exceeding 10 years) or both for certain types of offences[887] and fine or imprisonment (for a period not exceeding 12 months) or both for certain other types of violations[888] of the POPI Act has been prescribed.[889]

---

[882] Lucy Lyons, 'Enforcement and sanctions under the GDPR', Taylor Wessing (April 2016) available at: https://www.taylorwessing.com/globaldatahub/article-enforcement-sanctions-under-gdpr.html, (last accessed 20 October 2017). Please note that as per Article 84, EU GDPR, Member States may lay down rules on other penalties applicable to infringements of the EU GDPR, especially those infringements, which are not subject to administrative fines.

[883] Section 55, UK DPA. Per Section 60 of the UK DPA, a fine capped at a particular amount is prescribed as penalty.

[884] Section 80Q, Privacy Act. The penalty is 60 penalty units or imprisonment for one year or both.

[885] Section 28, PIPEDA.

[886] Per Section 8(8), PIPEDA, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under the PIPEDA that she may have.

[887] For instance, for failure to comply with any enforcement notices (Section 103, POPI Act) or obstructing the functioning of the Information Regulator (Section 100, POPI Act).

4.11 Provisional Views

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

2. The quantum of penalty and term of imprisonment prescribed may be enhanced as compared to the provisions of the IT Act.

3. A more stringent penalty may be prescribed where the data involved is sensitive personal data.

4. The power to investigate such an offence may lie with a police officer not below the rank of Inspector.[890]

4.12 Questions

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

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

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

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

5. Who will investigate such offences?

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

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

---

[888] For instance, per Section 54, POPI Act, any person acting on behalf of or under the direction of the Information Regulator must treat as confidential the personal information which comes to his or her knowledge in the course of performing her official duties.
[889] Section 107, POPI Act.
[890] As reflected in Section 78, IT Act.