White Paper on Data Protection framework for India

Table of contents

The 21st century has witnessed such an explosive rise in the number of ways in which we use information, that it is widely referred to as 'the information age'. It is believed that by 2020, the global volume of digital data we create is expected to reach 44 zettabytes. Much of that new information will consist of personal details relating to individuals, including information relating to the products they have purchased, the places they have travelled to and data which is produced from 'smart devices' connected to the Internet.

There are a large number of benefits to be gained by collecting and analysing personal data from individuals. Both the public and the private sector are collecting and using personal data at an unprecedented scale and for multifarious purposes. While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of an individual. This was also the subject matter of the landmark judgement of the Supreme Court in Puttaswamy, which recognised the right to privacy as a fundamental right. In this light, in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a data protection law is the need of the hour for India.

Government of India has constituted a Committee of Experts under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna to study various issues relating to data protection in India and make specific suggestions on principles to be considered for data protection in India and suggest a draft Data Protection Bill. The objective is to “ensure growth of the digital economy while keeping personal data of citizens secure and protected.” A White Paper has been drafted to solicit public comments on what shape a data protection law must take.

Overview of the White paper

The White Paper outlines the issues that a majority of the members of the Committee feel require incorporation in a law, relevant experiences from other countries and concerns regarding their incorporation, certain provisional views based on an evaluation of the issues vis-à-vis the objectives of the exercise, and specific questions for the public.

Summary - Key Principles of a Data Protection Law

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

1. Technology agnosticism - The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance.
2. Holistic application - The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims.
3. Informed consent - Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria.
4. Data minimisation - Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.
5. Controller accountability - The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing.
6. Structured enforcement - Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms.
7. Deterrent penalties - Penalties on wrongful processing must be adequate to ensure deterrence.

Scope And Exemptions - Provisional views

1. **Territorial And Personal Scope**
    - The primary test for applicability of law may be processing of personal information which takes place in the territory of India by entities which have a presence in India. The term processing involves any action with respect to data including collection, use or disclosure of data. The clause would then cover individuals in India, companies and other juristic entities which have an establishment in India which process data.
    - However, it may be necessary to make the law applicable to all kinds of processing which the State may have a legitimate interest in regulating even though such processing may not be entirely based in India or may be carried out by non- Indian

entities that do not have a presence in India.

- Carrying on a business, or offering of services or goods in India are parameters worth incorporating in the law in light of international practices. Thus, an entity which does not have a presence in India but offers a good or service to Indian residents over the Internet, or carries on business in India may be covered under the law.
- It may also be worthwhile considering making the law applicable to any entity, no matter where they may be located that process personal data of Indian citizens or residents. This partially adopts the new EU GDPR formulation and puts the data subject squarely at the centre of the legislation, ensuring that the law is made applicable to anyone who would processes personal data of the data subject.
- The extent of jurisdiction may not be so wide as to constitute an unnecessary interference with the jurisdiction of other states or have the effect of making the law a general law of the Internet. For instance, the mere fact that a website (operated from abroad) is accessible from India should not be a reason for subjecting the website to Indian law.

2. **Other Issues of Scope**
   - Given prevalent best practices, the law may apply to natural persons only. The primary object of the legislation being to protect the informational privacy right of an individual, the proposed law may not be extended to include data relating to companies and other juristic entities.
   - The law may apply to data about natural persons processed both by public and private entities. However, limited exemptions may be considered for well defined categories of public or private sector entities.
   - The law may have a transitory provision to address the issue of retrospective application.
3. **What is personal data?**
   - It is data about/relating to an individual that may be the subject matter of protection under the law. Data in this context ought to include any kind of information including opinions or assessments irrespective of their accuracy.
   - Data from which an individual is identified or identifiable/reasonably identifiable may be considered to be personal data. The identifiability can be direct or indirect.
   - New technologies pose considerable challenges to this distinction based on identifiability. This standard may have to be backed up by codes of practice and guidance notes indicating the boundaries of persona l information having regard to the state of technology.
4. **Sensitive personal data**
   - Health information, genetic information, religious beliefs and affiliations, sexual orientation, racial and ethnic origin may be treated as sensitive personal data. Caste information may also be treated as sensitive personal data.
   - Though qualitatively different from the information in the previous category, financial information may also be included as sensitive personal data. Financial information has been categorised as sensitive information in India since the formulation of SPDI Rules.
   - In other categories such as philosophical or political beliefs, an assessment may be

made whether these are matters in which a person has an expectation of a high degree of privacy

5. **What is Processing?**
    - The data protection law may not attempt to exhaustively list all operations that constitute processing.
    - The definition of processing may be broadly worded to include existing operations while leaving room to incorporate new operations by way of interpretation.
    - The definition may list the three main operations of processing i.e. collection, use and disclosure of data. It may be worded such that it covers the operations/activities incidental to these operations.
    - The law should cover both automated and m anual processing.
6. **Entities to be defined in the law: Data Controller and Processor**
    - To ensure accountability, the law may use the concept of ' data controller'. The competence to determine the purpose and means of processing may be the test for determining who is a 'data controller'.
    - The need to define data processors, third parties or recipients depends on the level of detail with which the law must allocate responsibility. This has to be determined on an assessment of the likely impact of imposing obligations on processors and the compliance costs involved, amongst other things.
7. **Exemptions for Household purposes, journalistic and literary purposes and research**
    - A wide exemption may be provided for data processed for household purposes.
    - A wide exemption may be provided for data processed for journalistic/artistic and literary purposes. However, the requirement to have adequate security and organisational measures for protecting data against unauthorised access should be applicable.
    - An exemption may be provided for data processed for the purpose of academic research, statistics and historical purposes. However, adequate safeguards may be incorporated in law to ensure that the data is being used for a bonafide purpose, and has been lawfully obtained. The law must provide for adequate security and organizational safeguards in the handling of such data.
    - The law may provide exemptions for the following purposes/processing activities: (i) information collected for the purpose of investigation of a crime, and apprehension o r prosecution of offenders; (ii) information collected for the purpose of maintaining national security and public order.
    - The exemptions must be defined in a manner to ensure that processing of data under the exemptions is do ne only for the stated purpose. Further, it must be demonstrable that the data was necessary for the stated purpose.
    - In order to ensure that the exemptions are reasonable and not granted arbitrarily, an effective review mechanism must be devised.
8. **Cross-Border Flow of Data**

There are two tests identified for formation of laws related to cross border data flow, namely the adequacy test and the comparable level of protection test for personal data. In order to implement the adequacy test, there needs to be clarity as to which countries provide for an adequate level of protection for

personal data. The data protection authority should be given the power to determine this. The adequacy test is particularly beneficial because it will ensure a smooth two-way flow of information, critical to a digital economy. In the absence of such an adequacy certification, the onus would be on the data-controller to ensure that the transfer is subject to adequate safeguards and that the data will continue to be subject to the same level of protection as in India. However, an adequacy framework would require a proactive data protection authority that needs to actively monitor the developments of law and practice around the world.

9. **Data Localisation**

From these practices it emerges that certain countries have embraced data localisation in some form or manner. However, most countries, do not have a data localisation mandate. India will have to carefully balance the enforcement benefits of data localisation with the costs involved pursuant to such requirement. Different types of data will have to be treated differently, given their significance for enforcement and industry. It appears that a one-size-fits-all model may not be the most appropriate. Thus while data localisation may be considered in certain sensitive sectors, it may not be advisable to prescribe it across the board

Grounds of Processing, Obligation on Entities and Individual Rights - Provisional views

1. **Consent**
    - The importance of consent in data protection law is widely recognised. Keeping in mind the importance of consent, it is proposed that consent of individuals should be one of the grounds for collection and use of personal data. However, at the same time is it recognised that consent is being used as a means to disclaim liability. In the context of data collected and processed by the government, the individual often has no choice but to provide her data. Thus the validity of consent will have to be carefully determined.
    - In order for the consent to be valid, it should be freely given, informed and specific to the processing of personal data by way of a well - designed notice.
    - All transactions may not warrant the same standards of consent. Therefore, there may be a need to explore and accommodate standards of consent within the data protection law and align it with different types of information. Additionally, the standards for implied consent may need to be evolved in order to ensure that adequate information is provided to the individual giving her consent.
2. **Child's Consent**
    - From studies relating to Internet use among children, it has been observed that

children are generally recognised as a vulnerable group, and merit a higher standard of protection due to their relatively limited ability to adequately assess online privacy risks and consequently manage their privacy.

- One solution to this could be to seek parental authorisation or consent when data controllers process personal data relating to children. This may also be a solution to the conundrum that children do not have the capacity to enter into a valid contract. Many jurisdictions recognise that solely relying on parents ' consent would have a chilling effect on the use of the Internet by children. Therefore, these jurisdictions have created an age-limit, below which a parent's consent is necessary, in order to protect very young children from privacy harms. Similarly, a variable age limit can be drawn (not necessarily 18 - which is the generally accepted age of majority in India) below which parental consent is to be mandatory. Methods for effectively ensuring parental consent must be considered, either for certain categories of services or through certain processes that may be onerous for the child to circumvent.
- In addition, or in the alternative, perhaps distinct provisions could be carved out within the data protection law, which prohibit the processing of children's personal data for potentially harmful purposes, such as profiling, marketing and tracking. Additionally separate rules could be established for the manner in which schools and other educational institutions that collect personal information about children as part of their regular activities need to collect and process this data. Similarly, regulations should be prescribed as to the manner in which the government collects and processes data about children.

3. **Notice**
    - Mandatory notice is a popular form of privacy self - management, which plays a role in most data protection laws. Notice is important as it operationalises consent.
    - The law may contain requirements regarding the form and substance of the notice.
    - The data protection authority could play an important role by issuing guidelines and codes of practice that could provide guidance to organisations on the best way to design notices, so that it conveys relevant information in the most effective manner to individual s. This may include giving advice on how to redesign notices, making them multi - layered and context specific, informing them of the importance that timing plays while providing notices, etc. This may be further bolstered by sectoral regulators as well.
    - Privacy Impact Assessment or other enforcement tools may take into account the effectiveness of notice s issued by organisations.
    - In order to address issues relating to notice fatigue, assigning every organisation may be assigned a 'data trust score' (similar to a credit score), based on their data use policy.
    - Similarly, having a 'consent dashboard' could help individuals easily view which organisations have been provided with consent to process personal information and how that information has been used.
4. **Other grounds of processing**
    - Consent continues to play a very important role in data processing activities. It may not be possible to seek consent of the individual, prior to collection and use of her information in all circumstances, particularly when information is used for various

purposes for which they might not have been originally intended. There may be a need to have certain legally recognised grounds to permit processing of personal data in these circumstances.

- Grounds such as performance of contract; and necessity for compliance with law appear to be intuitively necessary, and have been adopted, as is, by jurisdictions.
- Other grounds such as the public interest ground finds mention within the EU GDPR; however lack of specificity as to what it comprises, has led to countries such as the UK to modify it to fit the particular administrative, judicial and legislative requirements of each country. For instance, other grounds of processing could include collection of information in the event that it has been ordered by a court of law; where a public authority needs to collect data necessary to the exercise of the functions of the legislature, such as the drafting of new laws. Adaptations suitable for India will have to be explored.
- There may also be a need of a ground which permits the collection of information in situations of emergency where it may not be possible to seek con sent from the affected individual.
- The 'legitimate interest' ground under the EU GDPR appears to be subjective and difficult to enforce. It places a heavy burden on the data controller who must carry out the balancing test weighing its interests against that of the rights of the individual. Despite this, there may be a need to have a residuary ground under which processing activities could take place, as it is not possible for the law to foresee and provide for all situations, which may warrant the processing of information without seeking consent of the individual. This residuary ground would be intended for the benefit of the individual. As an alternative, the data protection authority could designate certain activities as lawful, and provide guidelines for the use of these grounds and the data controller would be permitted to collect information under these grounds.

5. **Purpose Specification and use limitation**
    - The current regime of purpose specification and use limitation is designed to ensure that individuals retain control over the manner in which their personal data is collected, used and disclosed. This is a valuable objective.
    - Standards may have to be developed to provide guidance to data controllers about the meaning of data minimisation in the context of their data collection and use.
    - In light of recent developments in data flow practices and new technologies, data may be multi - functional and being required to specify each use in an exact manner within a privacy notice may prove to be burdensome. Using layered privacy notices, which provide hyperlinks to more information on data use practices, which can be accessed as required, could mitigate this situation. Further, incompatible purposes, irrespective of how beneficial they may be to the user may not be permitted for further processing.
    - The use limitation principle may need to be modified on the basis of a contextual understanding of purposes and uses. This is captured by the reasonableness standard, i.e. a subsequent use is permitted as long as a reasonable individual could reasonably expect such use. This may be further developed by sectoral regulators.
6. **Processing of personal sensitive data**

- It is recognised that the processing of certain types of personal data has a greater likelihood of causing harm to the individual, due to the inherent nature of the information.
- The existing categories of information defined as 'sensitive' under the SPDI Rules may be re-examined to determine whether those categories are sufficient or need to be modified. These categories need to be examined keeping in mind India ' s unique socio-economic context, where individuals have faced discrimination and harm due to various reasons currently not captured in the definition.
- There may be a need to provide heightened grounds of protection for the processing of such types of data.

7. **Storage Limitation and data quality**
    - Storage Limitation: The principle of storage limitation is reflected in most data protection laws and may consequently also find place in a data protection law for India. Further, it may not be feasible to prescribe precise time limits for storage of data since the purpose of processing will determine the same. However, the use of terms 'reasonably necessary/necessary' may be employed and thereafter guidelines issued by the regulator, industry practices, interpretation by courts can bring clarity when it comes to implementation.
    - Data Quality: The principle of data quality is reflected in most data protection laws and consequently may be incorporated in a data protection law. Further, such a provision ought to achieve a balance between the burden imposed on industry and the requirement for accuracy. Again, the employment of terms 'reasonably necessary' may be employed to achieve this purpose.
8. **Individual participation rights**

Right to Confirmation, Right to Access, and Right to Rectification

- The right to seek confirmation, access and rectify personal data allow an individual control over data once such data has been collected by another entity. These rights may be suitably incorporated. However these rights are harder to enforce in the context of personal information that has been derived from the habits and observed behaviour of the individual and other such inferred insights . This information is nevertheless personal and an individual should be made aware of the fact that the data controller has this sort of information.
- Given that responding to individual participation rights can be costly for organisations, and comes with its set of technical challenges, a reasonable fee may be imposed on individuals when exercising these rights. This will also discourage frivolous and vexatious requests. The fees may be determined via sector specific subsidiary legislation or regulations. An illustration of this is the CIC Act under which the charge for accessing a copy of a person's credit information report by a specified user is laid down by the RBI via regulations.
- Reasonable exceptions to the right to access and rectification exist in all jurisdictions. Such exceptions must also be carved out to ensure that organisations are not overburdened by requests which are not feasible to respond to.

Right to Object to Processing, Right to Object to processing for purpose of

Right to Object to Processing, Right to Object to processing for purpose of Direct Marketing, Right to not be subject to a decision based solely on automated processing, Right to Data Portability, and, Right to restrict processing.

- It is important to include concepts of data portability into Indian privacy jurisprudence in order to ensure that the data subject is placed in a central position and has full power over her own personal data. Accordingly, every individual should have the rig ht to demand that all personal data about that individual that is in the control of the data controller be made available to her in a universally machine readable format or ported to another service provide with the specific consent of that individual. All data must therefore be held in an interoperable format.
- A general right to object to processing may not prove to be suitable for India. This is because, as explained in the section on other grounds of processing in this note, public interest and legitimate interest may not be imported as grounds for processing in a data protection law for India.
- Automated decisions have proven to have detrimental consequences in many cases. This right is also found across most EU data protection regimes. However, given the concerns raised about automated decisions and their pervasiveness in the digital economy, a practically enforceable and effective right may be carved out.
- Processing of personal data for direct marketing purposes may be recognised as a discrete privacy principle in a data protection law for India. This is because despite there being independent legislations regulating direct marketing, direct marketing is medium and technology - agnostic and consequently needs to be governed by general rules.

Right to be forgotten

- The right to be forgotten may be incorporated within the data protection framework for India as has been adverted to by the Supreme Court in Puttaswamy. Further, international practices in the EU GDPR and Canada also envisage a right to be forgotten in some form or manner thus strengthening the case for its incorporation.
- The right to be forgotten should be designed in such a manner that it adequately balances the right to freedom of speech and expression with the right to privacy. The scope and contours of such a right may be determined in accordance with the capabilities of the data controllers to undertake the balancing exercise and determine the legitimacy of the request. Further, clear parameters on the basis of which a controller will carry out the balancing exercise may be incorporated in the law to enable them to effectively carry out this exercise. A residuary role for a sector regulator to develop particular guidelines for each sector may become necessary.

Regulation and enforcement - Provisional views

1. **Enforcement models**

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.

2. **Accountability and enforcement tools**
    - Accountability, as a principle of data protection, h as 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.
    - It may be important to incorporate and make provision for codes of practice within a data protection framework.
    - Such codes of conduct or practices may be issued by a data protection authority after appropriate consultations with the industry and individuals.
    - 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.

Personal data breach notification

- 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.
- The law may also require that the data protection authority or any authority be notified immediately on detention of data breaches.
- 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.
- The data protection authority may issue codes of practice which prescribe the formats for such notification.

Categorisation of Data controllers

- The effective enforcement of a data protection law may require some form of differentiated obligations s o 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.
- The following additional obligations mentioned below may find place within the mechanism as appropriate:

mechanism as appropriate.

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

Data Protection Authority

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. **Adjudication process**
   - 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.
   - 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.
   - 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

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.

- 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. 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.
- In addition to the powers described in the previous section on 'Data Protection Authority', the data protection authority may be given the power to impose civil penalties as well as order the defaulting party to pay compensation.
- Specifically, in case of compensation cl aims, 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.
- 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.

4. **Remedies**

Penalties

- 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:
    - *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.

- *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.
- *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 ad opted. 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.

- 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 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
- 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.
- 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.

Compensation

- 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.
- A claim for compensation may be filed in accordance with the provisions set out in the previous chapter on ' Adjudication Process'.
- 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).

Offences

- 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.
- The quantum of penalty and term of imprisonment prescribed may be enhanced as compared to the provisions of the IT Act.
- A more stringent penalty may be prescribed where the data involved is sensitive personal data.
- The power to investigate such an offence may lie with a police officer not below the rank of Inspector

To access the complete document, click here.

Source : MeitY
