Bill No. __ of 2018

THE DATA PROTECTION BILL, 2018[1]

A Bill to establish rights of individuals vis-a-vis their personal data and to codify the law governing personal data including collection, use, storage, sharing, processing and disclosure of personal data by all entities:

to create an ecosystem to enhance the flow of data for the sustained growth of the digital economy;

to advance human rights, promote economic mobility and economic growth by giving individuals more control over their personal data and protecting the informational privacy of individuals and preventing potential harms and misuse of any individuals' personal data, and

to align Indian data protection laws with international standards, allowing India to retain and strengthen its competitiveness in the international market.

BE it enacted by Parliament in the Sixty-Eighth Year of the Republic of India as follows:

CHAPTER I

Preliminary

1. (1) This Act may be called the Data Protection Act, 2018.

[1] This is a working document to holistically represent the different aspects of our vision at Dvara Research for protecting personal data in India. It attempts to bind together ideas on various elements of data protection like definitions, standards, rights, obligations, remedies etc. to present an integrated approach. We recognise our limitations in legislative form and drafting, and welcome feedback and comments on this as a learning document to refine our thinking. Comments welcome at Communications.Research@dvara.com.

(2) It shall extend to the whole of India, and as provided in this Act, to any offence or contravention of the provisions of this Act committed outside India by any entity.

(3) It shall come into force on such date as the Central Government may, by notification in the official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provisions to the commencement of this Act shall be construed as a reference to the commencement of that provision.

2. In this Act, unless the context otherwise requires,

(a) "automated decision-making" is the ability to make or assist in making decisions by technological means;

(b) "bench" refers to each bench established pursuant to section 23(6)(f) of this Act;

(c) "breach" means unauthorised access, destruction, use, processing, storage, modification, re-identification, unauthorised disclosure (either accidental, incidental or unlawful) or other reasonably foreseeable risks or data security breaches pertaining to personal data transmitted, stored or otherwise processed;

(d) "complaints database" means the database established pursuant to section 23(7) of this Act;

(e) "consent" means the specific, informed and unambiguous acceptance by an individual, who is not under any duress or undue influence of any entity or third party at the time of such acceptance, through clear, affirmative action signifying agreement of the individual to the collection of personal data relating to him or her;

Provided that in the case of an individual who is known or could reasonably be believed to be under 13 years old, it shall refer to the consent of the individual with parental responsibility over the individual whose personal data is sought;

(f) "data controller" means the natural or legal person which, alone or jointly with others, (1) determines the purposes and means of the processing of personal data or (2) collects personal data from an individual prior to or during the performance or provision of a service or product, or when entering into a contract;

(g) "data processor" means a natural or legal person which processes personal data on behalf of the data controller;

(h) "Data Protection Authority" or "Authority" refers to the authority established pursuant to section 22 of this Act;

(i) "de-identified Information" is information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual;

(j) "enforcement action" means any action taken by the Data Protection Authority to ensure adherence to the provisions of this Act, including the actions specified in section 23(4)(c) of this Act;

(k) "entity" is a data controller or data processor, and includes

   i. any body corporate incorporated under any law for the time being in force in India; or

   ii. a foreign company within the meaning of section 2(42) of Companies Act, 2013 (No. 18 of 2013);

(l) "Government" means, save as otherwise provided in this Act, the Central Government and any State Government or State Governments.

(m) "harm" is actual or potential injury or loss to an individual, whether such injury or loss is economic or non-economic, quantifiable or non-quantifiable;

(n) "identifiable natural person" is the natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(o) "individual" means any identifiable natural person in India who is the subject of personal data;

(p) "judicial authority" is the authority established pursuant to section 23(6)(f) of this Act;

(q) "legitimate purpose" means, with respect to personal data of an individual, the legal, necessary, proportionate and fair use, disclosure and retention of personal data which is:

   i. limited to what is necessary for performance of a service or provision of a product or at a stage immediately prior to performing the service

or providing a product , and where no less intrusive means are available; or

ii. required in furtherance of a legal obligation; or

iii. necessary for administration of justice pursuant to a court order; or

iv. required for performance of any statutory, governmental or other functions by data processor or data controller as duly specified to the individual subject to data collection; or

v. necessary to protect the vital interests of the individual or of another individual, particularly where the individual is a child, including but not limited to the case of an individual's medical emergency which is fatal or may likely lead to permanent or irreversible bodily harm; or

vi. necessary for the third party to whom data is disclosed after it is duly informed to the individual, provided that the interests of data processors or data controller or third parties shall be adequately balanced against any prejudicial effect of the same on the rights and freedoms of the individual as guaranteed under this Act:

Provided that the interests of data processors or data controllers or third parties do not override the interests, rights and freedoms of the individual as provided under the Constitution of India;

(r) "national identifier" means any form of national identification issued by the Government including an identification number issued to an individual under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (No. 18 of 2016), identification documents or numbers issued under the Passport Act 1967 (No. 15 of 1967), the Representation of People Act, 1950 (No. 43 OF 1951), the Income Tax Act, 1961 (No. 43 of 1961), the Citizenship Act, 1955 (No. 57 of 1955), the Registration of Births and Deaths Act, 1969 (No. 18 of 1969) or any other Act or Scheme of the Government;

(s) "personal data" means any information that relates to an individual which, either directly or indirectly, including in combination with other information available or likely to be available, is capable of identifying such individual;

(t) "privacy notice" means the notice given in accordance with section 15(2) of this Act;

(u) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, analysis, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(v) "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(w) "protected characteristics" include race, gender, ethnic origin, political or religious beliefs, place of birth, caste or indicators when used to identify caste, marital status, age, genetic or health status, sexual orientation and any other characteristics as may be incorporated or defined from time to time by the Government;

(x) "sensitive personal data" includes such personal data which consists of information relating to or which serves to reveal —

i. racial or ethnic origins, political or religious views;

ii. passwords;

iii. financial information such as bank account or credit card or debit card or other payment instrument details or financial transactions records or other information that would permit access to an account;

iv. physical, physiological and mental health condition;

v. sexual activity;

vi. medical records and history;

vii. biometric data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification including, but not limited to, facial images, genetic information, fingerprints, handprints, footprints, iris recognition, handwriting, typing dynamics, gait analysis and speech recognition;

viii. any details relating to clauses (i) to (vii) above as provided to body corporates for providing service; and

ix. any of the information received or collected under clauses (i) to (vii) above by body corporates for processing, stored or processed under lawful contract or otherwise;

(y) "systemically important data entities" means entities categorised pursuant to section 23(4) of this Act;

(z) "third party" means a natural or legal person other than the individual, data controller, data processor and natural or legal persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

3. This Act shall apply to

(a) all data processing activity, including collection, use, storage, sharing and disclosure of personal data of all individuals through wholly or partially automated or manual methods;

(b) all entities as defined herein, and such body corporate, incorporated by any Act for the time being in force, as the Central Government may, by notification, specify in this behalf, subject to such exceptions, modifications or adaptation, as may be specified in the notification.

4. This Act shall not apply to

(a) reasonable safeguards for sovereignty or integrity of India, national security and for the defence of country;

(b) investigation of cognisable and non-bailable offences under the Indian Penal Code, 1860 (No. 45 of 1860) after a report has been duly filed under section 154 of the Criminal Procedure Code, 1973 (No. 2 of 1974);

(c) investigation of any other offences under the Indian Penal Code, 1860 (No. 45 of 1860), or any other Act for the time being in force;

(d) maintenance of public order in situations of imminent danger of breakdown; and

(e) personal data used for purely personal or household reasons, journalistic, artistic or literary purposes, or of a deceased individual or to any de-identified information.

save that, the provisions of section 18 shall apply to all entities involved in the activities mentioned in this section 4 and **provided that** the exemption in this section

4 must be, reasonable and proportionate, not excessive in nature but satisfy necessary and legitimate purposes, and must be imposed in the manner prescribed.

Chapter II

Individual Privacy Rights and Protections

5. Individual Rights and Protections

(1) No entity shall collect, store, process, share, disclose or otherwise handle any personal data, intercept any communication of another individual or carry out surveillance of any individual except in accordance with the provisions of this Act and all applicable laws.

6. Rights at Collection and Rights relating to Consent

(1) For the collection of personal data, consent must be obtained from the individual pursuant to the notice under section 15 of this Act and consistent with such notice.

(2) Where the purpose of processing of personal data is modified in any material manner, additional data collection or the processing of any personal data previously collected for a different purpose which is in variance with the initial purpose shall not be done without the prior consent of the individual.

(3) Any entity requesting consent must do so in close proximity to the time of the collection of the personal data, in a manner that is accessible clear, and conspicuous and prominent considering the context in which it is obtained, using clear and plain language taking into account the level of understanding and communications skills of the individuals whose consent is sought.

(4) Consent, not limited to sub-section (2), shall not be the basis for overriding or reducing protections and limitations, including on using, storing, processing, sharing, disclosure or other handling of personal data, in this Act or any other applicable law.

(5) Notwithstanding the above, consent may be overridden in cases where there is a legal obligation or medical emergency which is fatal or may likely lead to permanent or irreversible bodily harm, provided that any consent may only be overridden to the extent necessary and, where practicable, the individual so affected shall be informed of the same.

(6) Entities shall not condition access to services on providing consent unless the personal data is necessary for the provision of services. At any time, an individual shall be entitled to revoke consent and have all personal data collected by the entity returned and deleted, except as otherwise required by law. It shall be as easy to revoke consent as it is to give it.

(7) Collection of personal data shall only be for legitimate purposes and only the minimum information necessary for such purposes shall be collected.

(8) With regard to national identifiers,

(a) individuals shall not be denied any right, benefit, or privilege because of such individuals' refusal to disclose their national identifier unless necessary for legitimate purposes or otherwise required by law;

(b) any entity requesting disclosure of a national identifier shall inform that individual whether:

i. such disclosure is mandatory or voluntary

ii. the nature of information that may be shared;

iii. the uses to which the information received may be put by the requesting entity; and

iv. alternatives to submission of the particular national identifier information in question to the requesting entity,

(c) such entities shall maintain records of the disclosures sought which may be communicated to the relevant authority issuing the national identifier as required under the law,

(d) any entity that collects national identifiers shall be prohibited from using such National Identifier in a manner that provides access to that national identifier by the public, including but not limited to publicly displaying or printing the national identifier on any card used to access products or services provided by the individual.

7. Rights relating to Processing for Legitimate Purposes

(1) Processing of personal data is only permitted to the extent of the legitimate purposes for which the information was collected as stated in the notice provided.

(2) At any time, upon notice from the subject of the personal data, or their

representative, entities must cease contacting the individual for solicitation or marketing purposes.

(3) Any additional or further processing of personal data for archival or scientific or historical or statistical research, shall be considered compatible with the initial purpose if it is,—

(a) bona fide;

(b) in public interest; and

(c) subject to adequate safeguards.

8. Sharing and Access to Personal Data

(1) Data controllers may share information with other data controllers whose security procedures and privacy policies are no less rigorous and only if consistent with the legitimate purposes for which such information was collected.

(2) Data controllers may share information with data processors in support of the legitimate purposes for which the information was collected only if the data processor agrees to maintain security procedures and privacy policies no less rigorous than those employed by the data controller.

(3) If an entity receives a request from a statutory authority for access to personal data, where practicable and if not prohibited by law, the entity shall promptly notify the individual who is the subject of the information to provide that individual with the opportunity to object to disclosure of personal data to the Government or statutory authority or sharing of personal data with the Government or statutory authority.

(4) If an entity receives a request for access to personal data from a statutory authority, the entity may provide such access if:

(a) required by law or court order; or

(b) in cases of imminent threats to health and safety.

(5) An entity may transfer personal data to a successor entity in the same line of business if individuals are provided advance notice of the transfer and the option to have their personal data collected by the entity returned and deleted prior to the transfer.

(6) Data controllers and data processors shall not disclose personal data to any third party other than as provided in sections 10 of this Act.

9. Rights to Access and Quality of Personal Data

(1) Every individual shall have the right to seek access to personal data from such individual or generated by or associated with that individual's personal data, which is collected, processed, used or stored by an entity, and such access will be provided:

(a) upon proper identification;

(b) within a reasonable time not to exceed ten business days;

(c) at no charge or a nominal charge;

(d) in a reasonable manner, and through a clear user interface that allows them to make informed choices about who sees their data, how it is used, and where and how it is stored;

(e) where possible, through the same medium in which the information was provided; and

(f) in a form that that can be retained and is intelligible to the individual.

(2) When access to personal data is provided, the individual shall be informed of:

(a) The purposes of processing the information;

(b) the recipients of such information;

(c) whether the individual's national identifier is provided;

(d) the period for which such information will be retained;

(e) the right to dispute such information and request that it be corrected or erased;

(f) the right to lodge a complaint with the Authority;

(g) where the information was not collected from the individual, information about the source of the information;

(h) the existence of automated decision making and profiling.

(3) If any individual believes that his or her personal data is inaccurate, untimely or incomplete, or unlawfully collected or processed, he or she shall have the right to have his or her personal data updated, corrected or deleted by the entity.

(4) Any individual may make an application to an entity to exercise his or her right to have his or her personal data updated, corrected or deleted by the entity.

Provided that

(a) the entity will have thirty calendar days from receipt of such an application to examine the application, following which the personal data must be updated, corrected or deleted unless the examination of the application confirms the correctness of the current personal data; and

(b) while a dispute is pending, the entity shall restrict processing of the disputed personal data of the individual; and

(c) upon completion of the investigation, if a change results, the entity shall take steps to provide an update to third parties that were provided the personal data prior to or during the dispute.

(5) Every entity has a duty to take reasonable steps to ensure the accuracy, timeliness and completeness of personal data it holds or controls.

(6) The individual shall have the right to receive personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another specified data controller without hindrance from the data controller to which the personal data have been provided, especially where the processing is carried out by automated means.

(a) In exercising his or her right to data portability, the individual shall have the right to have the personal data transmitted directly from one data controller to another, where technically feasible and practicable;

(b) the right referred to in this subsection shall not adversely affect the rights and freedoms of other individuals.

10. Cross Border Transfers of Personal Data

(1) Any transfer of personal data outside the territory of India to a foreign country shall take place only if the data controller or data processor has ensured that necessary, reasonable and enforceable safeguards, with effective legal remedies for individuals, are available in the territory of the foreign country such as:

(a) the foreign country's level of legal protections;

(b) adequate contractual provisions;

(c) an agreement between the foreign country and the Central Government or an international agreement to which the Central Government is a party.

(2) Notwithstanding the foregoing, a transfer of personal data to a third country shall be permitted if:

(a) The transfer is necessary for the performance of a contract between the individual and the data controller;

(b) necessary in public interest;

(c) necessary to protect the vital interests of the individual or of other individuals where the individual is physically or legally incapable of giving consent;

(d) transfer is necessary for the establishment, exercise, or defense of legal claims;

(e) the personal data is publicly available.

11. Retention of Personal Data

(1) No personal data shall be retained or kept in a form which permits identification of individuals

(a) for longer than necessary after the achievement of legitimate purpose for which it was collected;

(b) if obtained unlawfully;

(2) Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the legitimate purpose for which it was collected or received, or, if that legitimate purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if there are overriding legitimate interests and it is necessary—

i. for compliance of a legal obligation or court order or an any action taken by an officer in exercise of the power vested in him or her;

ii. for establishing or defending a legal claim;

iii. it is required to be stored for legally mandated purposes, such as tax, historical, statistical or research purposes:

(i) Provided that only that amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored, subject to the implementation of the appropriate technical and organizational measures to safeguard the rights and freedoms of the individuals, and any personal data that is not required to be stored for such purpose shall be destroyed forthwith;

(ii) any person who maintains or otherwise possesses personal data for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

12. Rights relating to Automated Decision-making: If an automated tool is used by the entity in whole or part to make decisions regarding an individual, the entity:

(a) must provide meaningful information to the individual about the basis on which the decision was made at, as well as the significance and envisaged consequences of such processing for the individual;

(b) has a duty to disclose reasons for decisions;

(c) demonstrate through a prior assessment that the tool is predictive for a legitimate purpose and non-discriminatory against protected characteristics;

(d) be subject to data audits by the Authority.

13. Right against Harm:

(1) Every entity shall make reasonable efforts to ensure that personal data is not used, disclosed or retained in ways that cause harm to individuals.

14. Right to Informational Privacy:

(1) All individuals shall have a right to informational privacy pursuant to which they shall have the right to prevent information about themselves from being disseminated and to control the extent of access by any entity to their personal data.

(2) Every entity shall make reasonable efforts to ensure that it accesses and processes personal data in a manner that is consistent with the right to informational privacy of individuals as described in section 14(1).

15. Notice

(1) Every individual shall be duly informed about the collection and processing of personal data through issuance of a privacy notice as described in section (2) which shall be conspicuous, concise, timely, updated, transparent, intelligible and easily accessible form written in clear, plain and understandable language both in English and predominant language of the individual's geographical area and, where a significant portion of the population has limited literacy skills, in a visual and written format, in a form that can be retained and provided free of cost to the individual.

(2) Where personal data relating to an individual are collected from the individual, the data controller shall, at the time when personal data are obtained, provide the individual with all of the following information through a privacy notice:

(a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
(b) the description of the information collected including from third parties;
(c) whether providing the personal data is voluntary or mandatory and the consequences of failure to provide the personal data;
(d) the contact information for revoking consent;
(e) the legitimate purposes for which the information will be used;
(f) to whom the information may be disclosed including transfers of personal data to another country;
(g) describing the right of the individual to request access to the information;
(h) describing the right of the individual to withdraw the collected information;
(i) describing any potential use of automated decision making, and in doing so also be in accordance with section 6(3);
(j) indicating where there is a possible transfer of personal data to countries that do not provide adequate legal protection and safeguards for the data;
(k) for information collected about the individual from third parties, the notice must also provide information regarding –
    i. the identity and contact information for such third parties;
    ii. the purposes of processing that information and the legal basis for such processing;
    iii. the categories of data;
    iv. the right to access such information and dispute its accuracy;
    v. the nature of security measure to protect the information;
    vi. how long information will be retained.

(3) If the data controller is making automated decisions, the notice must also –
(a) inform the individual that the data controller is engaging in this type of activity;
(b) provide meaningful information to the individual about the basis on which the decision was made arrived;
(c) and explain the significance and envisaged consequences of such automated decision making.

(4) The Authority is authorised to provide guidance regarding the format and substance of notices, including the publication of model notices.

16. Privacy By Design

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the data controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data protection principles, including data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Act and protection of the rights of individuals.

(2) The data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

17. Data Protection Officer

(1) Every data controller, data processor or third party shall appoint a Data Protection Officer having adequate technical expertise in the field of data collection or processing and the ability to address any requests, clarifications or complaints made with regard to the provisions of this Act:

(2) Provided that the data controllers and processors employing less than five hundred people and having an annual turnover of less than one crore rupees may jointly appoint a Data Protection Officer, for resolving or addressing any requests, clarifications or complaints made herein in collaboration with other bodies with similar size or turnover.

(3) The Data Protection Officer shall:

(d) inform and advise the data controller or the data processor pursuant to this Act;

(e) monitor compliance with this and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;

(f) cooperate with and act as the contact point for the Authority.

(g) in the performance of his or her tasks have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.

(4) Individuals may contact the Data Protection Officer regarding all issues related to processing of their personal data and to the exercise of their rights under this Act.

(5) The Data Protection Officer shall be bound by appropriate secrecy or confidentiality obligations concerning the performance of his or her tasks in relation to the handling of personal data.

(6) The Data Protection Officer may fulfil other tasks and duties. The data controller or data processor shall ensure that any such tasks and duties do not result in a conflict of interests.

(7) No additional fee shall be charged for resolving or addressing any requests, clarifications or complaints made herein.

(8) The Data Protection Officer shall—

(h) act as an independent person;

(i) address requests, clarifications or complaints made in writing, including through electronic form, by any aggrieved individual or legal representative thereof;

(j) take steps to initiate an inquiry and commence proceedings within seven days of receiving the complaint;

(k) resolve the matter within thirty days of receipt of complaint, and where the matter is not resolvable in this period provide an explanation to the individual making the complaint and the period by which the matter will be resolved which shall not exceed ninety days;

(l) recommend the data controller or data processor to take appropriate action; and

(m) record the proceedings, the results thereof and the reasons for arriving at the decision in writing.

(9) In cases where the Data Protection Officer has not been appointed or is unable to or does not adequately resolve the complaints within the stipulated period of ninety days, the complainant may approach the Authority for redressal of complaints.

18. Data Security

(1) Data controllers, data processors, and entities exempt under section 4, shall take security measures necessary for safeguarding and securing the personal data in their custody with due diligence including:

(a) designating one or more employees to coordinate their information security program;

(b) identifying and assessing the risks to personal data in each relevant area of their operation, and evaluating the effectiveness of the current safeguards for controlling these risks;

(c) designing and implementing a safeguards program, and regularly monitoring and testing it;

(d) selecting service providers that can maintain appropriate safeguards, making sure their contract requires them to maintain safeguards, and overseeing their handling of customer information; and

(e) evaluating and adjusting the program in light of relevant circumstances, including changes in their business or operations, or the results of security testing and monitoring.

(f) Data controllers and data processors, where appropriate, shall employ methods for de-identification and encryption of personal data.

(2) When designing any procedures or systems for handling personal data, data processors and data processors shall address and incorporate any appropriate security measures.

19. Breach Notification

(1) Every individual shall be promptly informed about any breach involving sensitive personal data that is likely to cause harm,

a. **Provided that** it is the duty of the data controller or, on its behalf, the data processor or third party, to provide a breach notification to the individual as soon as possible from the occurrence of the breach as well as take adequate measures to mitigate any harm or damage:

b. **Provided further** that in the event that such breach notification is impractical, due to an inability to contact individuals or the substantial number of individuals involved, a breach notification may be made by publication in a manner reasonably likely to clearly and unambiguously put such individuals on notice of the breach,

Save that where a public body responsible for the prevention, detection, or investigation of offences or the Authority determines in writing that such notification will impede a law enforcement investigation or result in other adverse consequences

for public order or safety, the breach notification may be delayed for the period specified in such written determination.

(2) The burden of proof to substantiate that adequate measures have been taken in accordance with the provisions of this Act, shall lie on the data controller or data processor or third party.

(3) The breach notification provided under this section as specified by the Data Protection Authority shall include:

(a) the identity of the data controller, even in cases where the notice is provided by the data processor or a third party;

(b) a general description of the breach;

(c) the types of information compromised and the likely consequences of the breach;

(d) the estimated date or range of dates of the breach;

(e) the number of individuals involved;

(f) the steps taken to mitigate and remediate the breach;

(g) the rights available to individuals and the contact information of the entity providing the notice.

(4) The data controller or data processor, on its behalf, shall notify the Authority any time such notice has been provided. The notice to the Authority shall state:

(a) The nature of the breach

(b) The systems affected

(c) The number of individuals whose data was compromised

(d) The remedial actions taken.

(5) Every breach must be notified to the Data Protection Authority.

(6) The Authority shall establish and maintain a public registry of breach notifications received from data controllers and data processors and publish all notices received on the registry.

20. Liability of entities:

Any entity that fails to collect, store, process, disclose, use, share or otherwise handle any personal data in accordance with the terms of this Act shall be liable in respect of the violation of any of the rights provided under this Act as a result of such failure,

Provided that where multiple entities are responsible for a failure under this provision, their liability shall be joint and several.

Provided further that, such entity shall be given a reasonable opportunity of being heard before the judicial authority before any penalty is imposed.

21. Burden of Proof:

Where an individual establishes prima facie that an entity's act or omission has resulted in a violation of any of such individual's rights provided under this Act, the burden of proof shall lie on the entity to prove that it did not commit or was not responsible for the commission of the acts or omissions in question.

CHAPTER III

Powers and Functions of the Data Protection Authority

22. The Data Protection Authority

(1) The Data Protection Authority shall be constituted to undertake the functions and fulfill the regulatory objectives specified in this Act.

(2) The Central Government shall, by notification in the Official Gazette, and in consultation with the Chief Justice of India, appoint a Chairperson and other members to the Data Protection Authority in such manner as may be prescribed.

(3) Regulatory Objectives: The Data Protection Authority shall carry out its functions in furtherance of the objectives in the Preamble to this Act.

(4) Relationship with the Cyber Appellate Tribunal[2]

(a) Appeals from orders of the judicial authority shall be made to the Cyber Appellate Tribunal constituted under Information Technology Act 2000 (as amended);

(b) The Data Protection Authority shall have the authority to monitor compliance with the orders of the Cyber Appellate Tribunal, where such orders relate to appeals from the orders of the judicial authority.

[2] We note that following the Finance Act of 2017, the Cyber Appellate Tribunal under the Information Technology Act was collapsed and the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) took over its mandate. However, a telecom appellate authority would not be an appropriate forum to consider the wide-ranging appeals that will arise in the broad field of data protection. Rather than using the TDSAT, a potential solution could be to refurbish the Cyber Appellate Tribunal structure and have its capacity strengthened, so that it can be a relevant appellate body for issues of data protection.

23. Powers and Functions of the Data Protection Authority

(1) **Directions**: The Data Protection Authority may, for the discharge of its functions under the provisions of this Act, issue such directions from time to time, as it may consider necessary.

(2) **Advice**: The Data Protection Authority may provide advice to other government agencies, entities or individuals regarding any matters within its jurisdiction as well as public and business education.

(3) **Monitoring and research**: The Data Protection Authority shall monitor cross-border transfers of data and security breaches exclusively for research purposes and engage in research regarding the collection, use, disclosure and retention of personal data.

(4) **Supervision and enforcement**: The Data Protection Authority shall ensure compliance with the provisions of this Act and any rules made under this Act, including by undertaking enforcement actions in accordance with the provisions of this section 23(4)(c) of this Act.

(a) The Data Protection Authority shall promulgate rules regarding its supervisory activities:

i. by developing a methodology comprising both quantitative and qualitative indicators according to which the entities processing personal data may be categorised as:

(1) systemically important data entities,

(2) normal risk entities, and

(3) low risk entities.

ii. on the types of enhanced supervisory activities undertaken by the Data Protection Authority based on an entity's categorisation as a systemically important data entity including, but not limited to:

(1) increased frequency and depth of supervisory activities;

(2) review of disaster recovery and resolution plans which may be mandated;

(3) Increased reporting obligations to the Data Protection Authority; or

(4) periodic audits in connection with data security.

iii. to allow for inter-sectoral coordination with relevant public authorities and sectoral regulators to operationalise supervisory arrangements with

regard to entities processing personal data that are not systemically important data entities.

(b) The Data Protection Authority,

i. may undertake enforcement actions on its own initiative, on the basis of complaints, including on the basis of information received from the scrutiny of the complaints database, and on the basis of referrals from other public authorities or government agencies; and

ii. shall undertake enforcement actions where information received from the scrutiny of the complaints database provide reasonable cause to suspect contravention, or the likelihood of contravention, of any provisions of this Act or any order or direction issued by the Data Protection Authority under this Act

(c) The Data Protection Authority may undertake such enforcement actions as required to fulfill its mandate under sub-section (4)(a) including through the:

i. issuance of a private warning;

ii. issuance of informal guidance in response to a clarification sought by any individual or entity;

iii. issuance of a public statement

iv. issuance of a show cause notice;

v. launching of an investigation in accordance with this section 23(4)(g) of this Act;

vi. issuance of a direction requiring any individual or entity to remedy any contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, including, but not limited to, compensation taking into account the amount of unfair advantage as a result of such contravention, the amount of harm to any individual, and the repetitive nature of the default;

vii. monitoring compliance with the orders of the Cyber Appellate Tribunal, where such orders relate to appeals from the orders of the judicial authority;

viii. imposition of a monetary penalty the amount of which shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require;

ix. recommendation to relevant public authorities and sectoral regulators to take such steps as they may be empowered to with respect to any particular individual or entity;

(d) Any enforcement action authorised by the Data Protection Authority must be proportionate to the contravention of the provision of this Act, or any order or direction issued by the Data Protection Authority under this Act, in respect of which such an enforcement action is authorized;

(e) The Data Protection Authority must consider the following factors while determining the enforcement action to be taken against an entity:

i. the nature and seriousness of the contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, by the entity,

ii. the consequences and impact of the contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, including the extent of,

(1) benefit or unfair advantage gained by the entity as a result of the contravention; and

(2) loss and harm caused, or likely to be caused, to individuals as a result of the contravention;

(3) repetitive or continuing nature of the contravention default prior to the enforcement actions; and

(4) other contraventions committed by the entity under this Act.

(f) An enforcement action by the Data Protection Authority for a contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, does not bar the Data Protection Authority from prosecuting an entity for an offence under this Act, but any fine required to be paid upon conviction for an offence may be set off against any monetary penalty paid by such entity in an enforcement action in respect of the same cause of action.

(g) Where the Data Protection Authority has information or reasonable grounds to suspect that any entity is in contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, it may investigate such contravention by:

i. appointing one or more investigators to investigate the contravention; and

ii. recording such appointment by providing

(1) the appointment of the investigator;

(2) reason for commencing the investigation;

(3) scope of the investigation;

(4) the duration of the investigation, which will not exceed one hundred and eighty days in the first instance; and

(5) the method of reporting of the investigation provided that the Data Protection Authority may modify the terms of appointment, if the circumstances of the investigation require such modification.

(h) The investigator appointed pursuant to this section 23(4) of this Act will have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, including in respect of the following matters, namely:

i. the discovery and production of any document, including books of account or other documents showing compliance with the provisions of this Act;

ii. summoning and enforcing the attendance of any natural person and examining them on oath;

iii. requiring such natural persons to produce relevant records and documents; and

iv. issuing commissions for the examination of natural persons or documents.

(5) **Inter-sectoral coordination**: The Data Protection Authority shall take steps to ensure coordination between relevant public authorities and sectoral regulators, in accordance with the provisions of this section 23 of this Act.

(a) In discharging its functions under this Act, the Data Protection Authority will coordinate with relevant public authorities and sectoral regulators, including telecom authorities, financial sector authorities, health authorities, the Unique Identification Authority of India and others as appropriate in order to:

i. request for information from the other authorities in respect of investigations in progress or in connection with enforcement actions;

ii. to receive references or notifications from other authorities of the contravention of the provisions of this Act, or to make available to other authorities any order or direction issued by the Data Protection Authority under this Act, with regard to entities regulated by them;

iii. to issue and enforce enforcement actions under this Act;

iv. to recommend enforcement actions to be undertaken by the other authorities;

v. to make rules for the coordination between authorities as required pursuant to this provision of this Act, including formation of memorandums of understanding between authorities in furtherance of this objective.

(6) **Adjudication**:

(a) The Central Government shall, by notification in the official Gazette, establish a judicial authority to adjudicate all disputes and contraventions of the provisions of this Act.

(b) The judicial authority shall consist of a Chairperson and not more than two Members to be appointed, by notification in the official Gazette, by the Central Government.

(c) The selection of Chairperson of the judicial authority shall be made by the Central Government in consultation with the Chief Justice of India.

(d) The selection of the Members of the judicial authority shall be made by the Central Government in consultation with the Chairperson.

(e) The judicial authority shall consist of at least one judicial and one technical Member,

i. A judicial Member shall otherwise be qualified to be a High Court Judge or have been a member of the Indian Legal Services and have held a post in Grade I of that Service for at least three years.

ii. A technical Member shall have expertise, special knowledge of and adequate professional experience in technology and processing/collection of data.

(f) Subject to the provisions of this Act,

i. the jurisdiction of the judicial authority may be exercised by the any benches constituted thereof.

ii. The judicial authority shall comprise such benches as the Central Government may, in consultation with the Chairperson, by notification in the Official Gazette, specify.

iii. A bench may be constituted by the Chairperson of the judicial authority with one or two Members of such judicial authority as the Chairperson may deem fit.

iv. The Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each bench of the judicial authority may exercise its territorial jurisdiction.

(7) **Procedure and powers of the judicial authority**:

(a) The judicial authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the judicial authority shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(b) The judicial authority shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:–

i. summoning and enforcing the attendance of any natural person and examining him on oath;

ii. requiring the discovery and production of documents or other electronic records;

iii. receiving evidence on affidavits;

iv. issuing commissions for the examination of witnesses or documents;

v. reviewing its decisions;

vi. dismissing an application for default or deciding it ex parte;

vii. any other matter which may be prescribed.

(8) Appeal to Supreme Court

(a) Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law, an appeal shall lie against any order, not being an interlocutory order, of the Cyber Appellate Tribunal to the Supreme Court on one or more of the grounds specified in section 100 of that Code.

(b) No appeal shall lie against any decision or order made by the Cyber Appellate Tribunal without the consent of the parties.

(c) Every appeal under this section shall be preferred within a period of ninety days from the date of the decision or order appealed against: PROVIDED that the Supreme Court of India may entertain the appeal after the expiry of the said period of ninety days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time

(9) **Redressal**:

(a) Where a complaint made by an individual to an entity pursuant to their rights under this Act has not been resolved within the stipulated period , the individual may bring a complaint against the relevant entity through online lodging, toll-free calling lines, e-mail, letter, fax or in person to the Data Protection Authority if:

i. the matter is not pending before, or has not been adjudicated upon by, another competent authority; or

ii. the complaint is prima facie not frivolous, malicious or vexatious.

Provided that the complaints shall be received, recorded and tracked by the Data Protection Authority within a complaints database.

(b) Following the receipt of the complaint, the Data Protection Authority shall:

i. promptly send a notice to the relevant entity seeking reasons for the delay in the resolution of the complaint; and

ii. upon failure to receive an adequate response from the relevant entity within fifteen business days, take such enforcement actions against the relevant entity pursuant to the Supervision and Enforcement powers under section 23(4) of this Act; and

iii. provide prompt notification to the individual of the steps taken under this provision using such modes of communication as used to receive the complaint.

(10) **Reporting**: The Data Protection Authority shall release a report providing aggregate details:

(a) every month, on the complaints received including the number, nature, category, geography, sector and such other factors relating to the complaint as appropriate; and

(b) annually, on the enforcement actions undertaken and complaints acted upon using a format stipulated by the Authority, including such qualitative commentary as it sees fit.

(11) **Meetings**:

(a) The Data Protection Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be provided by regulations.

(b) The Chairperson or, if for any reason, he is unable to attend a meeting of the Authority, any other member chosen by the members present from amongst themselves at the meeting shall preside at the meeting.

(c) The Data Protection Authority may make regulations for the transaction of business at its meetings

CHAPTER IV

Miscellaneous

24. Act not in derogation of any other law: The provisions of this Act shall be in addition to, and not in derogation of, the provisions of any other law for the time being in force.

25. Power to make rules:

(1) The Central Government may, by notification, make rules for carrying out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely,

(a) the salary and allowances payable to and the other conditions of service of the Chairperson of the Data Protection Authority and members appointed pursuant to this Act;

(b) the powers and functions of the Chairperson of the Data Protection Authority under this Act;

(c) The procedure for conducting an inquiry made under section 23 of this Act;

(d) the salary and allowances and other conditions of service of officers and other employees of the Data Protection Authority;

(e) the salary and allowances payable to and other terms and conditions of service of the Chairperson and other Members of the judicial authority established pursuant to this Act;

(f) the salary and allowances and other conditions of service of the officers and employees of the judicial authority;

(g) any other matter which is to be, or may be, prescribed, or in respect of which provision is to be made, by rules.

26. Delegation: The Data Protection Authority may, by general or special order in writing, delegate to any Member, officer of the Data Protection Authority or any other person, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act (except the power under section 27) as it may deem necessary.

27. Power to make regulations:

(1) The Data Protection Authority may, by notification, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely

(a) the times and places of meetings of the Authority and the procedure to be followed at such meetings, including quorum necessary for the transaction of business;

(b) the transaction of business at the meetings of the Authority under sub-section.

28. Rules and regulations to be laid before Parliament: Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry

of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

29. Power to remove difficulties:

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of three years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.