rebit.org.in

रिज़र्व बैंक सूचना प्रौद्योगिकी प्राइवेट लिमिटेड
Reserve Bank Information Technology Pvt. Ltd.

ReBIT, 18th Floor,
CyberOne Business Park Sector 30A,
Vashi, Navi Mumbai 400703

info@rebit.org.in

Analysis of the draft Data Protection Bill, 2018

Version: 1.0
Document Ref: ReBIT/2018/TPB/RI-103

Technology Policy Briefs

Abstract: This is an initial draft analysis of the draft Data Protection Bill, 2018 vis-à-vis the broader discussions captured in the report presented by the committee. The format used is the one recommended by the Data Security Council of India (DSCI) for analyzing privacy legislations.

Author/Contributors

Author	Ranjeet Rane
Reviewer	Vivek Srivastav

Contents

Executive Summary

What the Supreme Court judgment in the KS Puttaswamy case[1] started with declaring Right to Privacy as a fundamental right was taken forward by the central government when it constituted a committee to deliberate on and draft a data protection legislation. The draft legislation was recently released for public comments by the Ministry of Electronics and Information Technology.

The draft bill defines personal data and presents a detailed list of what will be considered as sensitive personal data. Various provisions of the draft with regards to collection, storage, processing and disclosure of data are structured around these definitions. A trust-based relationship has been proposed between erstwhile data controllers and data subjects, now defined as data fiduciary and data principles respectively in the draft. The draft also seeks to introduce new concepts like significant data fiduciary, to enable differentiated implementation of data protection practices basis the degree of exposure to personal data of data principles. Another concept is the idea of a data trust score that will be given to data fiduciaries by competent auditors post a data privacy assessment under the provisions of the draft. This may enable data-focused businesses to leverage their compliance to data protection as a competitive advantage.

The setting up of a Data Protection Authority of India as an independent regulatory authority to oversee implementation of the data protection regime is another prominent feature of the draft bill. Under the aegis of this authority, the legislation looks to build strong enforcement mechanisms. The authority would have powers to conduct inquires, request for documents, search and seize record books as well as decide on the fines and penalties applicable in to offenses under the new law.

Measures to protect the interests of data principles are deeply ingrained in the draft with elaborately defined grievance redressal and dispute resolution mechanisms. It also makes provisions for setting up of offices like a Data Protection Officer by data fiduciaries to act as a first point of contact for such issues. It also makes provisions for speedy resolution of cases through a well-defined appeal process. The penal provisions of the bill are strict and also non-bailable in case of offenses committed by individuals as well as companies. Transfer and storage of data outside India is tackled in detail by the draft and clear provisions have been drafted for ensuring compliance to this requirement.

The draft has clearly outlined the obligations of data fiduciaries and the rights of data principles in a rapidly evolving data ecosystem. It outlines the exemptions available under law to the provisions of the bill in a detailed manner. The horizontal application to state and private companies is supplemented with technology agnostic provisions.

Some provisions like the inclusion of financial data under the category of sensitive personal data may warrant further discussion. This document aims to give a holistic view of the draft bill as it maps its provisions with principles underlined in the committee report.

[1] https://timesofindia.indiatimes.com/india/right-to-privacy-is-a-fundamental-right-supreme-court/articleshow/60203394.cms

Introduction

The Personal Data Protection Bill, 2018 was released by the Committee of Experts entrusted with creating a Data Protection Framework for India on July 27, 2018. The Committee, chaired by retired Supreme Court judge, Justice Sri Krishna, was constituted in August 2017 by the Ministry of Electronics & Information Technology, Government of India (MEITY) to come up with a draft data protection law. The committee followed up their preliminary white paper[2] with deliberations and a series of country wide public consultations. The draft bill is accompanied by with a report[3] titled "*A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*" which provides context to the deliberations of the Committee. MEITY has presently asked for public comments on the draft bill[4] following which it will need to be approved by the union cabinet before it is placed before the Parliament.

Scope and Applicability

The Act will apply to processing of personal data that has been collected, disclosed, shared or otherwise processed within the territory of India.
It will apply to government and private organizations, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law.
If the organizations collecting/processing the data are not located in the territory of India, then data can be processed only for a business carried on in India, offering goods or services to data principals[5] within the territory of India and for profiling such data principles within the territory of India.
The Act will not apply to processing of anonymized data.

2 http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

3 http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

4 http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

5 "Data principal" means the natural person to whom the personal data is attributed to

Legal Relationships

The draft introduces a 'trust' relation between the data principle and the data fiduciary. This forms the foundation of all legal relationships in the proposed law. Some of the important entities defined in the draft are as follows:

Data Principle: Is the person, company, or entity whose information is being collected.

Data Fiduciary: Can be a person, state, company, or any entity that decides why data should be processed and how it should be processed. Commonly referred to as Data Controller. The draft also includes another category called "Significant Data Fiduciary" based on the volume and sensitivity of the data, the fiduciary's revenue, risk of "harm" to the principal, and type of technology used. Some regulations of the draft such as assessments, audits, record keeping, and hiring a data protection officer apply only to these significant fiduciaries.

Data Protection Officer (DPO): Data fiduciaries have been mandated to appoint DPO for advising on matters of understanding, interpretation and implementation of various requirements of the act. The DPO will also function as point of contact for grievance redressal and ensuring compliance to standards defined by the Data Protection Authority of India (DPAI).

Data Protection Authority of India (DPAI): The draft proposes to set up an independent regulatory authority, Data Protection Authority of India (DPAI). It would perform 24 types of functions predominantly grouped in the following categories:

Adjudication: To handle enforcement of the act and receive grievances.
Monitor: Data security breaches, internal assessments and external audits of the data fiduciaries
Policy Formulation: Specify terms like sensitive personal data, purpose for processing data, different types of consent and terms for lawful transfer of data outside India. Advise the central government on matters around data protection at national and international level
Research and Awareness: Promoting public awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data. Undertaking research for innovation in the field of protection of personal data
The authority would consist of a chairman and six members, it would have a central office and other offices across the country as approved by the central government. It would be responsible to the Parliament and subject to audit by the CAG.

Definition of Personal Information

Personal information has been defined granularly in the draft. Any data that can used to directly or indirectly identify an individual or can be used in combination with any other information to identify an individual has been defined as personal data. It further defines a sub category of 'Sensitive Personal Information' that includes the any information related to the following:
Passwords, financial data[6], health data, official identifier[7], sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation and any other data as specified by the DPA.

Privacy Principles

The draft bill is structured around seven core principles. These principles underline the philosophy of the Indian data protection legislation. These are:
Technology Agnostic: Flexible to take into account changing technologies
Horizontal Applicability: Applies to both government and private sector entities
Consent: Would be valid only if it is free, informed, clear, specific, and capable of being withdrawn
Purpose Limitation: Processing of data to be limited only for the purpose for which consent is acquired
Collection Limitation: Collection of personal data shall be limited to such data that is necessary for the purposes of processing
Accountability: The data fiduciary shall be responsible for complying with all obligations set out in this Act with regards to any processing undertaken by it or on its behalf
Enforcement: The law proposes the setting up a high powered statutory authority with powers to discourage and penalize wrongful acts

[6] "Financial data" means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history

[7] "Official identifier" means any number, code, or other identifier, including Aadhaar number, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal

Regulatory Infrastructure

Setting up of a Data Protection Authority of India (DPAI) is proposed in the draft bill. The DPAI will be comprised of one chairperson and six other members. They will be selected by a committee comprising of the Chief Justice of India, the Cabinet Secretary and one expert nominated by the CJI. The chairperson and the members of the Authority shall be persons of ability, integrity and standing, and must have specialized knowledge of, and not less than ten years professional experience in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects. The central government has been tasked to maintain a list of such experts. The committee members cannot be re-appointed. The DPAI will be funded by grants from the central government and subject to auditory requirements as specified by the CAG. The DPAI can appoint officers, consultants, and experts as needed for discharge of its duties.

Regulatory Mechanisms

The draft lists down an elaborate regulatory structure along with powers and functions of the DPAI, some of the important ones are captured here.
The primary duty of the DPAI is to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of the Act, and promote awareness of data protection. Towards meeting these objectives it can:
Specify reasonable purposes for which personal data may be processed, specify categories of sensitive personal information, take action in case of a data breach, specify the criteria for assigning a rating in the form of a data trust score[8] by a data auditor, monitoring cross-border transfer of personal data, and promoting public awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data to name a few.
Code of Practice: *The Authority shall issue codes of practice to promote good practices of data protection and facilitate compliance. It can also approve, and issue codes of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government. This provision widens the scope of sector regulators to determine broad contours of data protection practices relevant to their regulated entities.*
The authority would also be vested with powers to issue directives, call for information, conduct inquires, take action on the basis of such an inquiry, conduct search and seizure of records both in paper and electronic format. It would also have an adjudication wing, the constitution of which will be done by the central government

[8] Draft Data Protection Bill, 2018, Sec 35, sub-section (2), (5) & (6)

to maintain the independence and neutrality of the wing. The authority would need to consult with other regulator or authorities before taking action and may also enter into a memorandum of understanding with other regulators or authorities governing the coordination of such actions.

Data Transfer Instruments

The draft bill has strict provision for regulation cross border transfer of personal data. Every data fiduciary will need to maintain a local copy on a server based in India, of all personal data collected/processed by it. The central government will have the authority to define the category of 'critical personal data' which will be mandated to be processed and stored only in India. It can also notify certain categories of personal data as exempt from the requirement of being stored in India on the grounds of necessity or strategic interests of the State. The draft also outlines the conditions under which personal data other than sensitive personal data may be transferred outside Indian territory, including but not limited to standard contractual clauses, exceptions prescribed by the central government and explicitly consented by the data principle.

Organizational Measures

The act mandates the appointment of Data Protection Officer (DPO) by data fiduciaries to carry out the following functions:

- Provide information and advice to the data fiduciary to ensure compliance with this law
- Monitor personal data processing activities of the data fiduciary to ensure that such processing is compliant with provisions of the law
- Advise on the conduct of data protection assessments and review such assessments
- Ensure that data fiduciary adheres to the 'Privacy by Design' principle
- Act as a point of contact with the DPAI
- Act as a point of contact for data principles for raising grievances
- Maintain an inventory of all records of the data fiduciary

Data Breach Notification

A personal data breach has been defined in the draft as "any unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal". The data fiduciary is expected to inform the DPAI of such a breach only if it is likely to cause harm[9] to a data principle. Such a notification would include information about the nature of personal data impacted, number of data principles affected, possible consequences of the breach and measures being taken by the data fiduciary to remedy the breach. The DPAI would decide on whether data principles need to be informed of such a breach and also post details of the same of its website.

Rights of Data Subjects

The Sri Krishna committee report stresses on the rights that data principles will be entitled to through the new legislation. This focus has manifested in the draft bill in form of four rights to data principles, these are:

Right to confirmation and access: The data principles are entitled to receive a confirmation from the data fiduciary about personal data being processed, summary of personal data processed and summary of processing activities performed by the data fiduciary. All information should be provided in a clear and concise manner that is easily comprehensible by a reasonable person.

Right to correction (of personal data): Data principles can seek correction of inaccurate or misleading personal data, completion of incomplete personal data and updating of outdated personal data from data fiduciary. Data fiduciary can refuse such a correction with adequate justification in writing for rejecting the application.

Right Data Portability: Data principles can ask for personal data that was collected by the fiduciary for provision of a service, obtained as a profile or shared by the principle with the fiduciary in a structured, commonly used, and machine-readable format. The data principle can also have it transferred to any other data fiduciary in the format specified.

Right to be forgotten: The data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal where such disclosure has served the purpose for which it was made or the consent

[9] "Data principal" means the natural person to whom the personal data is attributed

for it is withdrawn or was illegally disclosed with reference to existing central or state laws. Applicability of this right is subject to determination of grounds for such an action by the Adjudication Officer of the DPAI. The officer should determine if the that the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen

Data fiduciaries can charge a reasonable amount of fee for performing all of the above asks, except for those of providing the data principles with a summary of their personal data and processing activities performed on their personal information. The data fiduciary is not obliged to comply with any request made where such compliance would harm the rights of any other data principal under this Act.

Liabilities

The draft defines acts that would be classified as 'offenses' under the data protection legislation. These include:

- Obtaining, transferring or selling of personal data contrary to the Act
- Obtaining, transferring or selling of sensitive personal data contrary to the Act
- Re-identification[10] and processing of de-identified personal data

Offenses committed by individuals will be punishable by varying prison terms as well as fines in excess of two lakh rupees. All offense are cognizable and non-bailable. For offences committed by companies, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

If an offence is committed by any department of the Central or State Government, or any authority of the State, the head of the department or authority shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

For non-compliance with provisions of the act, penalties are proposed to the tone of up to five crore rupees or two per cent of the data fiduciaries' total worldwide turnover of the preceding financial year, whichever is higher. If a data fiduciary is found to contravene provisions regarding processing of personal and sensitive personal data, failing to adhere to security safeguards and illegal transfer of data outside India, the penalties would be up to fifteen crore rupees or four percent of total worldwide turnover of the preceding financial year, whichever is higher. Further penalties are defined for data fiduciaries' failure to –

[10] Means the process by which a data fiduciary or data processor may reverse a process of de-identification (make anonymized data identifiable)

- comply with data principal requests
- furnish report, returns, information, etc.
- comply with direction or order issued by the Authority

All penalties and fines would be levied by the Adjudicating Officer after thorough inquiry. The appeal to the decision of the AO would lie with an Appellate Tribunal established by the central government for this purpose. The appeal to this tribunal would lie with the Supreme Court of India.

Strong penal provisions in the draft have been supplemented with equally strong enforcement mechanisms. The draft mandates the setting up of a 'Data Protection Fund' that will accrue all sums received way of penalties by the Authority. It also makes provisions of a 'Recovery Officer' who would be empowered to attach and sell moveable and immoveable property, bank accounts etc. for the recovery of fines.

Exceptions

The draft makes exemptions over application of the law for:

- Processing of personal data in the interests of the security of the State done in accordance with a procedure established by law passed by Parliament
- Prevention, detection, investigation and prosecution of contraventions of law
- Processing for the purpose of legal proceedings
- Processing of personal data by any Court or Tribunal in India for the exercise of any judicial function
- Research, archiving or statistical purposes
- Personal data processed by a natural person in the course of a purely personal or domestic purpose
- Journalistic purposes, in compliance to a code of ethics issued either by the Press Council of India or any media self-regulatory body
- Manual processing by small entities[11] using non automated means for data processing

Dispute Resolution Mechanisms

The draft law address both aspects of disputes, those originating from the data principle as well as those between the data fiduciary and the DPAI. For disputes between data principle and data fiduciaries, the draft mandates the setting up of appropriate procedures and effective mechanisms to address grievances of data principals efficiently and in a speedy manner. Such a grievance should be resolved

[11] Entity with annual turnover less than 20 lakhs, not processing personal data of more than one hundred data principals in any one day (annually) and does not collect personal data with intention of disclosure to any other individuals or entities, including other data fiduciaries or processors

within a period of 30 days, failing which the data principle can approach the Adjudication wing of the DPAI. Appeals will be with the Appellate Tribunal. Any data principal who has suffered harm as a result of any violation by a data fiduciary or a data processor, shall have the right to seek compensation from these entities.
For penalties and fines levied by the DPAI, the appeal would be with the Appellate Tribunal and the Supreme Court.

Conclusion

Preliminary analysis of the draft data protection bill underlines the long due need of such a legislation tailor made for Indian scenario. Some provisions like the classification of financial data as SPI, strict terms for transfer of data outside India, definition of critical personal data, role of sectorial regulators and criminal charges against company officials may need to further discussion.

References

A Free and Fair Digital Economy Protecting Privacy , Empowering Indians Committee of Experts under the Chairmanship of Justice B . N . Srikrishna. (n.d.). Retrieved from http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

THE PERSONAL DATA PROTECTION BILL, 2018 Retrieved from http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

Stay Connected

Reserve Bank Information Technology Pvt. Ltd
https://rebit.org.in

LinkedIn
https://www.linkedin.com/company/reserve-bank-information-technology-pvt-ltd

Twitter
https://twitter.com/reservebankit

Email
communications@rebit.org.in

Tech Policy Briefs

Technology is now embedded deep into the business success. It has the potential to disrupt existing business models even in mature industries. Information technology, which was once a cost center, has now become a strategic business imperative. ReBIT's "Technology Landscape Briefs" are series of papers that touches upon specific technologies or use of technologies as they pertain to financial domain with a focus on "security".

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. ReBIT disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any act or
omissions made based on such information. ReBIT does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel and other licensed professionals.

About ReBIT

Reserve Bank Information Technology Private Limited (ReBIT), has been set up by the Reserve Bank of India to serve its IT and cybersecurity needs and to improve the cyber resilience of the Indian banking industry.

Subscribe to ReBIT's Cyber Pulse Monthly Newsletter

https://rebit.org.in/newsletter