
Enterslice
PRIVACY AND
DATA PROTECTION

Contents

ABOUT US

ENTERSLICE IS A RENOWNED MANAGEMENT CONSULTANCY FIRM THAT HAS ESTABLISHED ITSELF AS A MARKET LEADER IN SERVING CORPORATE HOUSES AND ENTREPRENEURS WITH THEIR BUSINESS SETUP, BUSINESS MANAGEMENT, ADVISORY, FINANCIAL PLANNING AND MANAGEMENT, RISK ASSURANCE (VCFO) AND REGULATORY REQUIREMENTS. WE ARE A GLOBALLY RECOGNISED LEGAL TECH AND CPA FIRM BACKED BY AVANT-GARDE ARTIFICIAL INTELLIGENCE (AI) AND AUTOMATION, KNOWN FOR ITS CUSTOMER-CENTRIC, CUSTOMISED AND PEERLESS SERVICES TO ITS CLIENTS WORLDWIDE.

OUR TEAM COMPRISES SEASONED CHARTERED ACCOUNTANTS, COMPANY SECRETARIES, MBAS AND LAWYERS OPERATING FROM OUR OFFICES WORLDWIDE. WE ACT AS AN ALL-INCLUSIVE SOLUTION TO OUR CLIENTS, HELPING THEM ACHIEVE THEIR BUSINESS GOALS AND OPERATING UNHINDERED AND COMPLIANTLY. OUR TECHNOLOGY-DRIVEN SOLUTIONS ENABLE US TO BECOME YOUR PARTNER AND HELP YOU GROW YOUR VENTURE TO SUPERIOR HEIGHTS OF SUCCESS.

INTRODUCTION TO PRIVACY AND DATA PROTECTION

On 16th December 2021, the Joint Parliamentary Committee submitted their report to the Indian Parliament in regard to the Personal Data Protection Bill 2019 upon deliberation of upto two years for framing a robust data protection regulation for India. The Committee was then presented with the "revised" Data Protection Bill, 2021. Even though no specifically dedicated legislation in India addresses data privacy and data protection on a Sector-Nuteral basis, currently in India, data privacy and protection is governed under the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

In Justice K.S. Puttaswamy v UOI and Ors., the Supreme Court held that "the Right to Privacy is a basic fundamental right which resulted in changing the jurisprudence of privacy laws in India where the right to privacy is upheld as an inalienable, inherent, and natural right which is indispensable to a dignified life in accordance with Article 21 of the Indian Constitution.

Due to the significant impetus and the required digital transformation during Budget 2022, India undeniably requires comprehensive data protection legislation to develop the digital economy. Over the past few years, the Indian digital system has drastically transformed, and Sectoral Regulators have enacted necessary guidelines, regulations and policies that address concerns in regard to data protection of the interest of the consumers.

AN OVERVIEW OF THE PERSONAL DATA PROTECTION BILL, 2021

The Personal Data Protection Bill 2019 was modelled with reference to the European Counterpart, the "General Data Protection Regulation (GDPR)", which mirrors a delicate consensus among the stakeholders about basic principles that govern and regulate personal data. The Personal Data Protection Bill 2021 further includes non-personal data, digital media regulations and the certification of digital and Internet of Things devices which is expected to impact businesses majorly and lead to the demand for fresh industry-wide consultations in regard to the Personal Data Protection Bill 2021. The Joint Parliamentary Committee's Report also has suggested significant improvements in regard to the Personal Data Protection Bill 2019, such as clarity on timelines, removal of the concept of fixed penalties and emphasis on the growth of start-ups and small businesses, and has been welcomed by the business organisations.

The Personal Data Protection Bill 2021 states provisions for the data principal for exercising multiple options, which can be nominating a legal heir, exercising the right to be forgotten or appending the terms of the agreement in relation to the processing of any personal data in the event of death. The Joint Parliament Committee has also retained the clause where any agency of the Government may be exempted from the application of any or all the provisions of the Personal Data Protection Bill 2021.

The Joint Parliament Committee has also recommended that the Government needs to lay down a procedure for oversight that is required to be just, fair, reasonable, and proportionate.

Although the provisions are not altered from the Personal Data Protection Bill 2019, there are significant changes in the Personal Data Protection Bill 2021.

NON-PERSONAL DATA

Non-Personal Data under the Personal Data Protection Bill 2019

The Personal Data Protection Bill 2019 did not regulate Non-Prersonal Data. Clause 91 (2) of the Bill authorised the Central Government, with the consultation of the Data Protection Authority (DPA), for directing data fiduciaries or data processors for providing anonymised personal data or non-personal data, which served the purpose of better targeting delivery of services for the formulation of evidence-based policies. The Justice Srikrishna Committee had also deliberated on issues which concerned non-personal data and emerging processing activities which held considerable strategic and economic interest for India. The regulations were deliberated by future committees.

Observations

The Joint Parliamentary Committee had expressed their concern in regard to over keeping of non-personal data, which was outside the purview of the Personal Data Protection Bill 2021. In the opinion of the Committee, it is detrimental to privacy to define and restrict the new legislation only for protecting the personal data and for the Bill to be named Personal Data Protection Bill 2021. The Committee also observed that a large volume of non-personal data is derived from personal data, sensitive personal data, or critical personal data that has been either anonymised or converted to non-re-indentifiable data.

Analysis

The Joint Parliament Committee offered three justifications for including Non-Personal data in the Personal Data Protection Bill 2021 -

- Non-Personal Data can also affect privacy. In case the protocols for anonymisation are not strong enough, it enables the re-identification of Personal Data. Clause 83 of the Bill already states a strong deterrent, making re-identification a criminal offence.
- Difficulty in differentiating between Personal data and Non-Personal Data.
- Legally, one cannot have two different DPAs for dealing with two different kinds of data.

Key Recomendations

- The application of the Personal Data Protection Bill 2021 is to be extended to Non-Personal Data which also includes anonymised Personal Data.
- The DPA is to regulate both Personal and Non-Personal Data.
- One legislation that governs Personal and Non-Personal Data.
- When the provisions to regulate non-personal data are finalised, new legislation focusing specifically on non-personal data under the Data Protection Act.
- The Central Governement is authorised to frame policies that handle non-personal data, which includes anonymised personal data.
- The Personal Data Protection Bill 2021 retains provisions for mandatory sharing and non-personal data with the Indian Government along with introducing incremental concepts that pertain to non-personal data, known as Non-Personal Data Breach".

DATA-LOCALISATION AND CROSS-BORDER DATA TRANSFER

Data-Localisation and Cross-Border Data Transfer under the Personal Data Protection Bill 2019

Personal Data Protection Bill 2019 did not stipulate any additional obligation in regard to the cross-border transfer of personal data. The sensitive personal data can be transferred outside India that is subject to the explicit consent of the data principal along with the fulfilment of the following additional conditions - either through a contract or an intra-group scheme which has been approved by the DPA; the DPA has permitted to transfer for a specific purpose; or the transfer is made pursuing an adequate decision taken by the Central Government with the consultation of the DPA.

However, Critical Personal Data should be processed only in India and can only be transferred outside India where the transfer is to a person or entity that is engaged in the provision of health services or in case of any required urgent service or where the transfer decision does not affect the security and the strategic interest of the State.

Observations

Data Localisation, which refers to implication of restrictions on any cross-border movement of data along with the local storage of data after data processing is related to two strategic aspects of data -

- Geographically Located Data Storage
- Data Sharing

The recomendations of the Joint Parliament Committee of data localisation is rooted in four essential strategic objectives -

- National Security and Law Enforcement
- Privacy
- Employment Generation
- Bargaining Power in other countries

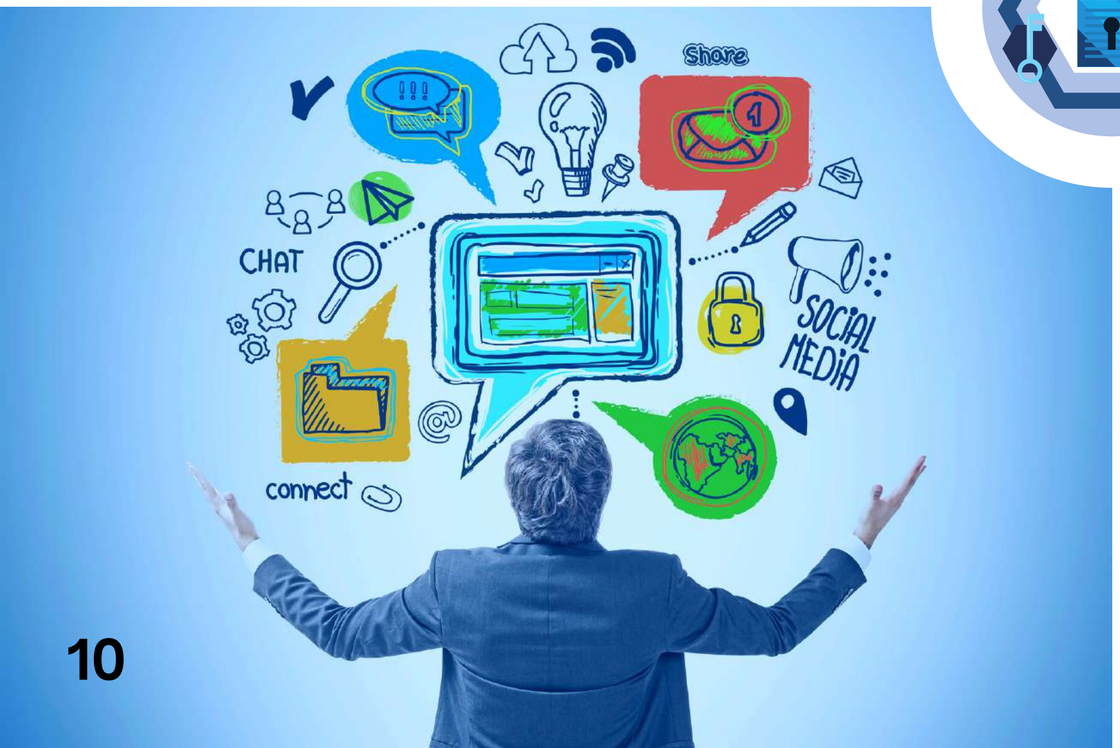
Analysis

- Expanded Role of the Central Government due to including the consultative role of the Central Government that grants cross-border transfer approvals through contact or Intra-Group Schemes/for specific purposes as anticipated by business organisations.
- As per the Personal Data Protection Bill 2021, the adequate decision for cross-border transfer of personal data is to be based on the findings of sensitive personal data that is not shared with any foreign agency or government unless approved by the Central Government.

Key Recomendations

- The Central Government needs to take concrete steps for ensuring that a mirror copy of sensitive and critical personal data that is already in the possession of foreign entities is to be mandatorily brought to India within the specified timeline.
- The Central Government, with the consultation of all secular regulators, need to prepare and pronounce a comprehensive policy on data localisation.
- The Central Government's surveillance of data stored in India needs to be strictly in terms of the necessity laid down in the legislation.
- The DPA is required to consult the Central Government in regard to approvals for transfers of sensitive personal data either through contract or Intra-Group Scheme or transfers for specific purposes.
- Any contract or Inra-Group Scheme for transfers that violate the public policies or state policies are not to be approved.
- An adequate decision by the Central Government for cross-border data transfer also includes restrictions on the onward transfer of sensitive personal data to any foreign agency or government with a prior approval from the Central Government.

SOCIAL MEDIA PLATFORMS



Social Media Intermediaries under the Personal Data Protection Bill 2019

The Personal Data Protection Bill 2019 does not include a constructive regulatory regime for Social Media intermediaries and instead lays down specific obligations for social media intermediaries. The definition of the term "Intermediary" mentioned in the 2019 Bill is in accordance with the IT Act.

The Personal Data Protection Bill 2019 was enacted when the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 was not enforced. The Justice Shrikrishna Committee made a similar remark to as the regulation as to the regulation of non-personal data and concluded that issues that concern intermediary liability, philosophical questions and effective enforcement of cyber security require greater deliberation but deferred regulation to the wisdom of the future committee.

Observations

The Joint Parliamentary Committee noted the cognisance of numerous concerns in regard to operations of social platforms which can range from "prevalence of fake accounts" to "insights across the globe to plan, organise and execute revolutions, protests, riots and spread violence".

Social Media intermediaries perform dual functions, and there is an urgent need to regulate social media intermediaries, as intermediaries often work as publishers owing o the fact they secure the ability to select the receiver content along with exercising control over the access to any such content as posted.

Analysis

Social media intermediaries often require reconsideration, and the laws of Data Protection do not provide adequate context for the same. There are also concerns in regard to social media regulations and cyber security which keeps rising daily as technology advances. A Personal Data Protection Legislation is required fulfilling the expectations of laying down a base for regulating personal data.

"Social media platforms" who have always been treated as intermediaries, should not be automatically treated as publishers because they have the ability to select the receiver of third-party content or can control access to such content. Such platforms may only exercise this ability in pursuance of their legal obligations under Section 79 of the IT Act.

Key Recomendations

- The social media "intermediaries" are to be designated as social media "platforms".
- Social media platforms are required to be held liable for content from unverified accounts on their platforms.
- Social media platforms are not to be permitted to operate in India if the parent company handling the technology does not have an office set up in India.
- The Statutory Media Regulatory Authority is required to set up in accordance with the Press Council for India to serve the purpose of regulating the contents of all such media platforms irrespective of where their content is published.
- The Committee dropped the exceptions in the 2019 Bill in regard to the definition of social media without providing any sufficient reason.
- The Committee has now retained the provision where social media platforms require to provide their users with a mechanism which verifies themselves voluntarily.

DATA BREACHES

Data Breaches under the Personal Data Protection Bill 2019

The Personal Data Protection Bill 2019 has laid down reporting obligations that are required to be undertaken by the data fiduciary in the event of any breach of personal data. The 2019 Bill does not explicitly define "Data Breach" but has laid down provisions that define "Personal Data Breach". The Bill stipulates data fiduciary reporting regulations only if the data breach is to cause any form of harm to any data principal, along with not specifying any fixed timeline for reporting any data breach.
According to the 2019 Bill, a data breach can only be reported to the DPA through a Notice. Upon receiving the Notice, the DPA can direct the data fiduciary for the following -

- Reporting the data breach to the data principal, taking into account the severity of the harm.
- Taking appropriate remedial action.
- Conspicuously posting the details of the breach on their website.

Observations

The Joint Parliamentary Committee has laid down a detailed analysis of data breaches and their impact on the individuals, along with expressing concerns over the subjective discretion of the data fiduciary in regard to the report of any data breach to the DPA and the lack of specific timelines for reporting such breaches.

The Committee states that there needs to be a realistic and finite timeline for reporting the data breach to the DPA, along with providing specific guidelines to be followed by the DPA while framing regulations regarding the same.

The Committee also pointed out that the 2019 Bill does not explicitly define "Data Breach".

Analysis

The Joint Parliamentary Committee has recommended that the data fiduciaries report all data breaches to the DPA irrespective of the level of harm caused to the data principles. The former is required to spend considerable time, effort and resources towards compliance, even for minor breaches, and then later to deal with a large number of non-serious data beach notices, which drifts the focus away from the essential data that requires the attention.

The Committee has further recommended a deadline for reporting data breaches, which is to be reported within 72 hours of becoming aware. Businesses now view this timeline quite stringently with no room for flexibility.

Key Recomendations

- Data Breach has been defined with the inclusion of Personal Data Breach and Non-Personal Data Breach. Similarly, Non-Personal Data Breaches are covered under the Personal Data Protection Bill 2021.
- The Personal Data Protection Bill 2021 defines "Non-Personal Data".
- All Personal Data Breaches must be reported to the DPA irrespective of the harm caused to the data principles.
- The data breaches are to be reported to the DPA within 72 hours.
- The DPA is permitted to take necessary actions in case of a Non-Personal Data Breach.
- The formation of proper guiding principles for handling data breaches is stated as follows -

1. The DPA needs to ensure the privacy of data principles while posting the details of the personal data breach.
2. The data fiduciary is to be held responsible for the harm suffered by the data principal due to any delay in reporting a personal data breach. The burden for proving the delay reasonable is on the data fiduciary.
3. The data fiduciaries are required to maintain a log of data breaches for personal and non-personal data.
4. The DPA is to maintain its discretion for authorising temporary orders and non-disclosure of details without compromising the interests of the data principal.

CHILDREN'S PERSONAL DATA

Processing of Children's Personal Data under the Personal Data Protection Bill 2019

Both Justice Srikrishna Committee and Joint Parliamentary Committee have emphasised the processing of children's personal data. The Personal Data Protection Bill 2019 states that every data fiduciary has to process any child's personal data in a manner that protects the right and is in their best interest. The verification of the child's age and the consent of the parent/guardian prior to processing the child's personal data is mandated. The 2019 Bill has empowered the DPA to classify any data fiduciary as a "Guardian Data Fiduciary" with offerings directed at children or processing large volumes of children's personal data. They are now barred from profiling, tracking, behaviourally monitoring children and their data, targeting advertisements at children or processing any personal data with an exception from obtaining the consent of the parent/guardian for the guardian data fiduciary who provides exclusive counselling or child protection services.

Observations

The Joint Parliamentary Committee has deliberated several concerns regarding the processing of children's data, including lowering the threshold and providing legally binding consent for children, fulfilling the requirement of age verification as it causes additional privacy risks along with the "right to withdrawal consent" by the child. The Committee further stated the threshold of 18 years to provide lawful consent following the age of majority in India. The Committee has expressed their concerns over the absence of any provisions that lays down the procedure of consent of the child upon attaining the age of majority.

Analysis

The legal age for entering into a contract in accordance with the Indian Contract Act 1872 to be read with the Majority Act 1875 is 18 years. The Joint Parliamentary Committee has stated the retention of the threshold for giving lawful consent under the Personal Data Protection Bill 2021. There is a need to maintain consent requirements between the age of 13 to 18 years. All data fiduciaries are now barred from profiling, tracking, behaviourally monitoring children and their data, targeting advertisements at children, or processing any personal data that can cause significant harm to the child. Businesses also have concerns in regard to the blanket ban on certain processing activities.

Key Recomendations

- Emitting the phrase "in the best interest of" and the data fiduciary is to process the personal data of a child in a way that protects the rights of a child.
- Data fiduciaries that deal explicitly with children's data have to be registered under the DPA.
- Three months prior to the child attaining the age of maturity, the data fiduciary is required to inform the child to provide consent again on the date of attaining the age of majority.
- The services being provided to the particular person are to continue unless the person opts from providing fresh consent.
- Emitting the "guardian data fiduciary" concept as a separate class that results in all data fiduciaries to now being barred from profiling, tracking, behavioural monitoring of children and their data, targetting advertisements at children, or processing any personal which can cause significant harm to the children.
- "The processing of data relating to children or provision of services to them" is to be a qualifying factor for the determination of data fiduciary, which is a significant data fiduciary under the Personal Data Protection Bill 2021.

CONCLUSION

The Joint Parliament Committee's report and the Personal Data Protection Bill 2021 are significant developments in India's Data Protection Framework Discourse. Businesses have expressed their concerns and consensus regarding the recommendations provided by the Committee.

The Personal Data Protection Bill 2021 presents several dichotomies that are required to be amended prior to it being tabled before the Parliament for being enforced in India. The 2021 Bill and the report of the Joint Parliamentary Committee portray a shift from the basic framework of the Personal Data Protection Bill 2019, which was centred around the regulation of Personal data when it ventures into the regulation of social media platforms, hardware producers, and broadens the scope of the 2021 Bill along with including non-personal data.

The 2021 Bill also stipulates that businesses will have to demonstrate the impartial algorithm or method used for processing personal data, along with not being permitted to deny a request for data portability on the grounds of it being a trade secret. The additional obligations on the business organisations have raised larger intellectual property and trade secret concerns.

CONTACT

Enterslice

EMAIL ADDRESS

info@enterslice.com

PHONE NUMBER

9870310368 | 8860712800

WEBSITE

www.https://enterslice.com/

Noida | Mumbai | Bengaluru | Chennai ***(22+ Countries Globally)***

Prepared By:
Sushree Dash
Legal Researcher | Enterslice