# DATA PROTECTION, DATA SECURITY AND PRIVACY- REGULATORY CONCERNS AND ISSUES

*Written By* ***Hemant Garg***

*Law Officer, The PSCADB Ltd, Chandigarh, India*

## WHAT IS DATA PRIVACY?

Before understanding data privacy, first, it is required to elucidate what privacy as a concept is and what sort of importance it holds under the law. Privacy which is not a new development, roots back to 1604 in the *Semayne case*[i], where it was recognised that "the house of everyone is to them as their castle and fortress." In general, it means that you cannot enter someone's home unannounced and break open the door without a warrant or notice, as that would be a violation of one's territorial privacy. Essentially, the law on trespass is also based on the essence of privacy. In further development, Justice Louis Brandeis and Boston attorney Samuel Warren propounded the term "right to privacy" in 1890, arguing that the protection of private space is a basis of contemporary individual freedom and that the law should recognise this right and impose punishment for any intrusions on it.[ii]This ideology till date exists in various data privacy legislations championing the cause of data protection all over the world. Data privacy is the branch of data management that deals with handling personal data in compliance with data protection laws, regulations, and general privacy best practices.

The necessity for data privacy emerges due to the inherent value of data, as knowledge about any entity which aids in characterising and identifying that entity. Previously, the data was used for legitimate objectives such as national security. With the development of technology, however, numerous alternative uses of data and the possibility of data as a commodity is coming to rise. As of today, the value of data has reached its all-time high and data is sometimes referred to as gold. The underlying reason is the harmony that has been created between the demand supply chain. As people have literally created their own virtual avatars on internet, no piece of information has been left private with them.

The dynamic and ever-changing structure of digitalization has driven the general populace to reveal various types of information, ranging from sensitive information such as bank credentials and government identification to inconsequential information such as skin colour and cuisine preference. With such a vast supply of data, its demand has also increased exponentially, as more information about an individual allows for a more accurate characterization of that person, which assists businesses in sending more precisely targeted advertisements and identifying trends in consumer preferences and behaviours.

## WHAT IS DATA TRADE AND HOW DOES IT WORK?

The data of an individual may be collected and sold with or without consent depending upon the local laws of their residence. After the data is collected, there are various channels of use. While some organisations may use this information for self-improvement, others may develop partnerships with similar organisations for the joint use of collective data or even sell it for financial gain. The data is not sold directly to buyers; instead, it is forwarded to data brokers and processors who categorise and analyse the data according to their many uses and purposes. These information clusters are subsequently sold to nearly all types of businesses for marketing purposes.[iii]

Owing to the magnanimous business market and the sensitivity of the commodity, there is a necessary requirement for the data privacy laws to be in place. Data privacy laws and regulations can be divided into two sub categories, first, territorial jurisdiction which sets regulations for different territories and second, industrial jurisdiction which form specific data privacy laws for specific industries. Both types deal with different issues of data that may come before them. For example, different states of Australia have different local data privacy laws depending upon the demographic and U.S.A has different data privacy laws for different industries such as Driver's Privacy Protection Act of 1994[iv] for government organizations and Cable Communications Privacy Act of 1984[v] for cable companies. One might ask why data privacy law is so dynamic, and the simple reason behind it is the ever-changing technology that these laws have to cope up with. More advanced technologies pose newer challenges to the data privacy. Therefore, there is a constant need to amend laws and counter the arising issues in this area.

## REGULATORY HISTORY

In 1980s, with increasing acceptability of globalization, the possibility of transborder flow of data also became probable. Therefore, a global need of regulation of data flow was felt. The led to the enactment of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines attempt to bring about synergy and harmonise the diverse interpretations of privacy standards that are observed in numerous jurisdictions. The fundamental privacy concepts such as the Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability were established at that time and have evolved with time in response to new requirements.[vi]

In 1995, the Directive 95/46/EC was passed for the first time by European Union (EU)[vii], which brought about a significant change in the privacy regulations. This directive established a framework for transfer/flow of personal data between EU member states, protection against unlawful processing of personal data, regulation of data processing, classification of sensitive data and its protection.

Prior to or roughly contemporaneous with the drive for codification of Directive 95/46/EC, there were other international laws, self-regulations, and privacy codes. A few are noteworthy from a relevancy standpoint and have been omitted from the extensive references above for brevity, such as the Swedish Data Act, 1973[viii], America's Fair Credit Reporting Act, 1970[ix], The Privacy Act, 1974[x], The Fair Information Privacy Principles, 1974.

In the latter quarter of the 20th century, the western nations began to address data privacy concerns. In the previous decade, these nations and organisations are regulating the same subject once again. Does this imply that the previous regulations were insufficiently comprehensive? The correct response is neither yes nor no. These requirements were among the most advanced laws at the time, however they were solely applicable to data protection concerns. Information technology has created an entire paradigm shift for data, posing emergent problems that were previously insurmountable.

## INFORMATION TECHNOLOGY, SOCIAL MEDIA AND THE DATA PRIVACY?

The advent of Information Technology had already begun in the second half of the 20th century but the spark of rapid expansion started in 1990's when social media expanded with the launch of SixDegrees.com.[xi] Soon after SixDegrees various other platforms also emerged such as LinkedIn in 2002, Facebook in 2004 and Twitter in 2006. The idea was to connect people to each other over internet. This was facilitated by smartphones which originated in the year 2000 when Ericsson released the first device marketed as a 'smartphone', combining a mobile phone, a PDA, limited web browsing and touchscreen.[xii] Along with digital illiteracy amongst masses there was also wilful ignorance among these technology giants with respect to user data privacy. In 2010, Facebook changed the default setting for user profiles from 'private' to 'public.'[xiii] Moreover, Facebook CEO Mark Zuckerberg even moved forward to state that "Privacy is no longer a social norm."[xiv] With the expansion of Information Technology, newer and newer sources of data collection unfolded. Smartphones could then track users[xv], or even know their health through smart watches with fitness features.[xvi] By the year 2015, Humans were creating 2.5 quintillion bytes of data each day.[xvii] For this reason, the present era is also known as The Age of Big Data.[xviii] Some of the latest growing technologies are future prediction of consumer's utilities and artificial intelligence. Therefore, it is clear as a crystal that the data privacy has to be actively regulated to counter emerging privacy threats.

## GLOBALLY APPLIED STRATEGIES TO COMBAT DATA BREACHES AND MAINTAINING PRIVACY

In 2016 The EU enacted the General Data Protection Regulation (GDPR) which was the biggest change in data-protection laws in more than two decades, imposing a single set of rules and tougher penalties across the EU.[xix]

Under GDPR, firms cannot legally process personally identifiable information (PII) unless they meet at least one of the six standards outlined below-

1. Explicit consent of the subject of the data

2. The processing is necessary for the fulfilment of a contract with the data subject or for the taking of steps prior to entering into a contract.
3. Processing is required to comply with a legal requirement.
4. Processing is required to safeguard the vital interests of the data subject or another individual.
5. For the fulfilment of a task in the public interest or in the exercise of official authority vested in the controller.
6. The processing is essential for the purposes of the controller's or a third party's legitimate interests, except where such interests are overridden by the data subject's interests, rights, or freedoms.

In addition, organisations that do extensive data processing or subject monitoring must also designate a Data Protection Officer (DPO) who is accountable for data governance and ensuring the organisation complies with GDPR. Legal repercussions for noncompliance with the GDPR include fines of up to 20 million euros ($24.26 million) or 4 percent of annual global turnover, which automatically ends up making data protection a significant compliance for these corporation, which come under the purview of GDPR. In addition, the individual in this capacity is responsible for ensuring the maintenance of personal data adheres to applicable data protection principles.[xx]

GDPR also provides for rights to data subjects providing a more accepting and peaceful ecosystem for individual's privacy. These rights include a Right to be forgotten wherein the individuals can request that their PII be deleted from a company's storage system. The corporation is permitted to deny requests provided it can successfully demonstrate a legal justification for doing so. Other rights include a right to access personal data, right to object on giving personal data A data subject may deny a business permission to use or process his or her personal information, right to port the personal data among many others. GDPR has able to permeate the data protection requirements to an extent that, as of today there are numerous countries that are following the GDPR guidelines or have incorporated the principles under GDPR into their local legislation or they could be part of European Union but still following it with changes, such as Norway. Norwegian data protection is governed by the Law on the Processing of Personal Data (Personal Data Act) of 15 June 2018 ('the Act')[xxi], which implements the General Data Protection Regulation. The Act and Regulation 0563/2018 on the

Processing of Personal Data[xxii]contains certain specific national variations and additions to the GDPR. The Norwegian data protection authority ('Datatilsynet') enforces data protection law.

The European Union countries have performed outstandingly owing to GDPR. Other than these, there are few other countries which have strong data privacy regulations which are up to the standards of GDPR and such countries include include Australia, Canada and Japan.

The privacy and protection of data in Australia are governed by a combination of federal, state, and territory laws. The Privacy Act of 1988 and the Australian Privacy Principles ("APPs") incorporated in the Privacy Act are among the federal legislation. The Privacy Act regulates how relevant entities handle personal information, and the Privacy Commissioner has the authority, under the Privacy Act, to conduct investigations, including own-motion investigations, to enforce the Privacy Act and to seek civil penalties for serious and egregious breaches or for repeated breaches of the APPs where an entity has failed to implement remedial efforts. The majority of Australian States and Territories, with the exception of Western Australia and South Australia, have their own data privacy legislation applicable to State or Territory government agencies and private firms that interact with State or Territory government agencies. Australia has also approved the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the "AA Act"), which provides law enforcement agencies access to encrypted data for the investigation of severe crimes and imposes requirements on "Designated Communications Providers."

Similarly, Canada governs the data privacy through its enactment, Personal Information Protection and Electronic Documents Act 2000 ('PIPEDA')[xxiii]. It also has state laws for micro-governance. Although these laws are in consonance with the principles provided under GDPR and has a similar outline, it does have some exceptional features that makes it stand out such as provisions relating to data retention and data of a child. The PIPEDA requires that personal information be kept only as long as necessary to fulfil the purposes for which it was collected, after which it must be securely destroyed, erased, or rendered anonymous. As there is no "one-size-fits-all" retention period, determining the appropriate retention period can be complicated in certain circumstances, but each case is viewed from a fresh perspective.

Japan, whose data privacy law is also in consonance with GDPR has taken steps in distinguishing between different types of data. The Act on the Protection of Personal Information (APPI)[xxiv] was one of the earliest data protection regulations in Asia when it was

adopted in 2003. In September 2015, a series of high-profile data breaches rattled Japan, and it became clear that APPI's criteria no longer fit contemporary needs. The modified APPI went into effect on May 30, 2017, a year before the EU General Data Protection Regulation (GDPR). APPI distinguishes between two categories of protected data: personal information and personal information requiring *"special care."* The first category includes personally identifiable information (PII) such as name, date of birth, email address, and biometric data. The 2017 update to the APPI clarified that personal data also includes numeric references that can be used to uniquely identify an individual, such as driver's licence or passport numbers.

## WHAT IS THE POSITION OF DATA PRIVACY LAW IN INDIA?

The IT Act[xxv] was enacted primarily to meet the needs of the Indian outsourcing industry and to prevent data thefts and misuse as they arose in an industry that dealt with the personal data of customers residing in countries with stringent data protection regulations. As we are moving towards a digital economy and there is an increase in government measures focusing on personal information of citizens for purportedly percolating benefits, advancing national security interests versus privacy concerns/risks, the IT Act is becoming insufficiently comprehensive in all privacy dimensions. Personal data of individuals have become a tradable commodity for brokers/dealers in the economy, as the digital economy is gaining momentum and individuals' data is frequently used for business operations across all industries. This has created a need to regulate the flow of data and the level of trust between those whose data is at risk and those who decide what to do with it. Therefore, a robust legal framework is required to, among other things, regulate the cross-border transfer of personal data of Indian residents and provide individuals with rights and remedies for the protection of their rights. In order to have a comprehensive data protection statute, the legislature has enacted the Personal Data Protection Bill, 2018 (PDPB) and is currently working on the 2019 version, which has been heavily influenced by the GDPR.

PDPB has been criticized for not addressing the requirements of the country's changing technology landscape comprehensively[xxvi]. Concerns have been raised by corporations regarding the inclusion of non-personal data, the treatment of social media as publishers, and the structure of the Data Protection Bill.[xxvii] It would also alleviate fears that current laws may harm the nation's nascent technology and start-up sector, which has seen a record 42 unicorns

founded in the past year.[xxviii] Due to the fact that the bill was drafted by a Joint Committee of Parliament, the government can only make minor changes to the provisions and cannot completely alter them. The only way to address its flaws would be to completely scrap it and introduce new legislation.[xxix] Although, the government officials have notified that there is possibility of changes in the bill, they still remain to be speculations.[xxx]

Due to the data localization provisions of the Data Protection Bill, the Ministry of Electronics and Information Technology (MeitY) released the dratt Data Centre Policy ("the Policy") for the development of Data Centre infrastructure within India in November 2020. The Policy emphasises its vision to make India a Global Data Centre hub, promote investment in the sector, propel digital economy growth, enable provision of trusted hosting infrastructure to meet the country's growing demand, and facilitate delivery of state-of-the-art services to citizens.

The Policy describes growth strategies for the Data Centre Sector (DCS). It proposes that DCS be granted "Infrastructure Status" so that it can obtain long-term credit from lenders on more favourable terms. It proposes establishing a Data Centre Incentive Scheme (DCIS) that will, among other things, outline fiscal and non-fiscal incentives for DCS. In addition, it proposes the establishment of specific zones known as Data Centre parks (i.e. secure Data Zones to meet the high demand for data storage, networking, and the provision of a variety of data-related services) with the necessary infrastructure, such as electricity, water, etc.

To foster an environment conducive to the efficient operation of DCS, the Policy identifies key areas of emphasis, such as the provision of better infrastructure, such as a quality, uninterrupted, and long-term power supply, the installation of power generation units in Data Centre Parks, the use of renewable energy, etc. It indicates that MeitY and the Department of Telecommunications would facilitate robust and cost-effective connectivity backhaul by providing utility corridors for Optical Fibre Cables, dark fibre, and other similar technologies. It suggests enabling a Dial Before You Dig Policy to "allow easy access to information about the underlying network infrastructure" and improving international connectivity, which "will be a key driver...for Data Centre investments by global players." The bill also proposes a single-window clearance system for the establishment of data centres and the designation of data centres as "Essential Service" under the Essential Services Maintenance Act of 1968 in order to ensure the continuation of services. It emphasises the need to create a separate category code for data centre buildings in the 2016 National Building Code.[xxxi]

The Policy proposes the establishment of Data Centre Economic Zones, which would consist of Hyper-scale Data Centers, Cloud Service Providers, IT companies, R&D units, etc. It proposes the establishment of the Inter-Ministerial Empowered Committee (IMEC), a decision-making body within the DCS, the Data Centre Facilitation Unit under IMEC to oversee the implementation of various measures and initiatives, and the Data Centre Industry Council to serve as a liaison between the DCS and the government.

## WHAT IS THE WAY FORWARD?

In order to completely eradicate the downfalls of Personal Data Protection Bill, a new bill will have to be introduced, completely scrapping the present bill. In case, it is redeveloped, the government must take the recommendations from all stakeholders. It is important because of India's unique position in growing IT sector. A balance between individual privacy and free business has to be created in order to prosper in the digital era. The Indian legislature should also take into account the present legislations around the globe to determine the best practices and apply them domestically the way its deems fit. Some of the noteworthy regulatory methods which can play a pivotal role in India's own data privacy policy are stated as follows-

- Canada has recognized the requirement of separate regulations for different types of data subjects. They are moving forward to treat children as different type of data subjects. In India, majority population is the youth, and therefore there can be a different set of guidelines that could be introduced for them.
- Australia has successfully implemented multiple regulations at federal level as well as at state level. Moreover, they have also separate regulations for different industries. This has helped in resolving issues typical to particular industry or demography which finally has resulted in effective governance.
- European Union has implemented a regulatory method opposite to Australia. They have clubbed all issues of data privacy in a single document while effectively addressing all the issues. This is alignment of Indian legislatures consolidation motive to tackle data privacy law.
- Japan has categorized types of data in a manner to protect data subjects from even remote danger to privacy. India's present bill has been criticized specifically for a faulty

definition of data so as to even include non-personal data. Japan's categorization of data can be incorporated in order to resolve this issue.

Data is gold and India is the biggest mine. India is only second to China in terms of population and given the fact that China does not have free internet, India is the undisputedly biggest hub of data. India is comparatively very new to the digital world but its potential growth rate is exponential. India has more than 300 million internet users while only 30 percent of the population is participating on Internet and these are reasons enough to compel India to enact the most unique, advanced regulation with an equilibrium between economic growth and social justice.

## ENDNOTES

[i] *Peter Semayne v Richard Gresham* [2006] 77 ER 194
[ii] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy', Harvard Law Review Vol. IV No. 5.
[iii] Usercentrics, 'Data is the new gold – how and why it is collected and sold' (*Usercentrics*, 21 October 2021) <https://usercentrics.com/knowledge-hub/data-is-the-new-gold-how-and-why-it-is-collected-and-sold/#:~:text=Your%20internet%20activity%20and%20data,of%20the%20modern%20digital%20economy.>accessed 7 May 2022
[iv] Driver's Privacy Protection Act 1994, 18 U.S. Code 2721 et seq
[v] Communications Privacy Protection Act 1984, 47 U.S. Code 551
[vi] OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', < https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 7 July 2022
[vii] The European Union and The Council of the European Union, 'Directive 95/46/EC' [1995] Official Journal L 281, P. 0031 - 0050
[viii] Swedish Data Act 1973 Datalag (1973:289)

[ix] Fair Credit Reporting Act 1973 15 U.S.C 1681
[x] The Privacy Act 1974 5 U.S.C. § 552a
[xi] The Economic Times, '7 social media sites that failed to become 'Facebook'', < https://economictimes.indiatimes.com/tech/internet/7-social-media-sites-that-failed-to-become-a-facebook/all-you-need-is-app/slideshow/58881474.cms > accessed 7 July 2022
[xii]Adam Pothitos, 'The History of the Smartphone', Mobile Industry Review, October 31, 2016
[xiii] Sarah Perez, 'The 3 Facebook Settings Every User Should Check Now',The New York Times, January 20, 2010
[xiv] Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder', The Gaurdian, January 11, 2010
[xv] Charles Arthur, 'iPhone keeps record of everywhere you go', The Guardian, April 20, 2011
[xvi] Joe Svetlik, '2014: Wearable tech review of the year', , https://www.wareable.com/wearable-tech/2014-the-wearable-tech-review-of-the-year> accessed 8 July 2022
[xvii] James Connington, 'It's time to make sure research is understandable to all',The Telegraph, July 27, 2015
[xviii] Steve Lohr, 'The Age of Big Data', The New York Times, Feb. 11, 2012
[xix] General Data Protection Regulation [2016] OJ L 119
[xx] Luther., 'Unzulässige Videoüberwachung - LfD Niedersachsen verhängt Bußgeld von mehr als EUR 10 Mio. gegen notebooksbilliger.de' < https://www.luther-lawfirm.com/newsroom/blog/detail/unzulaessige-videoueberwachung-lfd-niedersachsen-verhaengt-bussgeld-von-mehr-als-10-mio-euro-gegen-notebooksbilligerde#:~:text=gegen%20notebooksbilliger.de,-

Hintergrund&text=Die%20Landesbeauftragte%20f%C3%BCr%20den%20Datenschutz,verh%C3%A4ngt%20hat. >accessed 8 July 2022

[xxi] Law on the Processing of Personal Data (Personal Data Act) 2018 (EU) 2016/679

[xxii] Processing of Personal Data Act 0563/2018

[xxiii] Personal Information Protection and Electronic Documents Act 2000 S.C., c. 5

[xxiv] The Act on the Protection of Personal Information 2005, Act No. 119 of 2003

[xxv] Information Technology Act 2000, Act No. 21 of 2000

[xxvi] Personal Data Protection Bill 2018, Bill No. 373 of 2019

[xxvii] Surbhi Agrawal, 'Fresh legislation may replace Data Protection Bill', The Economic Times, 17 February 2022

[xxviii] Asit Ranjan Mishra, 'India's personal data protection bill may threaten innovation, growth: USTR', Business Standard, 29 April 2022

[xxix] *ibid*

[xxx] Tech Desk, 'Non-Personal Data May be Removed from Personal Data Protection Bill: Report', <https://www.news18.com/news/tech/non-personal-data-may-be-removed-from-personal-data-protection-bill-report-5412895.html> accessed 8 July 2022

[xxxi] Sri Lekha,' Summary: Draft Data Centre Policy 2020 (MeitY)

',<https://www.algindia.com/summary-draft-data-centre-policy-2020-meity/> accessed 8 July 2022