ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Landscape of Data Privacy Legislation in India

Technology, Privacy, and eCommerce


1234 5678
995 1312
865 783
420 1785
380
1573
1688
572
1208
2326
3267
2065


CreditCard
1234 5678
995 1312
865 783
1573
1688
572
1208

CHEAT SHEET

- ***A relatively new phenomenon.*** While the right to privacy has been long recognized as part of the constitutionally guaranteed fundamental rights in India, the data protection bug bit India largely due to the huge outsourcing business that India has seen in the last two decades.
- ***Two contrasting models.*** The European model for data privacy, the 1995 EU Directive, is compared with the 2008 Indian Parliament Amendments to the IT Act.
- ***Best practices.*** Comply with the Indian data privacy amendments by obtaining consent from data subjects over disposal and usage of sensitive data, most safely in writing, and appoint a grievance officer to manage such queries.

The idea of data protection of individuals' personal information started to take hold beginning in the 1970s, signifying a new type of protection compared to the earlier treatment of the issue through the concept of personality rights. Legislators and world leaders realized the need to establish this concept separately from private rights. However, when the time came for these governments to implement the concept, countries differed widely in the approaches that they took to data protection.

History of data protection legislative efforts

In the United States, the idea of a National Data Centre was envisaged that would register the data of all individuals and improve the public information system. However, this idea failed due to strong opposition by the US Congress. Congress believed that each individual thinks differently and therefore establishing such a National Data Centre would be infringing on the individual's rights. Thus, the United States preferred a sectoral approach to data protection relying on a combination of legislation, regulation and self-regulation, rather than overarching governmental regulations. The European Union in contrast believed in an overarching framework of data protection directives that would permeate into the provisions of the national laws of the various member states in the European Union.

The EU Data protection directive of 1995 and the German constitutional ruling on *'informational self-determination'* are largely credited with the data protection legislations that were passed in a majority of the European nations.

While the right to privacy has been long recognized as part of the constitutionally guaranteed fundamental rights in India, the data protection bug bit India largely due to the huge outsourcing business that India has seen in the last two decades. With growing concerns over the data protection framework in India, inter alia, to sustain the outsourcing business opportunities the legislature attempted to address these concerns by introducing amendments to the Information Technology Act, 2000 ("IT Act") and implementing the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("IT Rules").

Rationale and need for data protection legislation

Data protection is not prohibitive in nature. On the contrary, data protection legislation presupposes

that possession, handling and processing of personal data is legal. What data protection legislation attempts to do is construct a system of checks and balances that will prevent the abuse of the power granted to the data controller. The main goals of data protection are to provide various procedural safeguards that protect individuals' privacy, promote accountability and eliminate abusive record holding practices.

With the growth of e-governance, citizens will be forced to interact electronically with the government on a larger scale. This could potentially lead to a lack of privacy for civilians as their government obtains more and more information on them. Therefore, the rationale behind data protection in the public sector is the possibility that public authorities can easily misuse personal data and by having a sound legal framework in place, an initiative such as e-governance can do more good than harm. Due to the EU Directive, databases such as EURODAC[1] are viewed as low risk as the data contained in these databases are regulated by adequate procedural safeguards.

1 EURODAC is a database containing the fingerprints of all asylum applicants and all persons apprehended while irregularly crossing borders.

The concerns on data protection were also echoed when the issue was discussed in relation to the private sector. Legislators believed that the private sector is no different from the public sector and also has adequate opportunities to collect, store, process and transmit personal data. Due to outsourcing practices today, employees of service providers have access to extensive personal data about consumers and end user clients. This includes credit card numbers, social security numbers, driver's license numbers, dates of birth, medical records and other important personal information that has the potential for misuse.

The world has seen an exponential growth in social networking websites. While such networking websites are a boon in bringing the world and its people and cultures closer together, they too need to be regulated by appropriate data protection legislation.

Companies across the world outsource a significant amount of business to India, which includes a sizeable amount of personal data. The concerns such companies face are that they have a duty to shield their customers from the possibility that employees of foreign-service providers may misuse their personal data. Such concerns of US companies can be allayed with appropriate data protection legislations in India. It is in this context that the amendments to the IT Act and the IT Rules were introduced.

EU directive on data protection

It is important for the reader to note that this Part III of the article is not meant to be an in-depth analysis of the Directive, instead it is only a high-level view to compare the Directive to the Indian legislation on data privacy, which is captured in more detail in Part V below.

The EU Directive ("Directive")[2] was adopted by the European Parliament and Council on 24 October, 1995, with the twin objectives of protecting personal data and facilitating free movement of data. The EU directive is a result of Article 8 of the European Convention on Human Rights, which deals with the issue of *"Right to Privacy."*

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The salient features of the Directive are:

It applies to the processing of personal data in the electronic and non-electronic medium.
It clearly defines personal data thereby eliminating any ambiguity on the kind of information to which the principles of the Directive are applicable.
For the purposes of data protection, there are only four relevant parties, the (i) data controller; (ii) data processor; (iii) third parties; and (iv) data subject(s).
Procedural safeguards are mandated on the data controller, where the data controller must implement appropriate technical and organizational measures to protect the integrity of personal data.
The data controller and processor are permitted to access, use and process personal data in accordance with identified principles, such as the *'Openness Principle', 'Purpose Specification Principle', 'Individual Participation Principle', 'Accountability Principle'.*
The data subject is entitled to claim damages for unlawful processing of personal data by the data controller. A data controller can disclaim liability only if the abovementioned damages occurred due to no fault or responsibility of the data controller.
Transfer of personal data by the data controller outside the country of collection is permissible as long as applicable data transfer agreements are signed, for this purpose, between the data controller and data subject.

Indian data privacy landscape, amendments to the IT Act and the IT Rules ("Indian DP amendments")

In India, the Parliament deemed it necessary to implement a law that regulates the manner in which personal data is collected and used and consequently certain amendments to the IT Act were enacted by both houses of Indian Parliament on 23 December, 2008. These amendments came into effect on 27 October, 2009.

The amendments to the IT Act introduced two sections dealing with the concept of data protection, namely, Sections 43A and 72A. The IT Rules were then introduced on 11 April, 2011 pursuant to Section 43A.

Section 43A and IT rules:

Section 43A of the IT Act requires that any 'body corporate'[3] which possesses, deals or handles *'sensitive personal data or information'* through a computer resource owned, operated or controlled by it, maintain and implement *'reasonable security practices and procedures'* to protect such information.

3 The term "body corporate" has been defined in the IT Act to mean "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities."

If we break down this Section into parts, it can be understood as follows:

Body corporates and computer resources – this is applicable to bodies corporate; in relation to computer resources that they own, control or operate. Therefore, in the context of organizations, this Section is mostly applicable to (1) employee or client data stored or handled by it; (2) data accessed or processed during BPO operations and data received in Cloud offerings.

Security procedures and practices – a corporate body is required to implement reasonable security procedures and practices. The IT Rules prescribe certain of these practices, such as the publication of a privacy policy, obtaining consent for the collection, storage and transfer of Information, providing the person whose data is collected the ability to review and amend such data and the appointment of a grievance officer. The IT Rules also require the body corporate to maintain adequate security measures to safeguard such data and recognize ISO 27001 or equivalent standards as some of the standards that it deems sufficient.
Wrongful loss or wrongful gain to any person – the negligence of the corporate body to implement the reasonable security procedures and practices should result in harm to the data subject in order for the corporate body to be liable under this Section.
Electronic medium – the personal data covered by this Section relates to such personal data shared in the electronic mode only. Therefore personal data shared in a non-electronic medium, such as documents, are not covered by this Section and its protections.
Sensitive personal information – only sensitive personal information is covered by this Section. Under the IT Rules, *'sensitive personal information'* includes passwords, financial information, health information and medical records, sexual orientation, biometric information and any information received by body corporates relating to the above. Therefore personal data outside the scope of *'sensitive personal information'* is not covered by this Section and its protections.
Civil sanctions – under this Section it mandates only civil sanctions and penalties.

Section 72A and IT rules

If we break down this Section into its parts, it can be understood as follows:

- **Lawful contract** – there needs to be a lawful contract pursuant to which personal data is shared by the data subject to the data controller.
- **Intent to cause wrongful loss or gain** – this Section supposes that *'mens rea'* or an intention to commit wrongful loss or gain must mandated by this Section.
- **Personal information** – this Section relates to *'personal information'*, and the scope of *'personal information'* has not been elaborated unlike Section 43A and the associated Rules, where the Rules relating to Section 43A details the scope of *'sensitive personal information'.*
- **Electronic and other mediums** – unlike Section 43A this Section does not delve into the medium of storage. Therefore 'personal information' shared in both electronic and non-electronic mediums are covered by this Section. However, it is interesting to note that while Section 72A does cover both mediums, the IT Act is designed to regulate virtual data and electronic communications. Therefore the IT Act contemplates non-electronic mediums for this Section when the Act in itself is not designed to regulate the legal framework for non-electronic mediums.
- **Criminal sanctions** – this Section imposes imprisonment along with civil sanctions for contravention of the provisions under this Section.

Comparison between the Directive and the Indian DP amendments

While there are inherent differences between the Directive and the Indian DP amendments, it is important to note that the Directive has been in force longer than the Indian DP amendments and has been tested in courts of law across the EU member states, to eliminate ambiguity. Because the Indian DP amendments are more recent and have yet to be tested in court, it is difficult to truly understand the scope and impact of the Indian DP amendments.

The broad differences between the Directive and the Indian DP amendments are listed below for the reader's consideration:

ISSUE	**DIRECTIVE**	INDIAN DP AMENDMENTS
Scope of personal data	The Directive clearly defines the scope of the 'personal data' to avoid ambiguity on the nature of information being covered by the Directive.	• Under Section 43A and the Rules, 'sensitive personal information' has been detailed to eliminate ambiguity whereas the scope of Section 72A is broader in comparison. • Section 72A is likely an attempt by the Indian legislature to ensure all personal data shared by data subjects is protected. • However with such broad scope the possibilities of misuse or over-scrutiny increases.
Principles	The Directive has fundamental principles (detailed in Section III above) as the basis on which the Directive and its scope are structured. This is the reason the Directive is clear in its application and enforcement.	The Indian DP amendments do not have clear and defined principles on which the legislation is structured.
Dedicated legislation	The Directive was designed specifically to protect collection, utilization, retention and disposal of personal data. Therefore, these set of principles have withstood the test of time and been adopted across European nations via national legislations.	The Indian DP amendment was an attempt by the Indian legislators to ensure there is statutory coverage for personal data and data subjects have some form of protection.
Data controller and data processor	The Directive clearly identifies the roles of *'data controllers'* and *'data processors',* to ensure the responsibilities of the parties collecting and processing personal data is clearly defined.	The Indian DP amendments do not bring out distinctions in these roles. Please see best practices point below to understand how to mitigate the lack of clarity on this issue from an Indian perspective.

Best practices in India

- **Disposal** – the Indian DP amendments do not delve into the mode of disposal of personal data. Therefore, it is advisable for data controllers and data processors, especially Indian organizations dealing with employee and client personal data, to receive consent, in writing, from the data subjects on the mode of disposal of their personal data. Further, under the Indian DP amendments the consent needs to be secured by the data controller for the entire duration for which the personal data shall be accessed and used.
- **Form of consent** – The Indian DP amendments require that consent be obtained from the data subject for various activities that the data may be subject to. As a practical matter, it is

often extremely difficult to return to the data subject on numerous occasions to obtain such consent. It would therefore be advisable that the consent obtained covers as many activities as possible.

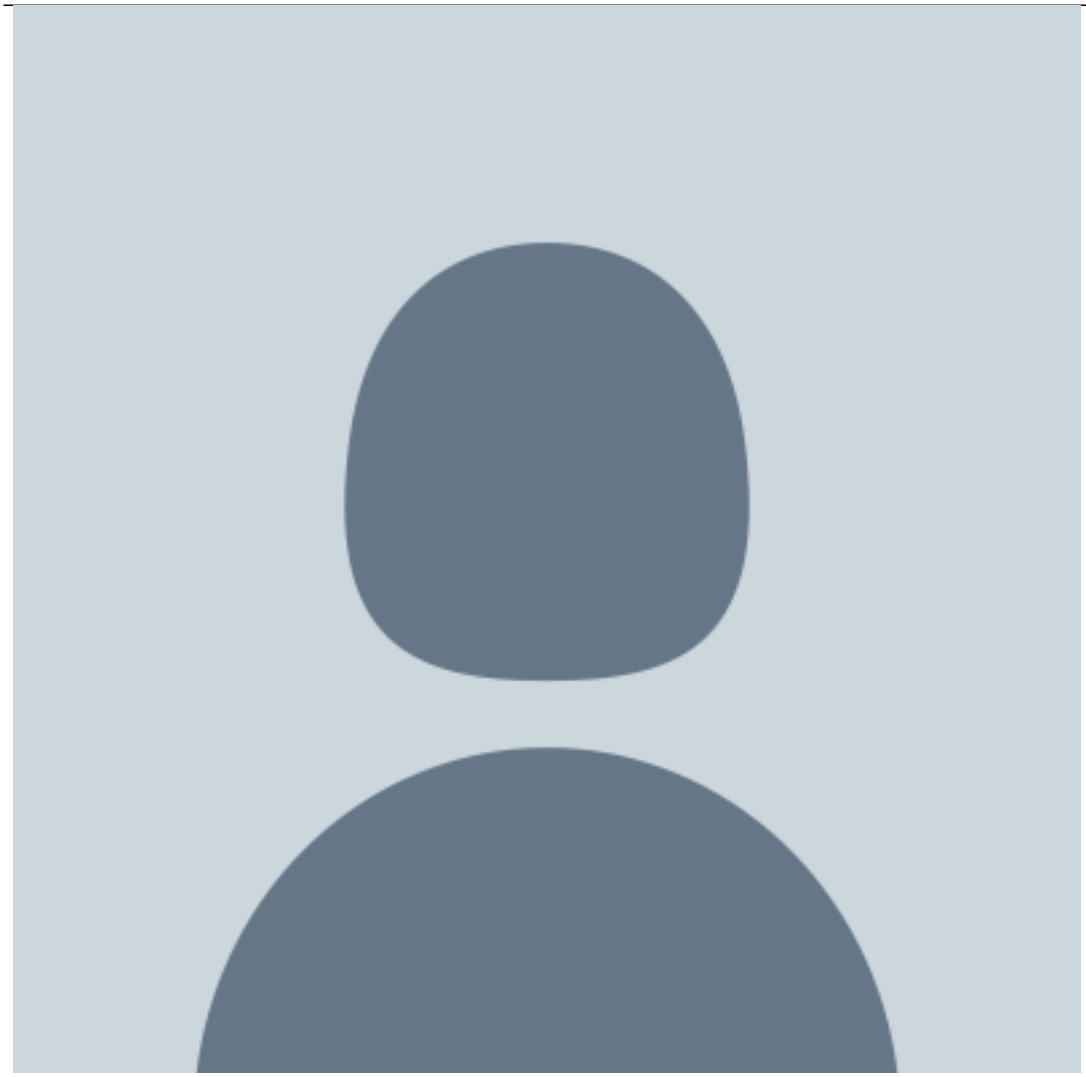
- **Mode of consent** – the Indian DP amendments contemplates consent from the data subject in written form. The practical difficulty faced by this mode of consent is for the BPO and call centers industry. These organizations often record consent in telephonic conversations and therefore applying the Indian DP amendments strictly, this form of consent recorded by these industries may not be strictly in line with the legislation. The clarifications issued by the government however states that the consent may be obtained by any mode of electronic communication.
- **Grievance officer** – the Rules require a *'Grievance Officer'* to be appointed by each organization to manage queries from data subjects. There are no other details around the *'Grievance Officer'* to truly understand the scope of this position.
- It is advisable for each organization to have a privacy office. Secondly, organizations should formalize the appointments of the 'Grievance Officer' via board resolutions, where such position reports into key managerial personnel[4] of the organization. The Indian Companies Act permits such appointments to be formalized by the board in circular mode, i.e., the board need not meet physically to record the consensus of all board members toward the appointment.
- **Data controller and data processor** – The Indian DP amendments do not specifically define a *'data controller'* and *'data processor'*. The Directive has clearly outlined the scope and responsibilities of these roles and captured the associated liabilities of the *'data controller'* and *'data processor'*. Therefore, it is advisable for Indian organizations to carve out the responsibilities and liabilities as either *'data controllers'* or *'data processors'* as the case maybe when dealing with employees, clients or third parties in the applicable contract with such persons or entities.

4 Key Managerial Personnel are those officers holding positions of CEO/Managing Director, CFO and Company Secretary under the Indian Companies Act.

Conclusion

The Indian DP amendments were a step in the right direction by the Indian legislators to ensure that personal data in India has statutory coverage and the rights of data subjects are adequately protected. However, the IT Act is not the vehicle to introduce this area of data protection law within India. The IT Act is a piece of legislation designed to regulate the virtual world and data privacy has its inherent complexities and nuances that means the IT Act should not also serve as a data protection law. There is a privacy bill pending within the Indian Parliament. Perhaps when this bill becomes law or if the legislature consolidates the bill with the existing Indian DP amendments, then India will have a dedicated data privacy law that captures the concepts set forth in the Directive and its principles while keeping in mind the unique context of India.

Abhijit Poonja

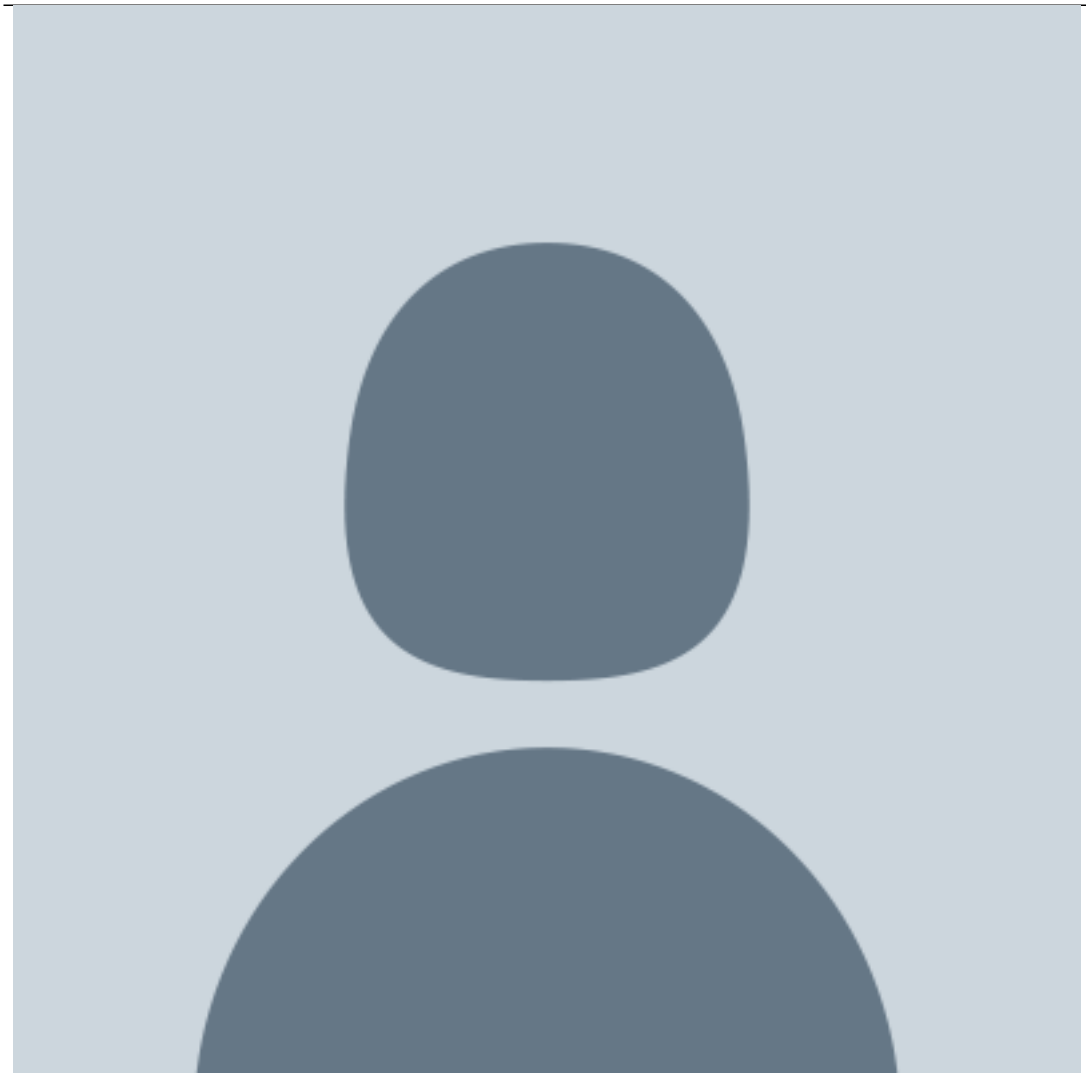


Lead Legal

EdgeVerve

He manages the global legal practice at EdgeVerve, an Infosys company. He has been with Infosys for the last six years. Prior to that, he worked at Trilegal, a top corporate law firm in India. He is also an alumnus of University Law College in Bangalore.

Anind Thomas



Partner

AZB & Partners in Bangalore, India