GDPR and India

By **ADITI CHATURVEDI**
Edited by **AMBER SINHA**

The Centre for Internet and Society, India

Designed by **Saumyaa Naidu**

At present, companies world over are in the process of assessing the impact that EU General Data Protection Regulations ("GDPR") will have on their businesses. High administrative fines in case of non-compliance with GDPR provisions are a driving force behind these concerns as they can lead to loss of business for various countries such as India.

India has had a peculiar economic structural transition.[1] Economic Survey reveals a top down structure of economy with 66.1% contribution of services sector to GDP. Out of this, information technology – business process management (IT-BPM) sector "is expected to touch an estimated share of 9.5% of GDP and more than 45 per cent in total services exports in 2015-2016 as per NASSCOM.[2]" Revenue contribution of Exports in IT-BPM is expected to touch 108 billion US dollars with a comparatively less domestic contribution of 22 billion dollar.[3] "Major markets for IT software and services exports are the U.S. and the U.K. and Europe, accounting for about 90 per cent of total IT/ITeS exports"[4] According to NASSCOM estimates for 2014, UK and Continental Europe respectively accounted for 17.4% and 11.6% of India's IT/ITES services export.[5]

Given the criticality of IT–BMP services, India must do all it can to protect and promote business in this sector. To a large extent, future of business will depend on how well India responds to the changing regulatory changes unfolding globally. India will have to assess her preparedness and make convincing changes to retain the status as a dependable processing destination.

This document gives a brief overview of data protection provisions of the Information Technology Act, 2000 followed by a comparative analysis of the key provisions of GDPR and Information Technology Act and the Rules notified under it.

Information Technology Act, 2000

The relevant Indian laws governing online data protection are the Information Technology Act, 2000 (IT Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The IT Act was enacted to give "legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication."[6]It provides for civil liability and criminal liability under Chapter IX and Chapter XI respectively. Section 43 under Chapter IX of the Act covers penalty and compensation in case of unauthorized access or damage to computer, computer system or network. This section is important for establishing criminal liability under Section 66 of Chapter XI.

In 2009, S.43A was inserted by way of an amendment as a result of "pressure from domestic and international IT industry" and to keep up with stringent data protection laws prevailing in Europe as "this was adversely affecting outsourcing".[7] Subsequently, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data

---

1 Three-sector theory has been modified in India. Instead of progressing from Primary to Secondary sector, India transitioned from primary to tertiary in terms of contribution to GDP. Manufacturing sector which is the secondary sector has been largely bypassed.

2 Pg.168, Economic Survey 2015-2016

3 Pg.167, Economic Survey 2015-2016

4 Indian Services Sector: Poised for global ascendancy, KPMG-CII, Source 3, 4, 5 NASSCOM Strategic Review 2015, NASSCOM, Pg. 13, April 2016

5 CRISIL Opinion, Why India will gain as economic recovery in US and EU gains momentum, July 2014, CRISIL Research

6 The Information Technology Act, 2000

7 Pg.189, Chapter 8, Data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

or Information) Rules, 2011 under S.43A were notified to provide further clarity. The 2009 amendment brought "body corporates" within the compensation mechanism for failing to protect "*sensitive personal* data or *information*" owned, controlled or operated by it. Subsequently, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act were notified. This section "is clearly intended to impose liability on ITES/BPO and other outsourcing service providers and for this reason, refers to body corporates and excludes natural persons and most public entities from its preview."[8]

Brief Comparison of Information Technology Act, 2000 and GDPR

This section brings out the similarity and difference between key features of the GDPR and the IT Act. A brief overview of the notable features of these data protection legislations has also been given.

The following table presents key highlights of the similarities and differences described below:

Principle	Section and Article	Similarity	Difference
Objective		Data transfer for electronic commerce	GDPR specifically confers protection to natural persons and their rights and freedom upon data processing. This is not expressed in the IT Act.
Principles of processing and collection of data	Art.5 of GDPR[9] Rule 5 of IT Rules, 2011[10]	Both laws require that: Collection of data should be for lawful purpose. Collection should be necessary for the purpose specified.	The principles given in GDPR apply in relation to data processing. On the other hand, the principles under IT Act apply to collection of information and use. It does not mentioned processing. Principles listed in the GDPR but not mentioned in IT Act are data integrity, protection from unlawful processing, accountability, fairness and transparency.

8 Pg.32, Chapter 2, Data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

9 EU General Data Protection Regulations (GDPR)

10 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

11 Rule 6 of IT Rules, 2011 mentions "Provider of the sensitive personal data or information"

12 Mentioned in Art.6 of GDPR

Lawfulness of processing	Art.6 of GDPR Rule 5 of IT Rules, 2011	Consent of provider of information[11] or the data subject[12] is a prerequisite for the purpose of collection of information and for processing under IT Rules and GDPR respectively.	Unlike the GDPR, the IT Act does not have a provision that specifically deals with "lawfulness" of processing. GDPR lists five additional conditions on necessity of processing and also confers upon the Member States the power to introduce specific requirements for processing. Similar conditions are not mandated under the IT Act.
Consent	Art.4, 8 of GDPR	Under both laws: i. Consent prior to data collection is needed ii. The provider has the option to withdraw consent	Unlike GDPR, the IT Act does not: i. Define consent ii. List special conditions for child's consent iii. Require demonstration of consent by the data controller.
Sensitive personal data	Art.9 of GDPR Sec.43A of the IT Act, 2000 and Rule 3 of IT Rules, 2011	Both laws include biometric data, health records and sexual orientation in the list of sensitive data.	GDPR and IT Act lay down additional categories of sensitive personal data that are not common to the two laws.
Rights	Art.(14 -18), Art.(20 - 22) and Art.7(3) of GDPR Rule 5(6), Rule 5(3), Rule 5 (7) of IT Rules, 2011	Some rules under Sec.43A of the IT Act loosely correspond to the rights under GDPR. These are: Right to rectification, Right to be informed and the Right to withdraw consent.	Unlike the GDPR, IT Act does not use the word "Right". IT Act excludes reference to some important rights given in GDPR. These are Right of access, Right to restrict processing, Right to data portability, Right to object, Right to erasure, Right in relation to automated decision making and profiling. The Rights have been described in considerable details in GDPR. On the contrary, the IT Act gives a vague description of some of these rights.

Security and Accountability	Art.32, 35, 37, 30, 33 of GDPR Rule 4 of IT Rules, 2011	Common data protection security practices include adoption of internal policies, security audit, adherence to voluntary code of conduct and certification mechanism.	GDPR consists of additional and elaborate measures for security of data processing. These include appointing a data security officer, conducting privacy impact assessment, maintenance of records of processing
Compensation and Liability			
Compensation for damages	Art.82, Art.82(2) of GDPR Sec.43A of IT Act, 2000 and Rule 8(1) of IT Rules, 2011.	Both contain provisions that award compensation from damages arising due to infringement. Both contain exemption from liability under certain conditions.	Compensation is a right under the GDPR but not under the IT Act. Different mechanisms and procedures, for claiming compensation, have been given under the two laws.
Punishment for disclosure of information	Art.83 of GDPR Sec.72A of IT Act, 2000	Both provide a provision for fines in case of breach.	GDPR imposes civil liability only. IT Act imposes criminal liability also.
Redress	Art.77, 78, 79, 82 of GDPR Rule 5(9) of IT Act, 2000 Sec.72A of IT Act, 2000	Both laws provider redress mechanisms.	Redress is a matter of right under GDPR but not under IT Act. The laws prescribe different redress procedures. There is ambiguity regarding authority that can be approached under IT Act, 2000.
Data transfer	Art.(44 - 50) of GDPR Rule 7 of IT Act, 2000	Both laws obligate that data transfers will be allowed only if the receiving party offers same level of data protection.	GDPR covers data transfers to international organisations as well. IT Act does not specifically mention international organisations. As compared to the IT Act, GDPR lists many more parameters for valid data transfer such adequacy decision, appropriate safeguards, derogations and judgement of a court of third country.

Objectives

The three objectives mentioned in the GDPR are; protection of natural persons when their data is processed, protection of their fundamental rights and freedoms with respect to data protection and freedom of movement of personal data for processing purpose. The Regulation confers protection to data subject as a matter of right. Further, it explicitly recognizes the Charter on Fundamental right of European Union and data protection rights conferred by the Treaty on Functioning of the European Union.

The objective of the Information Technology Act and Rules under Sec.43A is to provide a model law to facilitate e-commerce in a safe and secure manner.

Similarity

Both laws intend to facilitate transfer of data for the benefit of electronic commerce.

Difference

Facilitation of data transfer for commercial purpose is not the only objective of GDPR. The law goes further by conferring protection to natural persons when their data is processed and by securing their privacy rights and freedom.

On the other hand, protection of privacy rights or protection of natural person during processing of data have not been stated in the objectives of the IT Act.

Additionally, GDPR is a law that affords protection to personal data in relation to processing. The IT Act does not mention the word “processing”.

Further, GDPR is a law that is dedicated to data protection and elaborately deals with the issue. The IT Act, on the other hand, merely includes data protection, in relation to body corporate, as a part of the legislation.

Principles of Processing and Collection of the Data

Data protection principles have been laid down in the GDPR and in the Rules under IT Act.[13]

According to Rule 5 of the IT Act, information shall be collected for lawful purpose only.[14] This purpose should be connected with the activity of the corporate body.[15]Further, this information should be necessary for achievement of the purpose.[16] Also, the time period for storage cannot be more than what is required for purpose of collection or law.[17]

---

13 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

14 Rule 5, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

15 Rule 5, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

16 Rule 5, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

17 Rule 5, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

Under the GDPR, data processing is guided by purpose limitation,accuracy, storage limitation, integrity and confidentiality and accountability.[18]

Similarities

Like the GDPR, the Rules require that data should be collected for lawful purpose and collection should be necessary for that purpose. Rules also stipulate that data cannot be retained longer than the period for which processing is necessary for that purpose. Minor exceptions have been mentioned in the GDPR with regard to data retention[19].

Difference

While “Processing” has been defined by Art.4(2) of the GDPR, this is not the case under the IT Act or the Rules meant for data protection. The word processing has however been used under Sec. 2(o) in the definition of data.[20] As the word information includes data[21], it can probably be said, through circuitous reading of the law, that these principles apply to processing as well.

GDPR goes further than the principles of data retention, lawful purpose and necessity of information mentioned under the IT Act. Additional principles mentioned in the GDPR are data integrity, protection from unlawful processing or damage and fairness and transparency in processing. GDPR also provides for regular revision of data collected for achieving data accuracy.[22]

Significantly, the principle of accountability is a notable feature of GDPR. Under this, the controller has been given the responsibility to uphold the principles mentioned and to demonstrate compliance with them.

These principles are not mentioned in the IT Rules. Principle of accountability, though not specifically worded, can at best be inferred from Rule 5.[23]

---

18 Art.5, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

19 Longer data retention is permissible when data is processed solely in public interest, scientific or historical research or statistical purpose subject to data protection safeguards. This is not given under IT Act or the Rules thereunder.

20 "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

21 Sec. 2(5), Information Technology Act, 2000 defines information as: "information" includes 12 [data, message, text], images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

22 Article 5, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

23 For example, Rule 5(2) lays down that “body corporate or any person on its behalf” shall collect the information for lawful purpose and only if collection of such information is necessary for that purpose. Further, under Rule 5(8) “body corporates or any person on its behalf” must keep the information secure. Similarly, other responsibilities of body corporate with regard to the principles have been given in Rule 5.

Strangely, while some of the principles mentioned in the Rules are applicable to "sensitive personal data or information", other principles apply to "information". For example, the principle requiring that information can be collected only for lawful purpose connected with activity of the body corporate applies to "sensitive personal data or information"[24]. This requirement does not refer to "information" collected and going by strict interpretation, is inapplicable to it. Likewise, the purpose limitation requirement under Rule 5(5) applies to "information collected" and does not include within its fold "sensitive personal data or information". There is no clarity why this difference has been introduced.

In contrast, the principles of data processing mentioned in the GDPR are applicable to processing of "personal data" in general.

Interestingly, the principles under Rule 5 of the IT Act do not apply to "company collecting personal data under a contractual obligation with another Indian or foreign company".[25] [26] This means that only those body corporates that **directly** enter into contract with natural persons who provide sensitive personal data or information are subject to these principles.

GDPR does not stipulate such condition.

Lawfulness of Processing

Both IT Rules and the GDPR permit processing if it is lawful. Under Rule 5(2)(a) of IT Rules sensitive personal data or information cannot be collected unless it is for lawful purpose. Likewise, Art.5 of GDPR permits only lawful processing and Art.6 explains the meaning of lawfulness of processing.

Similarity

"Consent" of data subject or provider of information is an important criterion for lawfulness under the GDPR and IT Act.

Difference

Lawfulness has been explained in considerable details in the GDPR. Besides consent of data subject, other criteria necessary for lawful processing stipulate that processing must be necessary for:

performance of contract to which data subject is party (b) compliance with legal obligation to which controller is subject (c) protecting vital interests of data subject or another natural person (d) protecting public interest or in exercise of official authority vested in controller (e) fulfilling legitimate interests of controller or third party.

---

24 Rule 5(2)(a), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

25 Pg 195, Chapter 8, Data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

26 This can be inferred from the clarification issued by Department of Information Technology. According to the Clarification, body corporates that provide services "relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5 & 6." The Clarification further stated that "Body corporate, providing services to the provider of information under a contractual obligation directly with them, as the case may be, however, is subject to Rules 5 & 6." It goes on to explain that "Providers of information, as referred to in these Rules, are those natural persons who provide sensitive personal data or information to a body corporate."

GDPR further lays down that additional conditions can be specified by Member States by law. In case processing is for a purpose other than that for which personal data has been collected, controller can go ahead with processing if the new purpose is compatible with the one for which consent of data subject was sought. Criteria for determining compatible purpose have been listed in the GDPR.

The IT Act and the IT Rules, 2011 do not provide similar conditions and clarifications.

Sensitive Personal Data

GDPR provides for rights and liabilities with regard to processing of "personal data" in general. Further categorization of personal data has been done where such data is sensitive enough to cause significant risks to fundamental rights and freedoms.[27] Here the data that is classified as "special categories of personal data" has tougher procedures for permitting processing.

Section 43A of the IT Act and Rules associated with this section also confer protection to special category data termed as "sensitive personal data or information". The list of "sensitive personal data or information" has been given under Rule 3 of IT Act.

Similarity

Both GDPR and the Rules classify biometric data, health records and sexual orientation as sensitive data.

Difference

The list under Rule 3 of the IT Act excludes racial or ethnic information, political opinions, religious or philosophical beliefs and trade union membership, from sensitive data category. However, these have been included under Article 9 of GDPR.

Further, while the Rules include password and financial information within the list, these are not categorised as special category data in the GDPR.

Consent

Definition of consent has been considerably expanded under Article 4(11) of the GDPR.[28] Meaning of valid consent and demonstration of a valid consent are important elements of the GDPR.[29] Special attention under Article 8 has been given to a child's consent where information society service is involved.

---

27 Recital 51, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

28 Definition of valid consent has been added. Consent must be unambiguous, freely given, specific and informed. Conditions of valid consent have been given in Art.7. According to Recital 32, pre ticked boxes, silence or inactivity do not constitute consent.

29 Art.7, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

Similarity

Both GDPR and the Rules mandate that consent for using personal data is required prior to the collection of information. Moreover, the provider of information or the data subject has the option to withdraw consent.

Difference

Unlike the GDPR, consent has not been defined under IT Act. Rule 5 merely states that a written consent from provider of information has to be obtained before collection and usage of sensitive personal data or information. Further, unlike GDPR the IT Act does not require demonstration of consent nor does it have a special provision for the consent of a child.

Rights

The GDPR confers 8 well defined rights upon the data subject; Right to be informed (Art.14), Right of access (Art.15), Right to rectification (Art.16), Right to erasure (Art.17), Right to restrict processing (Art.18), Right to data portability (Art.20), Right to object (Art.21) and Rights in relation to automated decision making and profiling (Art.22).

None of these have been explicitly mentioned in the IT Act i.e the IT Act does not use the word "Right" anywhere. Though references to certain rights can be inferred from Rules, these lack the details given under GDPR with respect to the scope and enforcement of these rights.

Provisions under the Rules that loosely correspond to the rights mentioned in the GDPR are as follows:

Right to Rectification

Rule 5(6)[30] provides that the provider of information can request "**review of information**" for **amendment** of inaccurate or deficient personal information or sensitive personal data or information.

Similarity

This loosely corresponds to "Right to rectification" given in Art.16 the GDPR.

Difference

The GDPR provides this as a right and makes additional provisions with regard to obligations of the controller in general and obligations when the data is disclosed to third party. The Rules do not state these.

Right to be Informed

Under Rule 5(3) the provider of information must be informed that the information is being collected and also be made aware of the purpose of collection, the intended recipients of the information and the name and address of the agency responsible for collecting and retaining the information.

30 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

Similarity

This is analogous to Art.14 of the GDPR. The information to be given to the data subject includes the identity and contact details of the controller and the data protection officer, the purpose of processing, the categories of personal data and the recipients or categories of recipients of personal data.

Difference

Under the GDPR the data subject has been conferred with a specific "right" to be informed. Also, the requirements under Art.14 of the GDPR are more elaborate. For example, in case of third party transfers the data subject should be apprised of the suitable safeguards available. Further, additional information must be given to the data subject to ensure fairness and transparency. Moreover, if the personal data has to be processed for purposes other than that for which it was collected, the data subject has to be informed. The conditions under which this right shall not apply have also been mention.

None of these requirements have been listed in the IT Rules.

Right to Withdraw Consent and Right to Erasure

The provider of information can request withdrawal of consent given earlier under Rule 5(7) of the IT Rules, 2011.

Similarity

Under Rule 5(7) of IT Act and Art.7(3) of the GDPR, the provider of information and data subject respectively, have the been given the option to withdraw consent given earlier.

Difference

While the Rules provide an "option" to withdraw consent to the provider of the information, under the GDPR the data subject has been given the "right" to do so.

Further,according to the GDPR if consent is withdrawn by the data subject she shall have, under Art.17, the right to obtain from the controller the erasure of personal data without undue delay. The IT Act however, does not explain what will happen to the collected data once consent has been withdrawn except that the body corporate may refuse to provide goods or services for which the information was sought.

Security and Accountability

Security practices under the IT Act stipulate a privacy policy[31] and "reasonable security practices and procedures."[32]

---

31 Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

32 Pg 198, Chapter 8, Data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

According to the Rules, the privacy policy has to be published on website and made accessible.[33] It must state the type of data collected, the purpose of collection, disclosure of information and reasonable security practices and procedures.[34] Under this policy personal information can be collected only under a lawful contract.[35]

Rule 8 gives an account of what would qualify as a reasonable security practice and procedure. Every organization shall be deemed to have complied with reasonable security practices and procedures under two conditions: 1. If security practices and standards have been implemented; and 2. A comprehensive documented information security programme and information security policies have been implemented. This document should contain managerial, technical, operational and physical security control measures for data protection.

According to Rule 8 only IS/ISO/IEC codes of best practice and the codes duly approved and notified by Central government shall qualify as security standards. Organizations are obligated to perform yearly audit of such practices and procedures.

Organizations that successfully demonstrate they have implemented such security practices will be considered compliant in implementing security practice and will be free from liability to pay compensation under Sec.43A when wrongful loss or gain occurs due to data protection failure.

Similarity

Both GDPR and the IT Rules require adoption of internal policies and security audit for data protection. Data protection practices also include voluntary compliance with code of conduct and approved certification.

Difference

IT Act does not address security issues in a manner that is as rigorous as given under the GDPR.

As far as organisations under GDPR are concerned, practices for security of processing include data protection policy by design and default.[36] Organisation may demonstrate compliance with such technical and organisational measures such as pseudonymisation[37],

33 Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

34 Ibid.

35 Ibid.

36 Recital 81, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

37 Art.32(1), General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

privacy impact assessment[38], appointment of Data Protection Officer[39], maintenance of records of processing activities[40] and notification of data breach[41].

But for a broad outline of privacy policy and adherence to "reasonable security practices and procedures", other transparent and accountable features of GDPR are absent in the IT Rules.

Compensation and Liability

a. Compensation for Damages

Sec.43A of the IT Act lays down the liability of the body corporate to pay compensation when it is negligent in securing sensitive personal data or information. Similarly under Art. 82 of the GDPR compensation for damage can be claimed from the controller or processor when there is infringement of GDPR.

Similarity

Compensation for damages arising due to infringement of data protection clauses can be claimed by person affected under the GDPR and the IT Act.

However both laws provide for exemption from this liability.[42] As per Art. 82(2) of GDPR, if it can be proved that controller or processor was not responsible for causing the damage then the exemption from liability will kick in. Similarly, IT Rule 8(1) provides that the body corporate shall be deemed to have followed reasonable security practices if it can be shown that such measures were implemented that are commensurate with protection of information assets. Under this condition, the body corporate shall not be held liable for negligence in implementing reasonable security practice and thus escape the liability to pay compensation under Sec.43A of the IT Act.

Difference

The GDPR provides for compensation as a right of data subject in case of damages due to infringement. IT Act does not use the word "Right".

---

38 Art. 35(7)(d), General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

39 Art. 37, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

40 Art. 30 and Recital 82, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

41 Art. 33, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

42 Art. 82(3) of GDPR and combined reading of Rule 8(1) and Sec.43A

Further, under the IT Act, the authority before which the aggrieved person can claim compensation varies with the value claimed. According to Sec.46(1A) of the IT Act, the compensation amount for damages that can be claimed before the adjudicating officer cannot exceed Rs 5 crores. For claims of higher value, the aggrieved can approach a competent court.

On the other hand, the GDPR has left it to the Member States' courts, irrespective of the amount claimed, to decide the amount to be awarded in accordance with the case law developed by European Court of Justice.[43] [44]

To make things difficult, to claim compensation under this Section, the person affected must show that "wrongful loss" or "wrongful gain" has been caused to another person due to negligence in maintaining and implementing reasonable security practices and procedures.[45] [46] GDPR does not necessitate establishment of such mens rea (intention).

b. Punishment for Disclosure of Information

Information breach has serious repercussions under the GDPR and IT Act.

Similarity

Both laws make provisions for imposition of fines if breach occurs. Sec.72A of IT Act provides for fines upto 5 lakh rupees and Art.83 of GDPR allows for imposition of exemplary fines up to 10,000 000 EUR or 2% of total worldwide turnover of preceding financial year, whichever is higher.

Difference

The IT Act imposes criminal liability. Sec.72A of the IT Act applies when there is disclosure of personal data by service provider in breach of contract. Just like Sec.43A, it has to be proved that the disclosure was brought about with the intention of causing wrongful loss or gain to the person concerned and without the consent of the person concerned or in breach of contract. This section imposes a penal liability on the offender punishable with imprisonment up to 3 years or fine up to 5 lakh rupees or both.

GDPR, on the other hand, does not impose criminal penalties but makes way for imposition of high administrative fines for infringement of provisions under it.[47] Data breach, similar to the one provided under Sec.72A of the IT Act, can attract administrative fines up to 10,000,000 EUR under GDPR.[48]

---

43 Recital 146 and Art.82(6), General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

44 Google Inc. v Vidal-Hall & Others [2015] EWCA Civ 311)

45 Sec.43A, The Information Technology Act, 2000

46 Wrongful loss and wrongful gain have been defined under Sec.23 of Indian Penal Code

47 Article 83, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

48 Article 83, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

Thus GDPR imposes civil liability only.[49] It does not contain penal provisions as given under Sec.72A of the IT Act.

c. Redress

The redress mechanism under the GDPR gives data subject the right to lodge complaint with the supervisory authority against unlawful processing.[50] Data subject also has the right to effective judicial remedy against the decision of the supervisory authority.[51]

Where data subject considers that her rights under the GDPR have been infringed during processing due to non-compliance with it, the concerned data subject has the right to effective judicial remedy.[52] This provision can be exercised despite the availability of administrative or non-judicial remedies.[53] Also, every data subject has the right to receive compensation for the damage suffered awarded by competent courts of member state.[54]

According to Rule 5(9) of the IT Act the provider of the information can approach the Grievance Officer, designated by the body corporate, to resolve grievances related to processing of information.

To decide whether any person has contravened the law that makes him liable to pay compensation under the Act, an inquiry will have to be held by an adjudicating officer.[55] Appeals against decision of the adjudicating officer shall lie to the Cyber Appellate Tribunal[56]. If compensation value claimed under chapter IX of IT Act is more than 5 crore a competent court will decide the matter.[57] This compensation claim is subject to the caps on compensation provided under individual sections of Chapter IX.[58]

---

49 Under Art.83 of the GDPR high administrative fines can be imposed for violation of provisions mentioned in the Article. Penalties under Art.84 of GDPR can be imposed for infringements that are not covered by administrative fines.

50 Article 77, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

51 Article 78, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

52 Article 79, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

53 Article 79, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

54 Article 82, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

55 Rule 48, Information Technology Rules, 2011

56 Section 57, The Information Technology Act, 2000

57 Section 46, The Information Technology Act, 2000

58 As stated above, compensation claimed under S.43A cannot exceed Rs 5 crore

Similarity

Redress mechanisms have been provided under both laws for grievance related to processing of information.

Difference

Notable difference between GDPR and IT Act is that the redress mechanism under GDPR is available a matter of "Right". This is not the case under IT Act.

The IT Act directs that a competent court must be approached for deciding compensation claims above Rupees 5 crore. However, it is not clear which court would qualify as the court of competent jurisdiction for the purpose of filing the case under Sec.43A.[59]

Further, the IT Act creates a penal provision by way of Sec.72A for disclosure of information in breach of lawful contract. It "falls short of creating a private right of action on behalf of individuals whose data is being handled by any third parties because it is still cast as a penal provision and does not create a private right of action in civil law...an individual cannot file a suit in civil court under this section as it does not create a statutory right to damages or compensation, that is, there is no private right of action for damages in civil law"[60] In absence of recourse to civil court there is lack of clarity regarding the procedure to be adopted for imprisonment or fine against the offender.

Data Transfer

Data transfer conditions under the GDPR are governed by Chapter V, Art.44 to 50. Transfers can take place subject to adequacy decisions or appropriate safeguards in absence of adequacy decisions by the commission. The chapter also lists conditions for transfer when neither adequacy decision nor appropriate safeguards are available.[61] Further, decisions of courts and other administrative authorities of third country requiring controller or processor to transfer or disclose personal data can be enforced only if an international agreement is in force between the third country and the Member State.[62]

Data transfer under the IT Act is governed by Rule 7. According to it, the transfer of information will be allowed only if the transfer is necessary for performance of lawful contract between body corporate and provider of information.

---

59 Pg.33, Chapter 2, data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

60 Pg.202, Chapter 8, data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

61 Art.48, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

62 Art.48, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

Similarity

Both GDPR and IT Act provide that transfer of data to another body or country can take place only if they adhere to same level of data protection.

Difference

The Rule 7 permits data transfer from a body corporate or any person on its behalf to another body corporate or a person in India or located in any other country.

Data transfer under the GDPR not only covers the data transferred to a third country but to international organisations too. On the other hand, the IT Rules do not mention international organisations.

Further, the Rules allow data transfer only if the transfer is necessary for performance of lawful contract between the body corporate or any person on its behalf and the provider of information or where such person has consented to data transfer. In contrast, the GDPR lists several other parameters that ought to be fulfilled for satisfying the data transfer conditions. They are -

Factors to be taken account while deciding adequacy of safeguards under GDPR include[63]:

Rule of law, human rights, fundamental freedoms, relevant legislations, access of public authorities to personal data, data protection rules, rules for onward transfer of personal data to third country or international organization, case law, effective and enforceable data subject rights, effective administrative and judicial redress for data subject whose personal data is being transferred, existence and effective functioning of independent supervisory authorities for ensuring and enforcing compliance with data protection rules, international commitments undertaken .

Conditions to be fulfilled for providing appropriate safeguards include[64]:

Existence of legally binding and enforceable instrument between public bodies or authorities, existence of binding corporate rules, adoption of standard protection clauses adopted by commission, adoption of standard data protection clauses by supervisory authorities, approved code of conduct along with binding commitments, approved certification mechanism, binding corporate rules.

Some of these data transfer conditions vis-a-vis India's position have been discussed below:

i. ***Data protection law and international obligations***
As of now India does not have a dedicated data protection law. However, India is a signatory to International Convention on Civil and Political Rights, 1966 that upholds right to privacy under Article 17.[65] This international commitment favours India with regard to data protection principles.

ii. ***Data subject rights, Redress mechanisms and existence of effective independent supervisory authorities***

---

63 Article 45, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

64 Article 46, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

65 Pg. 198, Chapter 8, data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

The IT Act does provide a mechanism for redress in case of breach of data, complaints regarding processing and compensation mechanism due to damages. However, as explained before these mechanisms need clarity. Moreover, no provision for independent supervisory authority has been made and the IT Act does not confer specific data subject rights.

iii. ***Approved code of conduct along with binding commitments and approved certification mechanism***
Reasonable Security practices and procedures under Rule 8 stipulate a privacy policy and codes of best practices along with other security measures. However, legally binding commitments and practices like binding corporate rules given under GDPR have not yet been mentioned under the IT Act or the Rules.

iv. ***Rules for onward transfer of personal data to third country or international organization***
Transfer of sensitive personal data or information from a body corporate or any person on its behalf to another body corporate or a person in India or outside India is subject to conditions mentioned under Rule 7 of the IT Act. Transfer is allowed only if it is necessary for performance of lawful contract between provider of information and the body corporate or any person on its behalf or where the provider of information has consented to data transfer.[66]
It will be pertinent to note that the condition for data transfer under Rule 7 is applicable to sensitive personal data or information only. This excludes personal information that is not categorized as sensitive personal data. On the contrary, the data transfer conditions under the GDPR apply to personal data whether or not it is grouped as sensitive.

v. ***Access of public authorities to personal data***
Rule 6 of the IT Act gives power to the Government agencies, mandated under law, to obtain information of sensitive personal data from body corporates. Consent of the provider of information is irrelevant in this case. The only condition for getting access to such information is that a written request has to be made to the body corporate by the authorized government agencies. The request must specify the purpose for which information is sought. The government agency is prohibited from publishing or sharing the information obtained from any other person.

The GDPR also confers similar powers on law enforcement agencies.[67] Thus Member States can restrict the scope of GDPR under specified conditions.

The purpose for which they are exempt from data protection norms under Article 12 to 22, Article 34 and Article 5 have been specified under GDPR. Measures to safeguard national security, defence, public security and crime prevention are some of the purposes that are mentioned in the GDPR.

Moreover, Article 2 restricts the material scope of GDPR by excluding its application from processing undertaken for the purpose of prevention, investigation, detection or prosecution of criminal offences.

Thus, if the Union or Member State seeks to restrict the application of GDPR it can do so only through legislative measures.

On the contrary, the Rules under the IT Act give the power to the executive to access the desired information. Further, unlike the GDPR, in which the purposes for accessing

66 Rule 7, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Sec.43A of the Information Technology Act.

67 Article 23, General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

the information have been articulated, the IT Act or the Rules therein do not state such conditions.

Conclusion

On the face of it the Information Technology Act, 2000 and associated rules address data protection standards. However, as GDPR has a very high benchmark of data protection, the Indian laws on data protection will have to be worked out accordingly. Data protection procedures like breach notification; excessive documentation and appointment of data protection officer may have to be incorporated in the Indian laws as well. As non – compliance involves high fines, inability of India or the organizations situated in India to qualify as data secure destinations is likely to divert business opportunities to safer locations.

It is important to note that data transfer will also be permissible if a model contractual clause authorised by supervisory authority is entered into.[68] India could look at similar arrangements to qualify as an approved destination for data transfer. The European Commission has so far issued two sets of contractual clauses for transfers from data controllers to data controllers and the other for transfer to processors established outside the EU/EEA.[69] However, with reference to Schrems case[70], the validity of such contractual clauses approved by European Commission has come under scrutiny of Irish Data Protection Commissioner. Legal proceedings have been initiated before the Irish High Court in this regard. The proceedings are yet to be concluded and a decision is awaited.[71]

68 Recital 108 and Art.46(2)(c), General Data Protection Regulation (Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Official Journal of Europe

69 Model Contracts for the transfer of personal data to third countries, Building a European Area of Justice, European Commission, https://goo.gl/S6b3d5

70 *Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems*

71 Update on Litigation Involving Facebook and Maximilian Schrems, Explanatory Memo, Data Protection Commissioner,https://goo.gl/8eupnN