General Data Protection Regulation and Its Impact on Indian Enterprises

Dr. Brijesh Kumar Gupta
Braanet Technologies Pvt. Ltd., Ghaziabad 201 016 UP India
profguptabk@gmail.com, director@braanet.com

Abstract – **The General Data Protection Regulation (GDPR) has come into force and will have wide implications for the digital economy and business models of various technology firms. The GDPR aims to provide consumers with the control of their personal data, provide trust in the digital economy and harmonize data protection.**

Clearly, the GDPR would impact the services sector, especially data entry, customer care, advertising, banking and IT, among others. These services cannot be provided to a European client unless the Indian data protection laws are considered adequately rigorous by European Union (EU) standards, or on par with GDPR. The study outcomes presented in this paper attempt to analyse and outline how the GDPR will impact the digital data business of Indian enterprises, as well as providing new challenges and opportunities for innovation. Key highlights of the similarities and differences between IT Act 2000 and GDPR are presented.

Keywords: Data economy, Data portability, Data protection, European union, GDPR, IT Act 2000

I. INTRODUCTION

GATHERING of data and its subsequent commercialization transformed contemporary economies, politics, societies and cultures. The surge in digital technologies and platforms in recent years and the progression towards a digital economy has at its core, the monetization of personal data and the use of 'Big Data' to create value [1]. In the European Union (EU) for example, the value of the data economy is continuously increasing. In 2016, the value was calculated to be EUR 300 billion (1.99% of the EU's GDP) and is estimated in 2020 to be EUR 739 billion (4% of the EU GDP) [2]**.** Indeed, over the last few decades, multinational companies mushroomed with several of them ascending very swiftly to top of the Fortune 500 list and whose source of revenue and business models are dependent on the gathering and use of personal data.

A business model reflects how a firm attracts and provides value to consumers and converts this into a financial profit [3]**.** A successful business model can differentiate a firm from its competitors, provide huge financial returns and can ultimately create a paradigm shift in how an industry functions and conducts business. With an increase in digitization and the emergence of the digital economy, the variety as well as the complexity of different business models has only increased [4], [5], [6] and [7]. The seminal business model research and canvas done by Osterwalder *et al.* [8] had a profound impact in the start-up world.

Privacy and data protection have always been a priority policy for the European Union law maker. The legislation gradually developed to reach the point of adopting the General Data Protection Regulation. Claiming to promote the protection of fundamental rights, the GDPR also supports lawful business procedures to create a balanced environment.

II. GENERAL DATA PROTECTION REGULATION

The GDPR builds upon many existing concepts in European privacy law and creates new rights for the users whose data is being processed [9]. The result is new compliance obligations for organizations handling data. The Regulation addresses two main ideas: to strengthen and unify data privacy rules for individuals in the European Union; and to widen the territorial scope of the data protection by regulating the export of personal data of European citizens outside EU. It is known that the main goal of the GDPR is for both citizens and business to benefit from the new rules – *common welfare has always been first priority for the EU legislator*.

The General Data Protection Regulation is a European Union Law implemented on May 25, 2018 requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory [10]. The regulation includes *seven* principles of data protection that must be implemented and *eight* privacy rights that must be facilitated. It also empowers member state-level data protection authorities to enforce the GDPR with sanctions and fines. The GDPR replaced the 1995 Data Protection Directive, which created a country-by-country patchwork of data protection laws. The GDPR, passed in European Parliament by overwhelming majority, unifies the EU under a single data protection regime.

GDPR is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union, it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The

GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

III. BRIEF COMPARISON OF INFORMATION TECHNOLOGY ACT, 2000 AND GDPR

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" [11]. 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.

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:

TABLE 1 -- KEY FEATURES OF THE GDPR AND THE IT ACT

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 Rule 5 of IT Rules, 201110	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 mention processing. Principles listed in the GDPR but not mentioned in IT Act are data integrity, protection from unlawful processing, accountability, fairness and transparency.
Lawfulness of processing	Art.6 of GDPR Rule 5 of IT Rules, 2011	Consent of provider of information11 or the data subject12 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.

IV. GDPR IMPACT ON INDIAN ENTERPRISES

Following the Cambridge Analytica data hacking case reported in March 2018, the European Union (EU) enacted the GDPR 2018. As a result, e-commerce companies registered in non-European jurisdictions are subject to a legal framework on par with these regulations. To enforce such legislation, India's e-commerce companies need to have a similarly stringent legislation besides infrastructure and technologies in place.

Clearly, the GDPR would impact the services sector, especially sectors like data entry, customer care, advertising, banking and IT, among others. These services cannot be provided to a European client unless the Indian data protection laws are considered adequately rigorous by EU standards or on par with GDPR. Even if Indian companies do not directly interact with European citizens, they would still require GDPR compliance. This is so because personal data of European citizens have the potential to be exploited for other related data processing activities.

If so, Indian companies would attract heavy penalty for non-compliance. For instance, if an Indian company uses data of former European customers, it would be liable for penalisation under the GDPR. Accordingly, the differences between the existing legal framework in India and the EU on data privacy merits consideration. Both government agencies and trade bodies like FICCI and NASSCOM would have to formulate a regulatory regime to accomplish synergy between Indian and EU data protection regimes to promote India-EU trade to its full potential.

Europe is a substantial marketplace for the ITeS, BPO and pharmaceutical industry in India. The size of the IT industry in the top two EU member states (*i.e.* Germany and France) is estimated to be around 155–220 billion USD. Thus, for the Indian IT industry to keep continuing to do business in Europe, it needs to comply with the GDPR. The GDPR imposes a penalty structure of 20 million EUR or 4% of global turnover (on the higher side) in cases of non-compliances.

The regulation requires a programmatic approach to data protection and a defensible programme for compliance will be required to prove that are acting appropriately. As part of these efforts, answers to the following questions need to be sought:

- *What is our data footprint in the EU (e.g. data about employees, consumers and clients)?*
- *Are we prepared to provide evidence of GDPR compliance to EU or US privacy regulators who may request it?*
- *Do we have visibility of and control over what personal data we collect? How do we use it? With whom do we share it?*
- *Do we have a privacy-by-design programme, with privacy impact assessments (PIAs), documentation and escalation paths?*
- *Do we have a tested breach-response plan that meets GDPR's 72-hour notification requirement?*
- *Have we defined a roadmap for GDPR compliance?*
- *Have we identified a Data Protection Officer (DPO) as required by the GDPR?*
- *Have we adopted a cross-border data transfer strategy?*

V. THE CHALLENGES

Weak data protection law in India: India's outsourcing industry, which is estimated to be worth over 150 billion USD, contributes nearly 9.3% of the GDP. The EU has been one of the biggest markets for the Indian outsourcing sector and India's relatively weak data protection laws make us less competitive than other outsourcing markets in this space.

*Cross-border restrictions***:** Largely inflexible, the GDPR reduces the extent to which businesses can assess risks and

make decisions when it comes to transferring data outside the EU. Indian companies would need to implement sufficient safeguards, as required under the GDPR, to transfer personal data outside the EU, thereby further increasing compliance costs.

*Greater risk of penalties and litigation***:** Article 3 (Territorial scope) of the GDPR makes it clear that the regulation will be applicable regardless of whether or not the processing takes place in the EU. This means no business for Indian companies that do not comply with the GDPR or increased compliance costs for those who do and the risk of huge penalties on failing to do so.

VI. THE OPPORTUNITIES

Business opportunity rather than compliance burden: Indian IT companies serving the EU market, their second largest after the US, would be required to comply with the GDPR. However, rather than seeing this as an additional burden in terms of compliance, Indian companies should see it as a massive business opportunity knocking at their doors.

Opportunity to stand out: Over the years, India has become a technology hub equipped with deep expertise and a talented resource pool. The GDPR could be an opportunity for Indian companies to stand out as leaders in providing privacy compliant services and solutions.

Developments in India's privacy landscape: The 'adequacy requirements' under the GDPR allow the European Commission to consider whether the legal framework prevalent in the country to which the personal data is sought to be transferred affords adequate protection to data subjects in respect of privacy and protection of their data. In the wake of recent developments and the Supreme Court verdict, a data protection framework has been proposed by the Srikrishna Committee. It will be interesting to see how the forthcoming legislation shapes up and whether it will satisfy the criteria laid down under the GDPR.

VII. CONCLUSION

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. India could look at similar arrangements to qualify as an approved destination for data transfer.

REFERENCES

[1] M.P. Hartmann, M. Zaki, N. Feldmann and A. Neely, "Capturing value from big data – a taxonomy of data-driven business models used by start-up firms", *International Journal of Operations & Production Management,* vol. 36, pp. 1382 – 1406, 2016.

[2] European Commission, Building a European data economy. retrieved from https://ec.europa.eu/digital-single-market/ en/ policies/building-european-data-economy on July 21st, 2018.

[3] D. Teece, "Business Models, Business Strategy and Innovation. *Long Range Planning"*, vol. 43, pp.172-194, 2010.

[4] A. Afuah and C. Tucci, *Internet Business Models and Strategies: Text and Cases*, McGraw-Hill, Boston, 2001.

[5] L.M. Applegate,"Emerging e-business models: Lessons from the field", *HBS No. 9-801-172*. Harvard Business School, Boston, MA, 2001.

[6] R. Amit and C. Zott, "Value creation in e-business", S*trategic Management Journal,* vol. 22, pp. 493-520, 2001.

[7] E. Brousseau and T. Penard, "The economics of digital business models: A framework for analyzing the economics of platforms", *Review of Network Economics,* vol 6, no.2, pp. 81-110, 2007.

[8] A. Osterwalder, Y. Pigneur and T. Clark, *Business model generation. A handbook for visionaries, game changers and challengers*, Wiley, Hoboken, NJ, 2010.

[9] M. Hintze, "Viewing the GDPR through a De-Identification Lens: A Tool for Clarification and Compliance", 2017.

[10] EU General Data Protection Regulations (GDPR): https:// ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations.

[11] The Information Technology Act, 2000.

Dr. Brijesh Kr. Gupta is Founding Director of "BRAANET Technologies Private Limited" NCR-Ghaziabad. He joined teaching profession in 1991 after his post graduation. He possesses 27+ years of teaching, research, administrative and industry experience at various levels in Indian Education System & abroad. He served in Ministry of Defence, Govt. of India as a civilian officer. To carry out his research work in the area of High Speed Communications, he enrolled himself at Indian Institute of Technology, Roorkee, India in Jan. 1999. Worked on two major research projects sponsored by UGC and AICTE. Served reputed technical institutes of UP Technical University, Lucknow since 2003.

Published 51 research papers. Chaired Technical Sessions in International Conferences. Authored book on *Mobile Computing*. Guided M. Phil. and M.Tech. students. Organized conferences/workshop and faculty/students. Has keen interest to organize Industry–Institute collaboration programs. He is ITU-certified faculty for Information Security & Cyber Security for Enterprises, Visiting faculty for Central Detective Training Institute, BPRD, Ministry of Home Affairs, Govt. of India and Entrepreneurship Certified Faculty, Ministry of Skill Development & Entrepreneurship, Govt. of India.

Received "ShikshaGaurav Puraskar-2014" for contribution in the field of Technical Education, Listed in *Albert Nelson Marquis Lifetime Achievement Award -2017, 2018* USA, Honoured with "Howard Cosell Memorial International Honour Award-2018", West Bengal, National Education Day Awardee – 2019, New Delhi alongwith Roll of Honour 2019-2020, Govt. of India (E).