A Date with Data Protection

"Once you've lost your privacy, you realize you've lost an extremely valuable thing."- Billy Graham

The European Parliament released the European Union General Data Protection Regulations (**"GDPR"**) in the year 2016, which came into effect from May 25, 2018. GDPR provides for data protection for all individuals in the European Union (**"EU"**) and economic areas under the EU. The objective of the GDPR is to strengthen and regulate the data protection for individuals within the jurisdiction of EU as well as export and usage of personal data outside EU.[1] GDPR aims to create a balance vis-à-vis the individuals' privacy rights and free flow of data across the Digital Single Market.[2] One of the key objective of GDPR is to create a harmonized approach to data protection across the EU with enhanced right to privacy for individuals in the current age of rapid technological advances. GDPR aims to set a high standard for personal data protection throughout EU, imposes numerous stringent obligations in cases of violations by those handling the data, and provides for an enhanced enforcement regime. In the following paragraphs, this article has discussed the relevant concepts of GDPR.

Application of GDPR

The GDPR applies to organisations (whether acting as data controller or data processor[3]) that process personal data and are established in the EU. In some circumstances, it will also apply to organisations that process personal data and are established exclusively outside the EU. There are three key triggers for the application of GDPR. *Firstly,* if the organization has an establishment within the jurisdiction of EU and undertakes the processing of personal data. *Secondly,* if the organization does not have an establishment in EU and undertakes the processing of data which relates to the offering of goods or services to data subjects in EU. *Thirdly,* if the organization does not have an establishment in EU and undertakes the processing of data which relates to monitoring of behavior as far as the behavior takes place in EU.

Relevant concepts in GDPR

The GDPR applies to both controllers and processors. "Processing" has been defined very widely and includes collecting, organising, storing, altering, retrieving, using, disclosing, combining and erasing personal data, amongst other activities.[4]

---

[1] This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not; GDPR, Article 3(1), *Territorial Scope*

[2] This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system; GDPR, Article 2, *Material Scope*

[3] GDPR; Article 24, *Responsibility of Controller.*

[4] 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or

"Personal data" is any information relating to an identified or identifiable natural person. This might be by reference to an identifier such as a name, ID number, location data or online identifier, or by factors specific to them, such as their physical, genetic, economic or social identity.[5]

Allowed usage of personal data

In order to process personal data lawfully, a data controller (that is, the person that determines the purposes and means of the processing of personal data) must have at least one of a number of lawful grounds to do so. The lawful usage as per the GDPR are:

1. The data subject has given consent to the processing for one or more specific purposes.
2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
3. Processing is necessary for compliance with a legal obligation to which the controller is subject.
4. Processing is necessary in order to protect the vital interests of the data subject or another natural person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

One of the foundational principles under the GDPR is personal data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Rights conferred by GDPR

1. Right to access[6]

   This right to make a data subject access request (**"DSAR"**) is a right for a data subject to obtain confirmation from a data controller as to whether personal data about them is being processed, as well as a copy of that personal data. This right also entitles a data subject to obtain certain available information such as where the personal data was collected from and

---

otherwise making available, alignment or combination, restriction, erasure or destruction; GDPR; Article 4(2), *Processing*

[5] 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; GDPR; Article 4(1), *Personal Data*

[6] GDPR; Article 15, *Right of access by the data subject*

how it is processed, for instance whether the controller is using it for profiling purposes. It should be easily exercisable at reasonable intervals.

2. Right of rectification[7]
   This is a right for data subjects to obtain, without undue delay, rectification of inaccurate personal data about themselves. Depending on the purposes of the processing, data subjects may also have a right to have incomplete data completed.

3. Right to erasure[8]
   This right is also called "right to be forgotten", which entitles data subjects to have their personal data erased without undue delay.

4. Right to restrict processing[9]
   Data subjects have the right to obtain restriction of processing in certain circumstances. For example, if a data subject contests the accuracy of the personal data, processing may be restricted while its accuracy is being verified. This right also applies where the processing is unlawful but the data subject doesn't want it to be erased, or where the controller doesn't need the data but it is still required by the data subject for the establishment, exercise or defence of legal claims.

5. Right to object[10]
   This applies when the ground for lawful processing is based on it being necessary for performing tasks carried out in the public interest or in the exercise of official authority vested in the controller. It also applies where the ground is based on legitimate interests, including profiling based on those grounds. Data subjects can object based on their particular situation at any time.

6. Right to data portability[11]
   Individuals can ask to receive personal data that they have provided to a controller in a structured, commonly used and machine-readable format so that it can be easily transferred to another data controller/service. The idea is to give the data subject more control for example by facilitating switching between service providers.

Comparison with Indian Information Technology 2000

The Indian Information Technology Act, 2000 (**"IT Act"**) is Indian legislation governing the internet, and the procurement, and use of data in India.

This article has documented a comparative study of the rights and obligations enumerated under the GDPR and the IT Act hereunder:

#	Category	Particulars
1	Agenda	Both govern data protection rules and regulations in their respective territories, and transfer of data for business.

[7] GDPR; Article 16, *Right to rectification*
[8] GDPR; Article 17, *Right to erasure*
[9] GDPR; Article 18, *Right to restriction of processing*
[10] GDPR; Article 19, *Right to object*
[11] GDPR; Article 20, *Right to data portability*

	Individual Rights	GDPR provides for rights for individuals whereas IT Act does not provide any rights. These rights include, but are not limited to, right to object, erasure, accessibility and portability, and restriction.
2.	Principles of Processing, Use and Procurement of Data	GDPR has principles for procurement, processing and use whereas IT Act has principles only for procurement and use. Principles listed in the GDPR but not stated in IT Act are data integrity, protection from unlawful processing, accountability, fairness and transparency.
3.	Consent	Both IT Act and GDPR require consent as a pre-requisite for data procurement. However, unlike GDPR, the IT Act does not define consent, required provisions for minor's consent, or require demonstration of consent by the business.
4.	Security and Safety Provisions	Common data protection security practices include adoption of internal policies, security audit, and adherence to voluntary code of conduct and certification mechanism. However, 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
5.	Violations	1) Compensation: It is a Right under GDPR, but not under IT Act. Both include different procedures for compensation claims. Both have provisions for liability and exemption to liability. 2) Punishment: GDPR imposes civil, whereas IT Act imposes civil and criminal liability.
6.	Redressal	Both provide procedures for redressal. Although redressal is a right under GDPR and not under IT Act. There is ambiguity regarding the redressal authority under IT Act whereas it is specifically provided for under GDPR.

Effects on Indian Businesses

Businesses have to therefore comply with the GDPR Provisions with immediate effect. This will change their Business to Consumer and Business to Business Relations as they have to implement consumer rights, and make data protection and privacy as default and design of their businesses.

Due to weak Data Protection Laws in India, the EU's Commission may become a road block in transfer of data from EU to India, which will be detrimental to the businesses here. Also, EU Businesses engaged with Indian Businesses here may lessen their engagement due to potential non-compliance on part of Indian Businesses, making Indian markets less competitive internationally. Prior to the implementation of the Amendment to IT Act 2000 in 2009, the outsourcing sector was affected due to stronger Data Protection Laws in EU and USA than in India. Therefore, to further prevent this disadvantage, the Government brought the amendment to better Indian data protection laws.

In the short run, businesses have to expend major costs on institutionalizing technological, administrative and legal changes (appointment of Data Protection Officers and Representative of the Business in EU) in their Businesses to comply with GDPR. Also, penalties for violations of GDPR are extremely high and in case of a violation, it will be detrimental to the business especially the small and medium businesses. These costs are accompanied by the increasing protectionist and anti-globalization measures in International Trade and Commerce.

In India, GDPR will especially affect backend businesses, outsourced to India and/or which using EU data subjects' data (example, BPO, Banking, Insurance, Healthcare, and Retail). This will affect the Information Technology sector which exports services of USD 45 Billion to the EU. Therefore all the sectors have to comply with the GDPR as soon as, and in the best possible manner.

However, GDPR are potential 'magic beans' as Indian businesses can take the lead in providing, not only individuals in EU but also throughout the globe, the best data protection compliant services. Also in the long run, they can decrease their costs on data protection compliance.

Further, consultancy businesses can capitalize on this by providing services to businesses for complying with GDPR. This side market for GDPR compliance services is estimated to become a USD1.1 Billion market by 2020.

Conclusion and recommendations:

In this dynamic and changing contemporary technology, economic and legal environment, it is vital that India's laws on data protection take into account the following principles:

- That laws evolve with the evolving technology,
- Laws be applicable to public and private entities, and making them accountable;
- Provide for individuals, enforceable rights under the ambit to Right to Life and Personal Liberty
- procedures for penalties to prevent any violations, and an independent executive commission for enforcing data protection laws;
- Minimize data procurement, processing and use and demanding that businesses implement policies and programs to enforce data protection laws.
- Apply the data protection laws to foreign business operating in India and demand that Businesses procuring and processing data at a large scale, process and store data within the territories of India. If the data is to be exported outside, then it should be processed and stored under specific rules and regulations.
- Definition of data and its categories, and instituting procedures for handling of data especially sensitive data (religion, caste, sexual orientation)
- Provide for rights to individuals including but not limited to right to Access, Rectify, Restrict and Object, subject to India's interests.
- Consent that is granted by individuals to data procurement and processing should be explicit, intelligible, and unambiguous. Further provisions should be incorporated for data protection of minors.
- Processing of data should be minimized and data should be processed only for the purpose(s) for which it has been procured. After the completion of the processing, the data should be 'erased'.
- Institution of an Independent Executive Commission for enforcing of data protection laws. This should be accompanied with principles of liability, exemptions, and penalties.

- Address the principles of Aadhar Card and other State sponsored Data Procurement and Processing (example, surveys and census) explicitly.

(*This article has been contributed to the chronicles of Aureus by Vedant Madan. Vedant is a 12th Grade student at DPS Dwarka, as on date of this posting. Views are personal*)