DATA PROTECTION LAWS PREVAILING IN THE EUROPEAN UNION COMPARISION WITH THE INDIAN LAWS

BY C. ANIRUDH ARJUN
FROM SCHOOL OF LAW, CHRIST, BENGALURU

ABSTRACT

'Data Protection' is synonymous to the term 'Information Protection'. We live in the period of Globalization where all the enterprises whether small or big stay connected with the consumers. With the advent of Globalization and Modernization, the aspect of Data Protection also cropped up. Data Protection refers to the appropriate safeguards employed by the country/body corporate to assert, defend and protect the rights and interests of the Data Subject. The General Data Protection Regulation (GDPR), 2018 replaced the Data Protection Regulation,1998 in the European Union. The GDPR recognized the principles relating to the processing of Personal Data as well as Sensitive Personal Data, the rights of the Data Subject and the International transfer of Personal Data to the territory outside the European Union. One of the remarkable feature of this statute is that it recognized the rights and the duties of the Data Controller as well as the Data Processor. Another remarkable feature of the GDPR is that it recognized the transfer of Personal Data to a territory outside the European Union even though the territory failed to offer the adequate level of protection. On the flip side, there is an absence of a statute pertaining to Data Protection in India. Data Protection laws are enshrined under the Information Technology Act, 2000 and the Information technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. The main drawback in the Information Technology Rules, 2011 is that it failed to consider the aspect of transfer of Personal Data to a territory outside India if that territory failed to provide the adequate level of protection. This loophole must be rectified to adapt to the global economy.

Key Words: GDPR, Data Subject, Data Controller, Data Processor, Globalization and Modernization.

INTRODUCTION:

This article compares the Data Protection laws present in the European Union with India. The article mainly deals with the aspect of International transfer of personal data from the parent country to other countries. Firstly, we must understand that there is an absence of a separate statute in India which deals with the aspect of Data Protection. The concept of Data Protection in India is enshrined under the Information Technology Act, 2000 as well as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

In the case of the European Union, there is a separate statute in place recognizing the concept of Data Protection. The General Data Protection Regulation (GDPR) is the statute which deals with the concept of Data Privacy and Data protection in the European Union. The GDPR was implemented on 25th May 2018 and replaced the earlier Data Protection Directive (which was implemented on 24th October 1998). 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.[1] The GDPR has formulated various mechanisms to facilitate the transfer of Personal Data to the countries situated outside the European Union even though they do not offer the necessary legal protection. Binding Corporate Rules, Standard Contractual Clauses and Code of Conduct and Certificate Mechanisms are some of the mechanisms in place to facilitate the transfer of Personal Data of the Data Subject to the countries outside the European Union.

OBJECT OF REASONING

Heading 1: International transfer of Personal Data under the GDPR:

Before dwelling into the crux of the article, we must clearly understand the meaning and the essence of three concepts i.e.- Data Subject, Controller and Processor. **Data Subject** is an individual whose data is collected and processed. At this juncture, we must clearly understand the meaning of the term Personal Data. Personal Data has a two-dimensional definition. Firstly, Personal data is defined as the data which is related to living beings. Secondly, Personal data refers to that data by which living individuals can be identified from those data and other information which is in the possession of, or, is likely to come into the

[1] Article 3 of the General Data Protection Regulation, 2018.

possession of the data controller.[2] **Controller** refers to legal/natural person or public authority that is responsible for determining the purpose for which the data is to be used or processed.[3] **Processor** refers to any natural or legal person who is responsible for processing the data in the hands of the controller.[4]

The GDPR recognizes the transfer of personal data to International countries. Transfer of personal data to countries outside the European Union is possible if the legal systems prevalent in those countries are deemed to provide adequate level of protection to the Personal Data of the Data subject.[5] The Data Protection Directive, 1998 recognized the transfer of personal data to third-party countries whose legal system ensured adequate level of protection to the personal data of the Data subject. The GDPR recognized the transfer of personal data to the sectors within the third-party countries provided they have fulfilled the European commission's adequacy requirement. Transfer of personal data to the countries which offer an adequate level of protection to the personal data of the Data subject does not require prior authorization from the European commission or any of the member states. The adequacy decision shall be periodically reviewed to ensure that the entity is still offering the adequate level of protection to the Personal Data of the Data subject. In the periodic review, the commission or the member states may quiz the entity regarding the various developments initiated by them for enhancing the level of protection to the personal data of the Data subject. The GDPR recognizes transfer of personal data to third party countries which do not offer adequate level of protection to the Personal Data of the Data subject, provided, the controllers or processors adopt certain safeguards to ensure such adequate level of protection.[6]

The usage of 'standard contractual clause' by the European commission is one of the safeguards to be employed.[7] The GDPR has mandated the existence of written contracts between the Data processor and the Data controller. Thus, if the Data Processor employs another Processor for processing the Personal Data, there must be a written agreement between them. The contract must expressly contain certain provisions. The usage of these

[2] Article 4(1) of the General Data Protection Regulation, 2018.

[3] Article 4(7) of the General Data Protection Regulation, 2018.

[4] Article 4(8) of the General Data Protection Regulation, 2018.

[5] Article 45 of the General Data Protection Regulation, 2018.

[6] Article 46 of the General Data Protection Regulation, 2018.

[7] Article 46(2)(c) of the General Data Protection Regulation, 2018.

provisions in the agreement is to demonstrate the compliance to the provisions of the GDPR. The remarkable feature of the GDPR is that it recognizes the rights and liabilities of the Data Controller/Data Processor. Thus, the Data Controllers/Data Processors are penalized for the breach in their duty i.e.- to use standard contractual clauses. Firstly, the said contract must specify the purpose for which the Personal Data of the Data Subject is being processed. It must also address the question of 'retention'. Secondly, the contract must expressly state the rights and duties of the Data Controller/Data Processor.

The 'Code of Conduct' and 'Certificate Mechanisms' is another safeguard that can be employed by the Data Controller/Data Processor.[8] The codes of conduct are self-regulatory measures used elsewhere to demonstrate to the regulators that the organization acknowledges data protection standards. The said Code of Conduct can be prepared by an 'Association' action for/on behalf of the Data Controller/Data Processor. The existing Code of Conduct can be altered or modified to meet the growing requirements of the GDPR. The 'Data Protection Certification' is available to the Data Controller/Data Processor operating outside the European Union provided, the display their willingness to adhere and comply to the Data Protection standards mention in the GDPR. This certificate is valid for a period of three years.

The adoption of 'Binding Corporate Rules' is one of the safeguards to be employed by the Data Controller/Data Processor. [9] Before dealing with this aspect, we must first understand the meaning of the term 'Binding Corporate Rules'. Binding Corporate Rules are the internal rules of the Multinational Companies regarding the transfer of Personal Data outside the European Union. It is already understood that for the transfer of Personal Data to countries outside the European Union is possible only if those countries have adequate level of protection in place. In the absence of this, Personal Data can be transferred outside the European Union provided; adequate safeguards have been employed by the Data Controller/Data Processor. BCR's is one of the many safeguards to be employed to ensure the adequate level of protection. It is **mandatory** that such BCR's should have received the prior approval of the Commission. The BCR's must be drafted in a very precise manner. This means that the BCR's must be made applicable to every member of the Multinational companies. The BCR's must also expressly mention the rights and duties of the Data

[8] Article 49 of the General Data Protection Regulation, 2018.

[9] Article 47 of the General Data Protection Regulation, 2018.

Controller/Data Processor. The GDPR has also mentioned the circumstances under which the Personal Data of the Data Subject can be transferred in the absence of the adequate level of protection and appropriate safeguards. This has been enshrined under Article 49 of the GDPR. The **first** main exception crops up when the Data Subject has given consent to the transfer of Personal Data to a country (not possessing the adequate level of protection) outside the European Union. In such a case, the Data Subject has been informed about the potential risk associated with the transfer of such Personal Data. The **second** exception is that the Personal Data is transferred for the performance of a contract. This also encompasses the concept of transferring the Personal Data for the conclusion of a contract. The **last** exception is regarding asserting/ defending a legal claim or a legal interest of the Data Subject. This legal claim or legal interest of the Data Subject is defended by the Data Controller/Data Processor.

Heading 2: Data Protection under the Indian Law:

Before dwelling into the aspect of Data Protection, we must first understand as to whether the 'Right to Privacy' has been enshrined in the Indian Constitution. In the case of Justice K.S. Puttaswmay (Retd.) v/s Union of India[10], the nine Judge bench held that Privacy is a constitutionally protected right. The concept of Privacy has been enshrined under Article 21 of the Indian Constitution. Thus, it is understood that Right to Privacy is a Fundamental Right.

We must clearly understand that there is no separate statute present in India recognizing the concept of Data Protection. The aspect of Data Protection is embedded under the Information Technology Act, 2000 as well as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. The IT Act, 2000 deals with the payment of compensation for the wrongful disclosure of Personal Data of the Data Subject. The Information Technology Act states that any person who is negligent in using reasonable security practices and procedures (RSPPs) to protect sensitive personal data or information is liable to pay compensation for any wrongful loss or wrongful gain. [11]

The Information Technology Rules, 2011 deals with the principles relating to the processing of Personal Data. Rule 7 of the IT Rules, 2011 deals with the International transfer of

[10] WRIT PETITION (CIVIL) NO 494 OF 2012.

[11] Section 43(A) of the Information Technology Act, 2000.

Personal Data. The crux of this provision is that the Personal Data can be transferred to a country/body corporate outside India if country/body corporate offers the same level of legal protection. The Personal Data can only be transferred if it is required for the performance of a contract and the Data Subject has consented to such transfer. The IT Rules, 2011 fails to address the issue pertaining to the transfer of Personal Data of the Data Subject to the countries which fail to offer adequate level of protection. The transfer of Personal Data of the Data Subject by the Data Controller/Data Processor may be required to assert or defend a legal claim/legal interest. Secondly, the transfer of Personal Data of the Data Subject by the Data Controller/Data Processor may be required to protect the vital interest of the Data Subject when he is incapable of giving his consent. These are the two circumstances which have not been addressed by the IT Rules, 2011. At times, the Personal Data of the Data Subject possessed by an Indian Company must be transferred to its subsidiary company (situated in another country) but, the latter country does not offer adequate level of protection. In such a situation the IT Rules, 2011 does not come to the rescue. Thus, there is a need to incorporate provisions in the IT Rules, 2011 to cover these loopholes.

CONCLUSION:

Today, we are living in a digitalized environment where the aspect of Data Protection must be given utmost importance. To facilitate the protection of Personal Data of the Data Subject, the laws must be very robust in nature. The Data Protection laws must recognize the rights, duties and the obligations of the Data Controller as well as the Data Processor.

The General Data Protection Regulation (GDPR), 2018 has addressed the loopholes present in the Data Protection Directive; 1998.The GDPR has also recognized the transfer of Personal Data of the Data Subject to a country outside the European Union. The remarkable feature of the GDPR is that it facilitates the transfer of Personal Data to the countries (outside the European Union) which lack adequate level of protection provided, certain circumstances have been fulfilled. On the flip side, the Data Protection laws embedded under the IT Act, 2000 and the IT Rules, 2011 are primitive in nature.

The IT Rules, 2011 facilitate the transfer of Personal Data of the Data Subject to a territory outside India provided; they offer the adequate level of protection. It fails to take into consideration those territories which fail to offer the necessary level of protection. Thus, the IT Rules, 2011 must take into consideration the provisions mentioned in the GDPR, 2018

which facilitate the transfer of Personal Data to a country which fails to offer the adequate level of protection. There are two solutions to this problem. The first solution is that the IT Act, 2000 and the IT Rules, 2011 must be amended to include the above provisions. The second solution is that there can be a separate statute (like the European Union) to recognize the concept of Data Protection.