European Union's General Data Protection Regulation ("GDPR")

GDPR Alert
May 25, 2018

WHAT IS GDPR?

The European Union ("EU") Parliament on April 14, 2016 approved the General Data Protection Regulation ("GDPR") – a comprehensive data protection law for the EU – with the enforcement date of May 25, 2018. Since the GDPR provides for some very drastic and cost-intensive changes from the EU's erstwhile data protection law – the Data Protection Directive 95/46/EC, it was felt that some buffer period should be given to firms and organisations to level up their existing systems and processes to implement the GDPR norms.

HOW DOES GDPR AFFECT BUSINESS?

GDPR is a major departure from the existing EU norms. It has the potential of changing many core practices of existing businesses. For example, third level data processing activities can now only take place with explicit agreement with the original data controller. Even existing database of email ID and location data of individuals in the EU would require separate consent from the data subject. The data subjects would also be required to provide additional rights like the right to erasure, right to be forgotten and right to information.

Many businesses would face difficulty in engaging with cost-effective service providers located outside the EU if the country does not have adequate level of protection. Additional compliances, which may now include establishing representative within the EU and employing a Data Protection Officer, would definitely have major cost implications for the businesses.

Finally, the penalty for non-compliance is in the tune of EURO 20 million or 4% of global turnover, which depending on the size of the business could be substantial.

WHO IS LIABLE?

At the heart of GDPR is the fact that right to privacy is a fundamental right provided to every natural individual in the EU. There are three instances of application of GDPR to an enterprise (Article 3):

1) When a data controller or processor is established in the EU (irrespective of their geographic area of operation)
2) When a data controller, established outside the EU, processes or monitors personal data of individuals who are in the EU, irrespective of whether there has been any monetary transaction with the data subject
3) When the data controller is established in place outside EU where the law of any one of EU countries apply.

Thus Article 3(2) provides for extra-territorial application of its norms to firms established outside the EU. It seems that the GDPR contemplates a very strict interpretation of application of GDPR to enterprises. According to Paragraph 23 of the narrative to the GDPR, even though the mere availability of a website in the EU does not necessarily qualify for the enterprise situated outside the EU to fall under the scope of the GDPR; additional factors such as the use of a language or a currency generally used in EU Member countries would create the assumption that the website is targeted for individuals in the EU: and as such the GDPR is applicable.

WHAT ARE THE OBLIGATIONS?

1. Establishment of Representative within the EU

Article 27 mandates that if an enterprise is not established within the EU but processes or monitors the personal data of an individual in the EU, then such enterprise, subject to a few exceptions,[1] is required to establish a

[1] Exceptions being occasional processing of large-scale data which does not include data on racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic or biometric information identifying the individual, health and sex life or sexual orientation; and public body or authority.

representative in one of the Member States of the EU where the data subject is located. The appointment of such a representative should be documented in writing.

The "representative" can either be a natural or legal person and should represent the controller or processor with regards to their obligations under GDPR. However, it is to be noted that the data controller or processor can also be prosecuted independently for any breach of GDPR norms.

The GDPR does not provide further details with respect to the representative or the nature of relationship between the enterprise and the representative (apart from the fact that such relationship should be documented in writing).

2. Designation of a Data Protection Officer ("DPO")

The concept of a Data Protection Officer ("DPO") is distinct from that of a representative of an enterprise. According to Article 37(1), designation of DPO is required by a data controller or processor when:

a) Processing carried out by public authority or body (except for courts)

b) Processing activity which inherently require large-scale regular and systemic monitoring of data subjects

c) Processing activity which consists of large scale processing of data with respect to data on racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic or biometric information identifying the individual, health and sex life or sexual orientation; or personal data relating to criminal convictions and offences.

The DPO is required to be a professional with expert knowledge of data protection law and practices. A DPO can be either a staff member or a contract service provider. The GDPR also allows a group of undertakings to appoint a common DPO. The controller or processor is also required to publish the contact details of the DPO and communicate the same with the supervisory authority.

The DPO has been provided with some level of immunity whereby the DPO will not be instructed by the data controller or processor on the mode of fulfilling his duty and he is to report directly to the Management. Additionally, the GDPR provides that the DPO will not be dismissed or penalised for the performance of his duty.

3. Ensuring the Rights of Individuals

The GDPR recognises a wide range of rights that an individual in the EU enjoys as a result of the right to privacy being a fundamental right. Herein listed below are some of the rights afforded to same under the scheme of the GDPR:

a) The Right to information about the identity of the data controller and the purposed of collection of personal data (Articles 13 and 14);

b) Right to confirm and access personal data being processed by the controller/processor. (Article 15);

c) Right to file a complaint with the supervisory authority (Article 15);

d) Right to be informed of appropriate safeguards undertaken upon transfer of personal data to a third country or international organization (Article 15);

e) Right to rectification of inaccurate personal data held with the controller (Article 16);

f) Right to obtain erasure of personal data concerning the data subject without undue delay, upon satisfaction of certain conditions (Article 17);

g) Right to restrict processing of personal data by the controller upon the existence of the stipulated conditions (Article 18);

h) Right to be notified of any rectification, erasure or restriction of processing of personal data in accordance with the above by the controller (Article 19);

i) Right to transmit the data to another controller without any hindrance. (i.e. Right to data portability, Article 20);

j) Right to object to processing of personal data. (Article 21);

k) Right of a data subject not to be subject to a decision based solely on automated processing, subject to the conditions set out. (Article 22);

4. General obligations of the controller

In addition to the satisfaction of the rights of data subjects as highlighted above, the GDPR has outlined certain general obligations of the controller in respect of personal data under Article 24.

a) To implement appropriate technical and organizational measures to ensure and demonstrate compliance under the GDPR;

b) Implement appropriate data protection policies;

c) Adherence to codes of conduct (Article 40) prescribed under the GDPR or approved certification mechanism (Article 42) to demonstrate compliance;

Further, Article 30 imposes the requirement of maintaining records of processing activities containing the information iterated and stipulated thereunder.

5. Data protection by design and default

As per the requirements of Article 25(1), the controller is required to implement appropriate technical and organizational measures, in an effective manner to integrate safeguards into the manner of processing in order to meet the requirements of the GDPR.

6. Regulation of Processors

Article 28 outlines the manner and conditions of operations of processors. It imposes the framework within which controllers may contract with processors and the subsequent compliance requirements applicable to processors, inter alia:

a) Restriction on engagement of another processor by the original processor in the absence of written authorization of the controller;

b) To only process data within the documented instructions from the controller;

c) Deletion or return of personal data upon instructions of the controller.

7. Restriction on the transfer of personal data to third country

The GDPR has instituted stringent safeguards on the transfer of personal data to third parties being countries or international organizations. Article 45 provides for the framework within which the Commission, is to decide upon countries or International organizations which are deemed to provide an "adequate level of protection" to personal data. Where such third country or international organization has been approved by the Commission, no further specific authorization would be required by controllers. However, where the standard of adequacy falls below the satisfaction of the Commission, the notification of the same may be suspended.

In the determination of the adequacy of the level of protection afforded by third countries or international organizations, certain parameters have been identified to be taken into account by the Commission:

a) The **legal framework** for the effective implementation of the data protection rules and security measures undertaken for the onward transfer of personal data to third parties;

b) The **efficacy of the independent supervisory authorities** in the country to ensure compliance with and enforcement of the data protection rules;

c) The **international commitments** of the third country in respect of protection of personal data.

Pursuant to the above, Article 46 provides that where a decision has not been arrived at by the Commission, the controller or processor may transfer personal data to a third country or international organization only where the controller/processor has provided "**appropriate safeguards**" and on the condition that enforceable rights and effective legal remedies are available for the data subjects. The appropriate safeguards may be provided for by the following means:

a) A legally binding and **enforceable instrument** between public authorities or bodies;

b) Binding **corporate rules;**

c) **Data protection clauses** adopted by the Commission as well as by the supervisory authority;

d) An approved **code of conduct** as provided under Article 40;

e) An approved **certification mechanism** in accordance with Article 42.

The safeguards highlighted herein above could also be provided for by contractual clauses or provisions inserted into administrative arrangements between public authorities or bodies.

8. Obligations in respect of breach

Article 33 provides for an event of a breach occurring in respect of personal data, where the controller is required to notify the supervisory authority within 72 hours of having becoming aware of such breach. However, this would not require to be undertaken where it is deemed that the breach would not likely result in a risk to the rights and freedoms of natural persons.

Article 34 further provides that where a breach of personal data is likely to result in a high risk to natural persons, the controller is required to communicate the same to the data subject without undue delay in simple and plain language. The requirement of intimation to the data subject is subject to the fulfilment of the conditions set out thereunder.

9. Data protection Assessment

In the event where new technology is being used for the purposes of processing, and after having taken account of the nature and scope of the same, it is determined that it is likely to result in high risk to the rights of natural persons, the controller is required to carry out an assessment of the impact on personal data prior to such commencement of processing (Article 35).

ELP ECONOMIC LAWS PRACTICE ADVOCATES & SOLICITORS

MUMBAI mumbai@elp-in.com
NEW DELHI delhi@elp-in.com
BENGALURU bengaluru@elp-in.com
AHMEDABAD ahmedabad@elp-in.com
PUNE pune@elp-in.com
CHENNAI chennai@elp-in.com