LEXCOUNSEL
LAW OFFICES

LexArticle **December 28, 2018, New Delhi, INDIA**

GDPR COMPLIANCES BY INDIAN COMPANIES – A BRIEF OVERVIEW

If you have questions or would like additional information on the material covered herein, please contact:

Ms. Seema Jhingan, Partner

(sjhingan@lexcounsel.in)

Ms. Neha Yadav, Principal Associate

GDPR COMPLIANCES BY INDIAN COMPANIES – A BRIEF OVERVIEW

The introduction of European Union's ("**EU**") regulations on protection of natural persons with regard to processing of personal data and free movement of such data ("**GDPR**") has brought on certain significant implications on Indian entities processing personal data of EU Residents. Basically, since GDPR has extra-territorial application and applies to processing of personal data of EU residents even by entities situated outside EU, Indian entities who are acting as either a 'controller' (i.e. the person who determines the purposes and means of the processing of data) or a 'processor' (i.e. the person who processes the personal data on behalf of the controller), of personal data of persons of EU, in relation to offering of goods or services to such persons or monitoring their behaviour in so far as it takes place within EU, become subject to GDPR.

We had broadly assessed the issue of when is cross-border data transfer to non-EU countries (like India) permitted and implications on Indian companies in our Earlier Article[1]. But, given the increasing impact of GDPR on Indian entities, as more and more Indian companies provide services in information technology, international e-commerce, outsourcing sectors dealing with EU residents amongst others, it is worthwhile to take a deeper look at various compliances under GDPR which an Indian business dealing with personal data of EU residents would need to comply with.

(nyadav@lexcounsel.in)

LexCounsel, Law Offices C-10, Gulmohar Park New Delhi 110 049, INDIA.
Tel.:+91.11.4166.2861
Fax:+91.11.4166.2862

Recommended by:

The concept of "*personal data*" has been defined in GDPR to refer to any information relating to an identified or identifiable natural person (i.e. "**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, and therefore all such information is considered as 'personal data' under the GDPR.

For Indian companies dealing with such 'personal data' of EU residents, it then becomes imperative to implement the data protection requirements stipulated in GDPR within their systems. This requires a significant overhaul and re-writing of their privacy policies and contractual arrangements with EU counterparts/Data Subjects and their internal data protection protocols and systems to make them GDPR compliant. Discussed below are a certain key GDPR provisions which would require adherence (depending on the role played by the Indian entities i.e. 'controllers' and 'processors' under GDPR):

(i) General Principles: Processing of personal data is to be undertaken in compliance with *inter alia* the following principles:

- Processing should be done lawfully, fairly and in a transparent manner. Particularly, for lawful processing – at least one of the prescribed requirements under GDPR are to be met, such as where the Data Subject has consented to the processing; or processing is necessary for the performance of a contract to which the Data Subject is a party; or processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority etc.

- Personal Data should be collected for specified, explicit and legitimate purposes and not further processed if incompatible with those purposes (except where specifically permitted under GDPR), and it should be adequate, accurate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Personal Data should be kept in a form which permits identification of data subjects for no longer than is necessary.

(ii) Conditions of Consent: Where processing is based on consent, obtaining of consent should be specific, informed and unambiguous. While, this could include ticking a box when visiting an internet website, but silence, pre-ticked boxes or inactivity would not constitute consent. If the processing has multiple purposes, consent should be given for all of them. If the consent is given in the context of a written declaration concerning other matters, the consent request should be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(iii) Special Categories of Personal Data: Additional requirements are to be complied with while processing of special categories of personal data; processing of personal data relating to criminal convictions and offences; and processing which does not require identification.

(iv) Information to be provided to Data Subject: The controller at the time of obtaining the personal data, is to provide the Data Subject with all the prescribed information such as identity and contact details of the controller (or it's representative); contact details of the data protection officer (if applicable); purposes and legal basis of processing; recipients or categories of recipients of the personal data; period of storage of personal data; existence of the data subject's rights such as right to access, rectification or erasure of personal data; right to data portability; right to withdraw consent; the right to lodge a complaint with a supervisory authority; etc. Information on similar lines is also to be provided to the data subject (where personal data has not been obtained from the data subject) under Article 14 of GDPR, except in certain prescribed circumstances.

(v) Rights of the Data Subject: GDPR has also provided the Data Subject with various rights, such as:

- *Right of access*: Right to obtain from the controller confirmation regarding processing of his/her personal data, and also access to the personal data and information mentioned in (iv) above.

- *Right to rectification:* Right to obtain from the controller rectification of inaccurate personal data; right to have incomplete personal data completed,

- *Right to erasure ('right to be forgotten'):* Right to obtain from the controller erasure of personal data and the controller is required to erase such personal data where one of the prescribed grounds applies such as: (a) the personal data is no longer necessary in relation to the purposes for which it was collected/processed;

(b) the Data Subject withdraws his/her consent on which the processing was based; (c) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing, etc.

- *Right to restriction of processing:* Right to obtain from the controller restriction of processing in prescribed circumstances such as where the accuracy of the personal data is contested by the data subject; the processing is unlawful etc.

- *Right to data portability:* Right to receive the personal data provided to a controller, in a structured, commonly used and machine-readable format and the right to transmit those data to another controller. This right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(vi) Responsibilities of the Controller and Processor:

- Controller should implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. Adherence to approved codes of conduct or approved certification mechanisms as specified in GDPR may be used as an element to demonstrate such compliance.

- Where processing is to be carried out on behalf of a controller, the controller is to use only processors providing sufficient guarantees to implement appropriate technical and organizational measures such that processing is GDPR compliant. The GDPR further goes on to set out in detail various requirements to be met by such processor.

- A controller is required to maintain a record of processing activities under its responsibility containing certain prescribed information. Similarly, each processor is also required to maintain a record of all categories of processing activities carried out on behalf of a controller, containing prescribed information.

(vii) Data protection by design and data protection by default: In order to be able to demonstrate compliance with GDPR, the controller should adopt internal policies and implement appropriate technical and organizational measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymising personal data[2] as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

(viii) Actions to be taken upon a personal data breach:

- In case of a personal data breach, the controller is to without undue delay (and where feasible, not later than 72 hours after having become aware of it), notify (with prescribed details) the breach to the supervisory authority in terms of GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is to communicate the personal data breach to the data subject without undue delay, with prescribed details. The controller is also required to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

- The processor is required to notify the controller without undue delay after becoming aware of a personal data breach.

(ix) GDPR also provides for carrying out of data protection impact assessment in certain cases, and designation of a data protection officer by the controller and the processor are to designate a data protection officer in certain prescribed circumstances such as where the processing is carried out by a public authority/body (except for courts); or where the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale.

Compliance with GDPR has become particularly important given the heavy penalties associated with GDPR non-compliance. Failure to comply with the GDPR requirements can attract administrative fines of up to EUR 10,00,000 or 20,000,000, or in the case of an undertaking, up to 2% or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, depending on the nature of provisions breached. Also, for Indian Company with business dealings with EU companies, their EU counterparts are also likely to insist on compliance with the GDPR as part of their standard contractual clauses. We may also add that the Indian Government is also seeking to introduce a more robust regulatory framework for data protection and privacy. Therefore, companies having business interest in EU should take comprehensive look at evolving their data protection practices not just to be GDPR compliant but also in preparation for a more stringer data protection regulatory framework likely to be introduced in India in the near future.

[1]GDPR- What It Means For Indian Business? by Seema Jhingan

[http:/www.mondaq.com/india/x/731848/data protection/GDPR What It Means For Indian Business]

[2] GDPR defines 'Pseudonymisation' as processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymised data is subject to more relaxed standards of data protection under GDPR than other personal data.

Feedback