CLIENT NOTE

GDPR in a Nutshell: Business Entities Under the Sword of Damocles!

This is the age of information. To this effect, three years ago, the GDPR was introduced in the EU. Many companies outside of the EU were very slow in internalizing the GDPR. You certainly need to know what it is and what

People increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life. People further facilitate the free flow of personal data within many states and transfer their personal to third countries and global companies.

These developments require a strong and more coherent data protection framework, backed by strong enforcement, given the importance of creating necessary trust that will allow the digital economy to develop across global markets. Hence, it becomes crucial for every state to ensure high level of the protection of personal data. Countries should take necessary measures to provide sufficient level of protection of personal data. Pursuant to the following purpose, EU has adopted an instrument called "GDPR" as a result of which, there are a number of new or enhanced data subject rights and data protection guarantees incorporated in the foregoing regulation.

DESCRIPTION AND MAIN ESSENCE OF GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as "General Data Protection Regulation" or "GDPR") has brought new challenges for the protection of Personal Data due to the fact that the scope of the collection and sharing of personal data has significantly and rapidly increased. Thus, GDPR is a legal framework that

requires businesses to protect the personal data and privacy of European Union (EU) citizens for transactions that occur within EU member states. It covers all companies that deal with the data of EU citizens, specifically banks, insurance companies, and other financial and IT companies.

WHAT IS PERSONAL DATA UNDER GDPR?

The term "Personal Data" should apply to any information concerning an identified or identifiable[1] natural person (GDPR uses the term "data subject"), e.g. name and surname, home address, email address, identification card number, social security number, Internet Protocol (IP) address, cookie ID, etc.[2]

WHAT "INNOVATIONS" AND "SURPRISES" HAVE BROUGHT THE GDPR?

Extraterritorial Scope of GDPR.

In terms of territorial scope, GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of **whether the processing takes place in the EU or not.**

Moreover, the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller **or processor not established in the Union**, where the processing activities are related to:

(i) offering of goods and services or irrespective of whether a payment of the data subject is required, to such data subjects in the Union (e.g. the organization has an official website and/or online platform which give accessibility to EU individuals for signing up for the proposed services etc.); or

(ii) monitoring of the behavior of data subjects as far as their behavior takes place within the EU (e.g. when the organization tracks EU individuals by the cookies or IP addresses etc.).

The regulations under GDPR are wider as these do not actually make any reference to citizenship. That is, the protection afforded by the GDPR should apply to natural persons,

[1] Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

[2] According to provisions of GDPR, the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

whatever their nationality or place of residence, in relation to the processing of their personal data. Hence, it applies to any data subject in the EU, i.e. a person living in the EU.

Special Permission (Definite Consent) of Data Subject.

Processing shall be lawful only if the data subject has given consent to the processing of his or her personal data for one or more specific purposes. The exceptions from this rule are provided under GDPR and are stricter. Namely, processing shall be 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, or processing shall be necessary in order to protect the vital interests of the data subject or of another natural person etc. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data (a declaration of consent) should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.

Right to be informed (Accountability).

In order to provide necessary and adequate transparency and accountability of data protection, the data controller and/or processor shall provide the data subject with the following information:

- the identity and the contact details of the controller,
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
- the categories of personal data concerned,
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
- from which source the personal data originates, and if applicable, whether it came from publicly accessible sources,
- other information that are mandatory under GDPR.

In addition to the abovementioned obligation of data processor/controller, the data subject shall be entitled to the right of accessibility towards the information provided hereunder at any time.

Existence of Legitimate and Certain Purposes (Purpose Limitation)

According to this principle the personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In other words, it should be deduced that processing of personal data shall be necessary for the purposes of the legitimate interests pursued by the controller or by a third party (when the data subject has contractual obligation under loan or other agreement etc.). However, more complicated requirements are met if the data processor is dealt with special categories of personal data.

Right to erasure ("Right to be Forgotten")

The abovementioned right implies that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him/her without undue delay and the controller shall have the obligation to erase personal data without undue delay if the personal data is no longer necessary in relation to the purposes for which the
y were collected or otherwise processed, or the personal data has been unlawfully processed. This exclusive and inalienable right shall not be applicable in "extraordinary" cases stipulated under GDPR.

Personal Data Portability

According to this new approach, the data subject shall be entitled to transmit personal data to another controller without hindrance from the controller to which the personal data has been provided. It should be noted, nevertheless, that this right is not binding for data processors or controllers as the GDPR envisages that the discussed opportunity shall be provided in cases when the processing is carried out by automated means and when such transmission of personal data is technically feasible.

Appointment of Data Protection Officer (DPO)

In order to arrange and properly manage the procedure in respect of personal data processing, the GDPR imposes that the controller and the processor shall designate a data protection officer if the core activities of the latter consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.

Furthermore, the DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection laws and practices and the ability to fulfil the tasks referred to in sections of GDPR.

Adoption of Internal Rules for Compliance

In order to have full compliance with GDPR rules, each controller and/or processor shall have internal regulations and procedures for every aspects of processing and controlling of personal data, such as code of conduct, guidelines on processing of sensitive personal data,

consent management guidelines, procedures with respect to transfer of personal data to 3rd parties.

Notification of Personal Data Breach.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent authority. Moreover, where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Administrative Fines/Penalties.

The penalties under the GDPR are essentially higher. Under the GDPR the maximum fines
for infringement of certain important provisions (not having sufficient customer consent to process data or not compliance with the mandatory requirements promulgated under GDPR) can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). Fines for violations of lower gravity (for not having personal data records in order, not notifying the supervising/competent authority and data subject about a breach or not conducting impact assessment) can amount to up to €10m or 2% of company's worldwide annual turnover (whichever is greater).

Some factors such as nature, gravity, duration as well as the number of data subjects affected and the level of damage suffered by them, the intentional or negligent character of the infringement, any actions taken by the controller or processor to mitigate the damage suffered by data subjects shall be taken into consideration as well.

HOW CAN WE HELP?

Summarizing the main features of GDPR, it should be noted that entities involved in personal data processing and controlling shall pay exclusive attention to personal data issues in order to avoid any negative impacts that may arise due to the breach of the abovementioned requirements. Taking into consideration the extraterritorial applicability of the GDPR, it is beyond any reasonable doubt, that many non-EU entities subsequently shall be subject to administrative fines and penalties envisaged under the foregoing regulation despite the fact

that respective national legislation does not provide adequate and sufficient procedures and rules in relation with protection of personal data as the GDPR does.

Our team has extensive experience in helping clients in GDPR and local data protection legislation compliance. We can help you put together efficient data protection policies and procedures in line with the existing regulatory environment. So please, do get in touch when you want to get sophisticated advice.

NOTE: This material is for general information only and is not intended to provide legal advice.

Martin Stepanyan, Associate

mstepanyan@tk.partners