KOYUNCUOĞLU & KÖKSAL

# What Are The Differences Between

# The Data Protection Law And GDPR

The General Data Protection Regulation (EU) 2016/679 (the "GDPR") which is adopted by the European Parliament on 14 April 2016 and entered into force on 25 May 2018, repealed the Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Directive") which took effect in 1998.

The Directive, which is a framework legislation, has been used as a reference for the European Union ("EU") member states for establishing their national legislation on the protection of personal data. In other words, the Directive aimed to harmonize the national laws of the member states on the protection of personal data so that the personal data would have the same level of protection under similar principles throughout the EU countries and thus, ensuring the free movement of personal data without a security threat in the said countries. However, particularly the technological developments that have taken place in the recent years and the rapid increase of data sharing as a result of such developments, have necessitated a more comprehensive legislation and consequently the GDPR has been adopted. The most important aspect of the GDPR that distinguishes it from the Directive is its direct binding nature, meaning that it is directly applicable in the national laws of all the EU member states. However, the scope of application of the GDPR is not limited to EU member states only. Regardless of where the data controller and/or data processor operates globally, all EU citizens and all the persons included in the scope of application of the GDPR are covered by the legal protection provided by the GDPR (Article 3 of the GDPR).

Considering the national legal regulations in Turkey, it is understood that the main legislation on the protection of personal data is the Data Protection Law numbered 6698 ("*Kişisel Verilerin Korunması Kanunu*") ("KVKK") and the secondary legislation related to it along with the decisions of the Board of Protection of Personal Data (the "Board") are regarded as guidelines in interpretation and implementation of the KVKK. As a matter of fact, KVKK essentially is a framework legislation just like the Directive as KVKK is copied from the EU legislation namely the Directive. However, the legal and technical details regarding the application of KVKK had and will have taken shape by the secondary legislation such as the communiqués and regulations and various decisions of the Board. What is noteworthy at this point is that the secondary legislation and the Board decisions are aligned with the GDPR and the EU's application of the GDPR.

Should a general comparison be made between the GDPR and KVKK within this framework, the following issues will be most significant.

## a) In Terms of the Definition of Personal Data

Although, essentially there does not seem to be a substantial difference in the definition of personal data in the GDPR and KVKK, it can be noted that the GDPR has a more elaborate definition of personal data in which it diversified the definition with concrete examples. Accordingly, any information relating to an identified or identifiable natural person is defined as personal data and thus any information directly or indirectly relating to an identifiable natural person particularly name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person are considered to be personal data within the meaning of GDPR.

### b) Processing of Personal Data

Any operation which is performed on personal data beginning from the first time the data is obtained means "processing" in general and there is no difference in the GDPR and KVKK in terms of this definition. 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction are considered to be "processing of personal data" (GDPR art.4/2).

### c) Data Recording System

The term "data recording system" which is used in the definition of "processing of personal data" in KVKK means the system in which the personal data is processed by being structured in compliance with specific criteria. This term seems to correspond to the definitions of "personal data filing system" in the Directive as well as "filing system" in the GDPR. As it is indicated in the reasoning of KVKK, data recording systems can be formed both in electronic or physical environment.

### d) Explicit Consent

With explicit consent which is defined as "freely given, informed consent as regards to a specific subject" in KVKK, it is meant that the data subject's statement of approval that is freely given based on sufficient information, unambiguous and limited to a specific subject, concerning the processing of her/his personal data. In many of the provisions of KVKK and secondary legislation, explicit consent of data subject is regarded as a lawful ground in terms of collection, processing and storage of personal data. Therefore, it is essential that the consent to be obtained by the data controllers to be compatible with the "explicit consent" definition in KVKK.

Although it appears that the definition of explicit consent in KVKK is in compliance with the definition in the Directive, as per article 4/11 of the GDPR "consent" is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. In this context, the expression of consent to be given unambiguously is introduced in the definition as well.

### e) Anonymization

The term "anonymization" included under article 3/1-(b) in KVKK has not been used under the GDPR and instead, the term "pseudonymization" is defined under article 4/5 titled "Definitions".

It is noteworthy to mention at this point that these two terms are not substitutable as the term "pseudonymization" is one of the technical methods which can be used in the anonymization process. Essentially, both the terms anonymization and pseudonymization mean that the identity of a specific person is no longer traceable. However, anonymization refers to a situation in which a person's identity is not known, or deliberately concealed, while the pseudonymization refers to a technical method in which the person-specific data is altered by a given algorithm with encrypted data.

Such algorithm can always calculate the same "pseudonym" by combining multiple data from various sources relating to a person.[1] Thus, such characteristic of pseudonymization distinguishes it from anonymization since it is not possible to associate multiple data obtained from various sources to a specific person using anonymization method.

Under article 6/4 of the GDPR which sets forth the lawful grounds for processing of personal data, encryption or pseudonymization are listed as appropriate safeguards which shall be taken into account by the data controller *"in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected"* under paragraph (e). In this respect, it appears that pseudonymization is regarded as an appropriate safeguard in the context of EU personal data protection laws.

### f) Liabilities and Administrative Penalties

First of all, KVKK stipulates that solely natural persons and legal entities who are data controllers shall be held liable for administrative fines arising from the non-execution of personal data processing activities in compliance with the laws. However, the corresponding GDPR provisions state that, not only data controllers but also data processors shall be held liable for administrative fines.

In terms of sanctions envisaged in the event of a possible violation, the most significant difference between the GDPR and KVKK is that the administrative fines set forth under the GDPR are much higher than those of KVKK. In other words, while the administrative fines under KVVK vary from 5.000.-TL to 1.000.000.-TL, GDPR stipulates administrative fines up to 10.000.00-EUR or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, for some violations and fines up to 20.000.000.-EUR or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, for other violations.

Regarding liability, the GDPR also stipulates that in each individual case, due regard shall be given to the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them, when deciding whether to impose an administrative fine and deciding the amount of the administrative fine. Although administrative fines are not as high as the ones under the GDPR, KVKK foresees imprisonment penalties from one to four years by reference to the relevant provisions of the Turkish Criminal Code under the chapter "Crimes and Misdemeanors" along with the administrative fines.

While the right to compensation included in KVKK is stipulated as "*Compensation rights according to the general provisions of the ones whose personal rights are violated are reserved*", GDPR grants a compensation right equivalent to the collective action system in the American legal system including collective indemnity right for those who has suffered damages during the processing of personal data such as loss of data during unlawful processing. In order to ensure an effective protection and compensation right in the field of personal data protection law, GDPR stipulates that each controller or processor shall be held liable for the entire damage where more than one controller or processor, or both a controller and a processor, are involved in the same unlawful processing of personal data (GDPR art. 82/4).

[1] https://www.ucl.ac.uk/legal-services/guidance/general-data-protection-regulation-gdpr/gdpr-anonymisation-pseudonymisation (25.07.2018).

### g) Data Portability and Impact Assessment

Another term which is not included in KVKK is the "*data protection officer*". GDPR stipulates that in certain cases where for instance the core activities of the controller or the processor consist of processing operations that by their nature require regular and systematic monitoring of data subjects on a large scale or the core activities of the controller or the processor consist of processing on a large scale of special categories of data, the data controller or the processor shall designate a data protection officer.

Also, in relation to the position of the data protection officer, another mechanism called "*data protection impact assessment*" is envisaged in GDPR under article 35. Accordingly, in case processing of personal data operations in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller is under the obligation to carry out an impact assessment of the envisaged processing operations prior to the processing. However, the data controller shall also consult to the data protection officer when carrying out a data protection impact assessment. Having said that, in KVKK, the position of data protection officer and the mechanism of data protection impact assessment are not stipulated.

Another mechanism that is foreseen under the GDPR yet not included in KVKK is the "*right to data portability*" where the data subject is granted the right to receive back the personal data that he or she provided to the data controller and transmit those data to another data controller.

In light of our above explanations, it is understood that KVKK, which is the main legislation in the protection of personal data law in Turkey, is largely in line with the Directive when evaluated together with its purpose, scope and provisions. However, shortly after the publication of KVKK in the Official Gazette, the GDPR that is prepared within the scope of the EU Data Protection Reform is adopted by the European Parliament with the aim of modernizing and amending the provisions of the Directive. In this regard, it is understood that KVKK is constructed based on the provisions of the Directive that was in force at the time and not the GDPR. However, considering the secondary legislation and the decisions of the Board, it can also be noted that the implementation of KVKK will continue to be more in line with the GDPR.

Regards,

***Koyuncuoğlu & Köksal Law Firm***