EVALUATION OF SOFTWARE SALES TO LEGAL ENTITIES (HOSPITALS, CLINICS, INSURANCE COMPANIES, BANKS ETC.) IN TERMS OF PERSONAL DATA PROTECTION LAW

Our understanding of the case

A company (non-resident of Turkey) specializing in the development of medical software considers the possibility of selling their product "Emmacheck" (hereinafter – Software) in Turkey. The Software performs calculations of the risks associated with deviations from a healthy physiological state based on a set of indicators specified in the questionnaire that should be filled in by an End user.

The Software package includes:

(1) Software - Risk Engine;

(2) Software - Licensing Server;

(3) Software - Authentication Server;

where

(1) Risk Engine is a software that analyzes depersonalized (anonymous) data of human medical parameters in a "machine-readable form" and calculates a set of risks corresponding to the transferred data set in the Risk Engine.

(2) Licensing Server and (3) Authentication Server - software that controls the access (accounting of requests) of the End User to the Risk Engine.

Access to the Software is regulated by contractual relations based on SaaS between the copyright holder, distributor and End users of the Software - Clinics, Insurance organizations, Banks, etc.

The end user has his own software that accesses the Software via the API – hereinafter referred to as the KP System (3d parties' systems).

Data from the KP System is transmitted via the API to the software (2), then there is an access to the software (3) with simultaneous access to the software (1). The data from the KP System comes depersonalized, in machine-readable form (numeric values) with a unique ID.

Depersonalization of personal (medical) data is carried out by the End User in the KP System until the data is transferred to the Software.

The end user independently fills in personal (medical) data in the KP System, is the operator of personal data and is responsible for processing personal (medical) data, taking into account the local legislation on personal data.

Examples of processed data, using the Software: age (years), height, weight, medical gender. In total, it is possible to process up to 200 parameters. DNA-related indicators are not included in this set. The option of working with non-depersonalized data is not provided in the Software

Questions for analysis

As we understand you are interested in analysis of the following questions

1) Will the organization providing the Software be recognized as the operator of personal data in accordance with Turkish law?
2) Does Turkish legislation consider software "Emmacheck" as a medical device requiring state registration?

Address: Nisbetiye Mah. Gazi Güçnar Sk. Uygur İş Merk. No: 4/5 Zincirlikuyu İstanbul
Phone: 0212 337 57 69
Fax: 0212 337 87 60
Website: www.metropolconsulting.com.tr

METROPOL CONSULTING DANIŞMANLIK LİMİTED ŞİRKETİ
Nispetiye Mah. Gazi Güçnar Sok. Uygur İş Mrk.
No:4 İç Kapı No:5 Beşiktaş / İSTANBUL
Beşiktaş V.D.:620 131 0394

Law on the Protection of Personal Data

With the enactment of Law No. 6698 on the Protection of Personal Data in 2016, new rules and obligations have emerged that data controllers and data processors must comply with. Under the KVKK (Law on the Protection of Personal Data), severe fines and imprisonment penalties are envisaged for individuals and institutions that do not comply with these obligations.

Unfortunately, it is observed that many individuals and companies in Turkey generally do not take these obligations seriously or mistakenly believe that they are exempt from the relevant provisions of the KVKK. One of the most common mistakes is that individuals and organizations believe they are exempt from this KVKK and its legal provisions, citing that they are not required to register with the Data Controllers Registry (VERBİS).

This is a completely incorrect belief, as the obligation to register with VERBİS and the obligations under the Law are independent of each other. Therefore, even individuals and organizations that do not meet the requirements for VERBİS registration must absolutely comply with the obligations of the KVKK.

Determining Compliance with the KVKK Obligations

One of the biggest issues concerning the KVKK (Law on the Protection of Personal Data) in Turkey is that companies and individuals often do not understand the scope of this law or misinterpret it. The primary reason for this is the lack of a clear understanding of the terms mentioned in the law by company officials and their incorrect evaluation. Companies with incomplete or erroneous information in this way mistakenly believe they are exempt from the provisions of the KVKK and continue their business processes without taking any precautions.

Therefore, in order to determine whether your company or business is subject to the KVKK, first need to understand what the terms "personal data," "data processing," "data controller," and "data processor" mean.

a.) Personal Data is defined quite broadly in the KVKK (Law on the Protection of Personal Data) as "any kind of information relating to an identified or identifiable natural person." By leaving such a broad and open-ended definition, any data that can identify any natural person in any way is included within the scope of personal data. For example, information such as a person's identity details, name, surname, date of birth, health information, illnesses in the past, sexual preferences, phone number, passport number, CV, photographs, images, income, spending preferences, investments, marital status, number of children, address, hobbies, phone number, email address, IP address, location data, and similar other information would be considered personal data under this definition.

b.) The Processing of Personal Data is defined in the KVKK (Law on the Protection of Personal Data) as follows: "any operation performed on personal data, whether wholly or partially by automatic means or non-automatic means, which forms part of any data recording system, such as collection, recording, storage, retention, alteration, reorganization, disclosure, transferring, taking over, making personal data obtainable, classification, or preventing the use thereof." Within this context, the mere storage of any of the personal data mentioned above by a company, even if it is not collected or used in any way, would constitute a personal data processing activity.

c.) Data Controller is defined in the KVKK (Law on the Protection of Personal Data) as "the natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data recording system." To briefly illustrate, if your company, within the scope of any activity, stores any of its customers' information such as email addresses, phone numbers, addresses, names, and surnames (or other personal data) in any way it determines or through another service provider, in this case, it will be considered a data controller under the KVKK.

According to Article 12 of the Law on the Protection of Personal Data, the data controller is obliged to:

- Prevent the unlawful processing of personal data.
- Prevent unlawful access to personal data.
- Ensure the preservation of personal data.

Address: Nisbetiye Mah. Gazi Güçnar Sk. Uygur İş Merk. No: 4/5 Zincirlikuyu İstanbul
Phone: 0212 337 57 69
Fax: 0212 337 87 60
Website: www.metropolconsulting.com.tr

METROPOL CONSULTING DANIŞMANLIK LİMİTED ŞİRKETİ
Nispetiye Mah. Gazi Güçnar Sok. Uygur İş Mrk. No:4 İç Kapı No:5 Beşiktaş / İSTANBUL
Beşiktaş V.D.:620 131 0394

To fulfill these obligations, the data controller must take the necessary technical and administrative measures. Additionally, there is an obligation for the data controller to conduct audits. The technical and administrative measures to be taken for data security may vary depending on the structure and activities of the data controller. Therefore, specific measures are not predetermined. Within the scope of these obligations, the data controller must determine and implement measures that are suitable for the nature and characteristics of data processing.

Another obligation of the data controller is to promptly notify the data subject and the Data Protection Authority (Kurul) if personal data being processed is obtained by others through unlawful means.

According to Article 16 of Law No. 6698 on the Protection of Personal Data, data controllers are required to register with the Data Controllers Registry (VERBİS) before starting data processing activities. VERBİS is a registration system where data controllers declare information about their data processing activities, the purposes for which data will be processed, whether data is transferred, and other relevant details. The registration process includes the following elements:

Identification and contact information of the data controller and, if applicable, the representative.

- Explanation of the purposes for which personal data will be processed.
- Descriptions of the data subject group(s) and categories of data related to these individuals.
- Recipients or recipient groups to whom personal data may be transferred.
- Personal data that may be transferred to foreign countries.
- Measures taken for personal data security.
- The maximum duration required for the processing of personal data for the intended purpose.
- These elements are recorded in the VERBİS system as directed by the system's guidelines.

d.) Data Processor refers to "the natural or legal person who processes personal data on behalf of the data controller, based on the authority given by the data controller." In this regard, for example, if a company outsources its accounting services to a third-party individual or company, the accounting firm that processes the information provided by the company for accounting records would be considered a data processor.

e.) Data Recording System is defined as "the system where personal data is processed in a structured manner according to specific criteria." Within this context, any system used to store/retain personal data can be considered a data recording system.

Article 7 of the Law on the Protection of Personal Data No. 6698 ("KVKK") states that even if personal data is processed in accordance with the KVKK and other relevant laws, if the reasons necessitating its processing cease to exist, personal data must be deleted, destroyed, or anonymized by the data controller ex officio or upon the request of the data subject.

The Deletion, Destruction, And Anonymization of Personal Data

According to the KVKK and the Regulation, when all the conditions for the processing of personal data have ceased to exist, personal data must be deleted, destroyed, or anonymized by the data controller ex officio or upon the request of the data subject.

In addition, all actions related to the deletion, destruction, or anonymization of personal data must be recorded, and these records must be kept for a minimum of three years as a legal obligation.

- The deletion of personal data is defined as the process of rendering personal data inaccessible and unrecoverable for the relevant users.
- The destruction of personal data, on the other hand, is defined as the process of making personal data

inaccessible, irretrievable, and unusable by anyone. In this context, the deletion of personal data is achieved by issuing a deletion command in electronic media and obscuring the data in paper form. Data destruction, on the other hand, is achieved by demagnetizing the data, rendering it unreadable, or physically rendering the storage device unusable.

- Anonymization of personal data is the process of rendering personal data such that it cannot be associated with a specific or identifiable individual, even if matched with other data. This process involves altering or removing identifiers in the dataset to prevent the identification of the individual or to remove the distinguishability within a group.

Timeframes:

The data controller must establish periodic deletion timeframes in the data destruction policy. Periodic deletion refers to the deletion, destruction, or anonymization process that is carried out at recurring intervals when all the conditions for the processing of personal data have ceased to exist.

The Regulation specifies that a data controller who has prepared a data retention and destruction policy should state in the policy that they will delete, destroy, or anonymize personal data in the first periodic deletion process following the date when the obligation to delete, destroy, or anonymize personal data arises.

The maximum duration for the periodic deletion interval is indicated not to exceed six months.

A data controller who is not obliged to prepare a data retention and destruction policy must delete, destroy, or anonymize personal data within three months following the date when the obligation to delete, destroy, or anonymize personal data arises.

If requested by the data subject, the data controller must process their request within thirty days and provide an explanation if it is denied. Additionally, if personal data has been transferred to third parties, the data controller is obliged to inform the third party and ensure that the necessary actions are taken.

If all the conditions for the processing of personal data have not ceased to exist, the data controller may reject the data subject's request within thirty days with an explanation.

Obligation to Establish a Personal Data Storage and Destruction Policy

The regulation first states that data controllers obligated to register with the Data Controllers Registry ("VERBIS") are also obligated to prepare a personal data storage and destruction policy in accordance with their personal data processing inventory.

The personal data storage and destruction policy is defined by the regulation as the policy on which data controllers base their processes of determining the maximum period necessary for the purposes for which personal data are processed and the processes of deletion, destruction, and anonymization.

Within this scope, a personal data storage and destruction policy must minimally cover the following:

- The purpose of preparing the personal data storage and destruction policy.
- Record media regulated by the personal data storage and destruction policy.
- Definitions of legal and technical terms included in the personal data storage and destruction policy.
- Explanation of the legal, technical, or other reasons necessitating the storage and destruction of personal data.
- Technical and administrative measures taken to securely store personal data and prevent their unlawful processing and access.
- Technical and administrative measures taken for the lawful destruction of personal data.

METROPOL CONSULTING DANIŞMANLIK LİMİTED ŞİRKETİ
Nispetiye Mah. Gazi Güçnar Sok. Uygur İş Mrk.
No:4 İç Kapı No:5 Beşiktaş / İSTANBUL
Beşiktaş V.D..620 131 0394

- Titles, units, and job descriptions of those involved in the storage and destruction processes of personal data.
- A table indicating storage and destruction periods.
- Periodic destruction periods.

CONDITIONS FOR PROCESSING SPECIAL CATEGORY PERSONAL DATA

Special category personal data refers to data that, if disclosed, may cause the relevant individual to suffer harm or discrimination. Therefore, they need to be protected much more rigorously than other types of personal data.

The law attaches special importance to these data and introduces different regulations regarding them. The law categorizes them as special category personal data or sensitive data. Special category personal data can be processed with the explicit consent of the individual or in the limited cases specified by the law.

The law makes a distinction among special category personal data as well. It differentiates between the processing of personal data related to health and sexual life and the processing of other special category personal data without explicit consent.

The law has specifically listed the types of data that qualify as special category personal data. These include data related to a person's race, ethnic origin, political opinions, philosophical beliefs, religion, sect, or other beliefs, appearance, membership in associations, foundations or trade unions, health, sexual life, criminal convictions, and security measures, as well as biometric and genetic data. Expanding the definition of special category personal data through analogy is not possible under the law.

It should be noted that, like all fundamental rights and freedoms, protection regarding special category personal data is not absolute; it can be limited, as with other rights and freedoms, but such limitations must comply with the principles set forth in Article 13 of the Constitution. Therefore, the specific conditions and circumstances under which special category personal data can be processed are defined in the law. Indeed, the exercise of many fundamental rights and freedoms, such as the right to life, freedom of expression, and freedom of communication, may necessitate the processing of special category personal data. In this regard, it is not possible to categorically prohibit the processing of special category personal data.

According to the law, special category personal data can be processed with explicit consent. Furthermore, under the law, special category personal data, except for data related to health and sexual life, can only be processed in the cases foreseen by the laws. Data related to health and sexual life can be processed without the explicit consent of the data subject only for the purposes of protecting public health, conducting preventive medicine, providing medical diagnosis, treatment and care services, planning and managing health services and their financing, and by individuals or authorized institutions and organizations who are under the obligation of confidentiality.

CONCLUSION:

Will the organization providing the Software be recognized as the operator of personal data in accordance with Turkish law?

As mentioned, health data is considered as special category data under the KVKK (Personal Data Protection Law). When processing special category data like health data, specific obligations must be fulfilled, and measures for data security should be taken.

Therefore, all private legal entities and individuals providing health services under the Ministry of Health and thus processing health data are required to comply with the KVKK law and follow the Regulation on Personal Health Data.

A health service provider includes any organization that provides or produces health services. This includes various organizations of different sizes, from large hospitals to clinics, pharmacies, and other healthcare entities.

Address: Nisbetiye Mah. Gazi Güçnar Sk. Uygur İş Merk. No: 4/5 Zincirlikuyu İstanbul
Phone: 0212 337 57 69
Fax: 0212 337 87 60
Website: www.metropolconsulting.com.tr

METROPOL CONSULTING DANIŞMANLIK
LİMİTED ŞİRKETİ
Nispetiye Mah. Gazi Güçnar Sok. Uygur İş Mrk.
No:4/İç Kapı No:5 Beşiktaş / İSTANBUL
Beşiktaş V.D.:620 131 0394

From this understanding, whether it's due to the anonymization of data, preventing access to an individual patient's personal data, or ensuring that the collected data is processed in compliance with the KVKK, the responsibility lies with the hospital. Therefore, the company providing the Software "Emmacheck" does not have a direct responsibility in this regard as a software provider to hospitals.

In this context, such company is simply a service provider selling or leasing software to hospitals. Additionally, hospitals use multiple computer programs, such as patient tracking systems and accounting software, and the responsibility for all personal data entered into these applications lies with the hospital, not the software provider.

However, you should still assist hospitals in anonymizing, deleting, or destroying this personal data if needed. For example, as you described, ensuring that all data entered into the program arrives with an anonymous ID.

Does Turkish legislation consider the Software "Emmacheck" as a medical device requiring state registration?

There is no requirement to obtain a license or registration for this software in Turkey within the framework of the Ministry of Health. Licensing requirements typically apply to products such as pharmaceuticals, herbal medicines, vitamins, medical devices, biocidal products, and homeopathic medical products, for which approvals from the Ministry of Health or in some cases, the Ministry of Agriculture and Forestry, may be necessary.

We do not anticipate the need to register or obtain approvals for the software that will be sold to hospitals because it is not a pharmaceutical product or any type of medical device. For example, pharmaceuticals require licenses and have specific regulatory authorities for approval, but there is no such requirement or regulatory body for software.

05/10/2023

METROPOL CONSULTING DANIŞMANLIK
LİMİTED ŞİRKETİ
Nisbetiye Mah. Gazi Güçnar Sok. Uygur İş Mrk.
No:4 C Kapı No:5 Beşiktaş / İSTANBUL
V.D.:620 131 0394

Address: Nisbetiye Mah. Gazi Güçnar Sk. Uygur İş Merk. No: 4/5 Zincirlikuyu İstanbul
Phone: 0212 337 57 69
Fax: 0212 337 87 60
Website: www.metropolconsulting.com.tr