BIOLEGIS – DATA PROTECTION QUESTIONNAIRE (TURKEY)

QUESTIONS:

Accountability, Processing in Third Countries, and Information

(A) **Are there any special requirements, by way of law of practice, for technical and organisational measures with regard to the processing of genetic-, biometric-, or health data in your jurisdiction?**

Pursuant to Article 6 of the Turkish Data Protection Law numbered 6698 ("**DPL**"), personal data relating to the health, sexual life, biometric and genetic data are deemed to be sensitive personal data. While the DPL was originally based on the Directive 95/46/EC, it introduces further measures with regard to the processing of sensitive data when compared withthe GDPR and health data is process in limited conditions.

In that regard, the DPL states that sensitive personal data may only be processed with the explicit consent of the data subject.

While sensitive personal data other than data relating to health and sexual life may be processed without seeking explicit consent of the data subject in the cases provided for by other laws, personal data relating to health and sexual life may only be processed without seeking explicit consent of the data subject, by persons or authorised public institutions and organizations that have a confidentiality obligation, only for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing. The

restriction brought under the DPL leaves very limited room for processing of health data without explicit consent.

You may find the English translation of the DPL on the following website of the Personal Data Protection Board of Turkey: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf

Moreover, Article 6/4 of the DPL also states that the adequate measures determined by the Personal Data Protection Board ("**Board**") should also be taken while processing sensitive personal data

In that regard, the Board's decision numbered 2018/10 on the adequate measures to be taken by data controllers in processing sensitive personal data has been published in the Official Gazette no. 30353 dated 7 March 2018.

Accordingly, data controllers processing genetic-, biometric-, or health data should take the following measures in addition to acquiring the explicit consent of data subjects;

- The establishment of a separate privacy policy and procedures specific for the security of sensitive personal data
- Taking the following precautions regarding the employees in the processing of sensitive personal data;
  - Regular training about the DPL, its secondary legislation and the security of sensitive personal data
  - Signing special confidentiality agreements
  - Clearly determining the scope and duration of user access to sensitive data
  - Regularly performing authorization controls
  - Instantly revoking access of employees who resign or change positions and taking back the assigned data inventory
- Taking the following precautions if sensitive personal data is processed in digital form;
  - Storing the data using cryptographic methods,
  - Storing cryptographic keys in secure and various environments
  - Securely logging transaction records of all transactions on the data
  - Continuously checking security updates for the environments where the data is stored, regularly conducting security tests and recording test results
  - Applying access authorizations, conducting regular security tests and recording test results if the data is processed via a software,
  - Applying two-factor authentication if remote access to the data is required,
- Taking the following precautions if the sensitive personal data is being processed in a physical environment;
  - Ensuring that adequate security precautions are taken according to the nature of the environment in which personal data is stored
  - Ensuring the physical security of these environments by preventing unauthorized entry and exit.
- Taking the following precautions for the transfer of sensitive personal data;
  - Encrypting the data and using the corporate e-mail address or the Registered Electronic Mail (KEP) address if the data is transferred via e-mail
  - Encrypting the medium by cryptographic methods and cryptographic keys if it needs to be transferred via a medium such as portable memory, CD, DVD
  - Establishing a VPN or using a sFTP method if sensitive personal data is transferred between servers in different physical environments
  - Taking necessary precautions against risks such as theft, loss or unauthorized viewing of documents and sending the documents in a "confidential" format if sensitive personal data needs to be transferred physically on printed paper

(B) **Is there any specific additional requirements over the GDPR in your jurisdiction to conduct a DPIA in the context of processing genetic-, biometric-, or health data?**

Contrary to the GDPR, the concept of a DPIA is not introduced within the DPL. Therefore, there are no requirements in the Turkish jurisdiction to conducts a DPIA in the context of processing genetic, biometric or health data.

(C) In connection with the processing of genetic-, biometric-, or health data, are there any special requirements regarding the drafting of information according to articles 12 through 14 GDPR in your jurisdiction?

There are no special requirements regarding the drafting of information forms with regard to the processing of genetic, biometric or health data under Turkish jurisdiction. General information obligation envisaged under the DPL applies to processing of genetic, biometric or health data.

(D) Are there special requirements in your jurisdiction for the processing of genetic-, biometric-, or health data in third countries?

Pursuant to the DPL, processing genetic, biometric or health data in any third country out of Turkey will be deemed a transfer of the data abroad. While there are no special requirements for the transfer of sensitive data to third countries compared to non-sensitive data, the DPL does not give required comfort to implement GDPR requirements with respect to the transfer of personal data abroad. Thus, the special measures foreseen for the processing of sensitive data explained under Question (A) are also applicable for the processing of genetic, biometric or health data in third countries.

In that regard, any personal data including genetic, biometric or health data can be transferred abroad:

- if the relevant data subject gives her/his explicit consent for such transfer, or
- If the recipient country provides sufficient safeguards in case that there is any other legal reason to process such data rather than explicit consent, or
- If the data controller has obtained special permission from the Data Protection Board for such transfer.

As of May 2019, countries in the secure countries list is not determined yet by the Board and not expected to be determined soon. Therefore, the data controllers, which do not receive consent from data subject as having other legal grounds to process and transfer such data (such as legal interest, performance of agreement etc.), shall obtain a special permission from the Data Protection Board. For this, both the transferring and the recipient data controllers must submit written undertakings stating that they will provide sufficient protection.

Consent

(E) Describe any relevant restrictions on the use of consent as a lawful basis of processing of genetic-, biometric-, or health data, particularly as to whether local authorities interpret that a consent for secondary processing purposes (such as research) could not be validly obtained, or would be subject to significant limitations, when obtained from patients in the course of a) provision of healthcare services, b) clinical trials, or c) research, other than a clinical trial.

Pursuant to Article 6 of the DPL, sensitive personal data may only be processed with the explicit consent of the data subject. While sensitive personal data other than data relating to health and sexual life may be processed without seeking explicit consent of the data subject in the cases provided for by other laws, personal data relating to health and sexual life may only be processed without seeking explicit consent of the data subject, by persons or authorised public institutions and organizations that have a confidentiality obligation, only for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

In that regard, in the current situation, the DPL forces the data controllers to rely on explicit consent as a lawful basis of processing of genetic, biometric or health data.

(F) **Describe any relevant local limitations (either by way of local legislation or practice) on how broad data subject consent for research purposes may be, particularly in light of the GDPR allowing consents to be for a certain "field of research".**

Pursuant to Article 28 of the DPL, the DPL shall not be applied to personal data that is processed with scientific purposes, provided that national defence, national security, public security, public order, economic security, right to privacy or personal rights are not violated or that they are processed so as not to constitute a crime.

However, the scope of this Article is substantially limited since it states that the data should be processed without violating the right to privacy and that it does not constitute a crime. Thus, the unlawful processing of personal data is also regulated under the Turkish Penal Code and therefore, any processing that is not carried out in compliance with the DPL would automatically constitute a crime.

In that regard, it is advised to obtain consent for only a limited field of research and a broad consent of the data subject may discredit the validity of the consent.

Additional Restrictions on Processing

(G) **Other than as described above, has your jurisdiction used the right for members states to impose further restrictions on the processing of genetic-, biometric-, or health data? Please describe any relevant restrictions.**

Since Turkey is not a member state of the European Union, the DPL is not regulated under the GDPR. The further restrictions on the processing of genetic, biometric or health data under the DPL are described under Question (A) above.

Recent Developments

(H) **In the context of processing of health data, are you aware of any enforcement action by data protection authorities in you jurisdiction. Please describe any relevant recent developments.**

We are aware of two enforcement actions of the Board specifically related to the processing of health data to this date.

In its decision dated December 5th 2018 and numbered 2018/143, the Board has evaluated the complaint of a data subject regarding the transfer of his/her health data (the drugs used by the patient) by the pharmacy who supplied the drugs to the patient, to third persons without relying on any legal grounds. In that regard, the Board has imposed an administrative fine on the pharmacy. However, the details on the penalty is not shared by the Board.

In another summary decision published by the Board on its website without a decision number or a date, it is stated that the Board has imposed an administrative fine on a hospital since a healthcare professional employed by the hospital has shared a screenshot taken from the hospital's database application on social media. The Board's legal basis for this administrative fine was that the hospital was obliged to take all necessary technical and administrative measures to provide a sufficient level of security in order to ensure the retention of personal data pursuant to Article 12/1(c) of the DPL.

(I) **Please describe any other recent relevant developments in your jurisdiction with respect to processing of genetic-, biometric-, or health data which may be of interest.**

There are no other recent developments in Turkey with respect to the processing of genetic, biometric or health data that are known.

On the other hand, it should be mentioned that the current mechanism foreseen under the DPL for the processing of genetic, biometric or health data is widely accepted to be problematic for the time being. Under the current law, data controllers other than persons or authorised public institutions that have a legal confidentiality obligation (such as healthcare professionals) can only rely on the explicit consent of the data subjects as the legal ground for processing genetic, biometric or health data. Hence, even though data controllers such as pharmaceutical companies may have legal obligations to process health data (such as data regarding adverse events), they are forced to rely on the explicit consent of the data subjects, which can also be revoked by the data subject anytime. In that case, such data controllers are compelled to make a risk-assessment and choose between violating the DPL or other laws obliging them to collect and transfer health data. While there are no recent developments on this issue, the sector is expecting an amendment on the problematic Article 6 which would introduce more legal grounds for more data controllers regarding the processing of health data.