MOROĞLU ARSEVEN

# The Guidelines on Matters to Be Considered in the Processing of Genetic Data by the Personal Data Protection Authority Has Been Published.

*1 Nov 2023*

The Draft Guidelines on Matters to Be Considered in the Processing of Genetic Data was published by the Personal Data Protection Authority on 24 August 2022. As of 13 October 2023, the finalized version of the Guidelines on Matters to Be Considered in the Processing of Genetic Data has been shared with the public on the official website of the Personal Data Protection Authority.

Many provisions previously included in the Draft Guidelines on Matters to Be Considered in the Processing of Genetic Data ("**Draft Guidelines**"), published by the Personal Data Protection Authority ("**Authority**"), have also been incorporated into the Guidelines on Matters to Be Considered in the Processing of Genetic Data ("**Guidelines** "). *For detailed information regarding the Draft Guidelines, you can refer to the content titled "Draft Guidelines on Matters to Be Considered in the Processing of Genetic Data" in the Updated Version of Turkish Data Protection Law - Developments in Practice in the Seventh Year of 2023.*

The Guidelines provides detailed information on the following aspects:

- Definition of genetic data,
- Data controller, data processor, data subject, and general principles within the scope of the Personal Data Protection Law ("**DP Law**") in the process of processing genetic data,
- Evaluation of genetic data processing within the framework of personal data processing conditions stipulated in the DP Law and its cross-border transfer,
- Obligations of the data controller in genetic data processing and technical and administrative measures related to genetic data security,
- Recommendations and suggestions related to genetic data processing.

***Definition of Genetic Data***

Genetic data, considered as special category data under Article 6 of the DP Law, has received a comprehensive definition for the first time in the Guidelines. The Guidelines includes the definition within the scope of the European Union General Data Protection Regulation ("**GDPR**"). Ultimately, genetic data is described as "*all or part of the information obtained from the whole DNA, RNA, and protein sequence encoded from the cell nucleus or mitochondria of a living organism. Genetic data can range from a single nucleotide polymorphism (SNP) to comprehensive information about the entire genome sequence. These data encompass all genetic changes, whether hereditary or non-hereditary, derived from the DNA and/or RNA obtained from a living organism*". Furthermore, it is emphasized that genetic data should be considered:

- As requiring analysis to be meaningful or informative.
- As valuable and meaningful even before the analysis of raw data and biological samples, with the potential to identify an identifiable individual.
- With the possibility that samples taken from deceased individuals may be analyzed in a way that could identify an identifiable individual years later.

***In the processing of genetic data, the roles of data controller, data processor, data subject, and general principles under the scope of DP Law have considered as follows:***

*Data Controller:* Genetic Diseases Evaluation Centers must obtain a license from the Ministry of Health to operate, as per the Genetic Diseases Evaluation Centers Regulation. In this regard, tests related to the diagnosis of genetic diseases, the response to various diseases, determining whether an individual carries a gene responsible for a disease, or revealing genetic predisposition or sensitivity to a disease can only be conducted in Genetic Diseases Evaluation Centers, provided that it is for medical necessity or for medical scientific research and with the provision of appropriate genetic counseling services. The Guidelines also specifies that the Ministry of Health and universities will have the status of data controllers.

*Data Subject:* The Guidelines emphasizes that in the process of processing genetic data, data related to individuals who are genetically related to the data subject may also be processed. Hence, processing data of other individuals can serve a different purpose.

*General Principles and Retention Period under Legislation:* Genetic data shall be processed in accordance with the general principles of DP Law. In this context, it is essential to retain the processed genetic data for the necessary period and to ensure their immediate deletion when no longer required, in accordance with the personal data retention and disposal policy. According to the Genetic Diseases Evaluation Centers Regulation, reports and records in these centers must be retained for at least 30 years, electronic records should be backed up indefinitely, and samples and slides must be stored for a minimum of two years under appropriate conditions.

***Evaluation of Genetic Data under the Personal Data Processing Conditions in DP Law and its International Transfer***

Genetic data can be processed with the explicit consent of the data subject. The Guidelines clarifies that obtaining the explicit consent of data subject with processed genetic data is not merely about having them read and sign an explicit consent form; it is emphasized that data subject must clearly understand the genetic data processing activity and its outcomes. Moreover, genetic data may be processed without the consent of the data subject for mandatory tests in line with health requirements under Article 6/3 of the DP Law, within the framework of protective healthcare, medical diagnosis, treatment, and care services.

In the Guidelines, it is mentioned that the sending of samples abroad under the "Regulation on Genetic Diseases Evaluation Centers" can be registered through the licensed genetic diseases evaluation centers authorized by the Ministry of Health. Additionally, human-origin biological samples for examination purposes shall be recorded in the Ministry of Health's tracking system. As a result, the sending of samples abroad for non-operational tests can only be carried out through the "Foreign Biological Material Transfer System" securely and appropriately under the control of the Ministry of Health, facilitated by licensed Genetic Diseases Evaluation Centers and medical laboratories. Furthermore, it is stipulated that the authority to send samples abroad for examination purposes, according to the "Regulation on Medical Laboratories," may only belong to licensed medical laboratories, and the entry and exit of human-origin biological samples for examination purposes can be conducted with the approval of the Ministry of Health.

***Data Controller's Obligations***

*Obligation to inform:* The Guidelines emphasizes that providing a general information alone is insufficient when it comes to informing data subjects whose genetic data is being processed. In this regard, data subjects shall be separately informed about which genetic data is collected for what legal reasons and purposes, the significance of this data, and potential consequences in case of a breach (risks associated with processing genetic data). Data subjects shall clearly understand that the processing of genetic data can provide access not only to their data but also to the data of other family members. Furthermore, it is emphasized that the concept of "information" mentioned in the Patient Rights Regulation is distinct from the "notification" required under DP Law and does not replace explicit

consent.

Additionally, genetic data processors, as data controllers, are obliged to *register with the Data Controllers Registry ("**VERBIS**")* and *take the necessary technical and administrative measures*.

***Genetic Data Security***

The Guidelines highlights the need to adhere to the provisions set out in the Personal Data Protection Board's Decision dated 31 January 2018 and numbered 2018/10 regarding "Adequate Measures to be Taken by Data Controllers in the Processing of Special Category Personal Data." In addition to these general provisions, the Guidelines recommends specific measures that data controllers should take regarding genetic data processing:

*Technical Measures*

- *Storage of Genetic Data in the Cloud:* The Guidelines suggests that genetic data should not be stored in cloud systems. If it is necessary to process genetic data in a cloud, the following precautions are advised:
- Detailed records should be kept of the genetic data stored in the cloud,
- Backups should be maintained outside of the cloud,
- Remote access to genetic data in the cloud should employ a two-factor authentication control,
- Genetic data in the cloud should be encrypted using cryptographic methods that provide sufficient security,
- Industry standards and best practice examples, which include algorithms found in standardized and secure cryptographic algorithm suites, should be used for applications, devices, and systems,
- If non-standard cryptographic algorithms are deemed necessary, an analysis and evaluation of their security should be conducted by an authorized crypto-analysis laboratory before their use,
- A clear policy on encryption and key management should be defined,
- Access to cryptographic keys should be limited to authorized personnel with cryptographic security clearance (crypto security certificate),
- Whenever possible, separate encryption keys should be used for each cloud solution, especially for each cloud service provider.
- In cases where devices are delivered to authorized companies for maintenance, repair, or return of leased devices, data storage units on the devices should be removed or all data should be transferred to a hard disk and a written commitment from the company should be obtained, stating that there is no data on the company's devices or servers.
- Prior to system installation and after any changes, the system should be tested in testing using synthetic data (non-real data) whenever possible.
- In test studies using real data, genetic data should be processed in compliance with the data minimization principle.
- Measures that warn and report unauthorized access to the system or protect genetic data should be implemented.
- Certified equipment, licensed and up-to-date software should be used, patch management should be ensured, open-source software should be preferred whenever possible, and necessary updates to the system should be performed in a timely manner.
- User operations on genetic data processing software should be monitored and restricted. Transaction logs for all actions performed on the genetic data processing program/system should be maintained separately and securely.
- Hardware and software security tests of systems processing genetic data should be conducted periodically.
- Compliance with the measures outlined in the "Information and Communication Security Measures General Directive" numbered 2019/12 and the Information and Communication Security Guidelines, prepared under the coordination of the Presidency's Digital Transformation Office, should be considered.

*Administrative Measures*

- Although not covered by Turkish legislation, the Guidelines emphasizes the need to establish and manage genetic data based on the "Privacy by Design" principle and implement Data Protection Impact Assessments, as terms stated in the GDPR.

- Genetic data must be securely stored and accessible only by personnel who are authorized, trained, and have signed confidentiality agreements.
- A Personal Data Processing Inventory should be prepared, and notifications should be made to the VERB?S.
- Separate processing policies, emergency procedures, and reporting mechanisms should be established for genetic data processing processes.
- Genetic data stored electronically should be regularly backed up using a secure backup system, and backup data sets must be kept offline.
- The obligation to provide detailed and compliant information should be fulfilled, and explicit consent should be obtained from the data subject if necessary.
- Through internal random and periodic audits and risk analyses, the data controller should continuously assess and monitor their preparedness for a potential data breach resulting from genetic data processing activities.
- Service agreements with data processors in genetic data processing processes should include the necessary security measures, and periodic audits should be conducted or commissioned at the data processor's end to ensure that the required technical and administrative measures are in place.
- The data controller should document and publicize the fact that all of the above principles and criteria are met.

***Recommendations and suggestions***

As stated in the Presidential Circular No. 2019/12 on "Information and Communication Security Measures," it is emphasized that genetic data shall be considered as critical information and securely stored domestically. In this regard, it is recommended to process genetic data in accordance with national and international standards and information security criteria, as outlined in the "Information and Communication Security Guidelines" published by the Presidency's Digital Transformation Office.

You can access the Guidelines through this link.

## Related Practices

- Privacy and Data Protection

## Related Attorneys

- BURCU TUZCU ERS?N, LL.M.
- CEYLAN NEC?PO?LU, Ph.D, LL.M.