KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

GUIDELINE ON CONSIDERATIONS IN THE PROCESSING OF BIOMETRIC DATA

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

GUIDELINE ON CONSIDERATIONS IN THE PROCESSING OF BIOMETRIC DATA

Kişisel Verileri Koruma Kurumu
Address: Nasuh Akar Mahallesi 1407. Sokak No: 4 Balgat-Çankaya/ANKARA
Telephone: +90 312 216 50 00
Web: www.kvkk.gov.tr

INTRODUCTION

The Law on Protection of Personal Data (Law) No. 6698, adopted by the Turkish Grand National Assembly on 24.03.2016, in order to protect the fundamental rights and freedoms of individuals, especially the privacy of private life, and to regulate the obligations of natural and legal persons processing personal data and the procedures and principles to be followed in the processing of personal data, was published in the Official Gazette dated 07.04.2016 and numbered 29677 and entered into force.

Article 6 of the Law, titled "Conditions for processing of Special categories of personal data", states that "personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data are deemed to be special categories of personal data."

Biometric data, which is counted among the special categories of personal data by the law, has not been defined comprehensively in the legislation published to date. However, the definition of biometric data in Article 4 of the European Union General Data Protection Regulation (GDPR), which made significant changes and brought innovations in the field of personal data protection, is considered to be the most comprehensive definition ever made in this field. According to this definition, 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological[1] or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic[2] data. As included in the definition of GDPR, in order for personal data to have the quality of biometric data;

1 Physiological: Related to physiology, related to the body, (https://sozluk.gov.tr/)
2 Dactyloscopy: Fingerprint-based identification method (https://sozluk.gov.tr/)

- Distinctive features of the person, such as physiological, physical or behavioral characteristics, should be revealed as a result of data processing,

- The features uncovered must be personal data that serve to identify the person or verify the identity of the person.

It has been seen that definitions regarding biometric methods were also included in some judicial decisions before the adoption of the law. For instance; *"It is stated that biometric methods refer to authentication techniques that can be automatically verified and performed through measurable physiological and individual characteristics, and these methods include fingerprint recognition, palm scanning, hand geometry recognition, iris recognition, face recognition, retina recognition, DNA recognition.*[34]*"*

Based on these definitions, "biometrics" refers to the physical or behavioral characteristics of human beings, and biometric data is personal, unique. Biometric data is data that people cannot forget, generally does not change for a lifetime, and is easily owned without the need for any intervention[5]. Thanks to the use of biometric data, it becomes very easy to distinguish people from each other and the possibility of confusion with each other is almost eliminated.

While biometric data such as fingerprint, retina, palm, face, hand shape and iris constitute physiological biometric data; biometric data such as the person's walking style, pressing the keyboard, and driving style constitute behavioral biometric data. Physiological biometric data constitute the whole of the features that we carry in our body, such as fingerprints, retina and iris, which are generally unchangeable.

3 Decision No. 2014/4562 of the 15th Chamber of the Council of State

4 In addition to the definition of the Council of State, it should be noted that face geometry is also treated like hand geometry.

5 Satapathy S. C. & Joshi A. (2017). Information and Communication Technology for Intelligent Systems (ICTIS2017), Bhatnagar S. Cooperative Multimodal Approach for Identification – (Volume 1, s. 13-18)

Behavioral biometric data, on the other hand, are behavioral characteristics such as gait, movements to scroll the screen while using smartphones and similar devices, the way of pressing the keyboard, and the way of driving a car.

In the processing of biometric data, the existence of biometric data processing conditions and compliance with the general principles regulated in Article 4 of the Law are important. According to the third paragraph of Article 6 of the Law, personal data, except for data concerning health and sexual life may be processed without seeking explicit consent of the data subject, in the cases provided for by laws. In this framework, biometric data will be processed in the cases stipulated by the laws if there is no explicit consent. As it can be understood from the aforementioned Law provision, in the event that other laws expressly include provisions on the processing of biometric data, the provisions of the relevant laws will be applied. For example, the regulation regarding the receipt of biometric data in order to benefit from health services in Article 67 of the Social Insurance and General Health Insurance Law No. 5510 and the regulations in the Article 7 of the Population Services Law No. 5490, including the biometric data information in the family registers, are examples of the situations envisaged in the laws. In other words, if biometric data processing is prescribed by law, it is considered that the provision in question should be clear enough to leave no room for doubt.

In addition, **the general principles set out in Article 4 of the Law must always be followed** in the processing of biometric data. Article 4 of the Law titled “General Principles” stipulates that personal data shall only be processed in compliance with procedures and principles laid down in this Law or other laws.

It has been regulated that the following principles shall be complied within the processing of personal data: *"a) Lawfulness and fairness, b) Being accurate and kept up to date where necessary, c) Being processed for specified, explicit and legitimate purposes, ç) Being relevant, limited and proportionate to the purposes for which they are processed, d) Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed."*

In addition to the existence of the conditions stipulated in the Law on whether the biometric data is processed in accordance with the law, it is also important to make comments within the framework of the concrete case. As a matter of fact, evaluations on explicit consent and proportionality are included in the "The Decision of the Decision of the Personal Data Protection Board dated 25/03/2019, numbered 2019/81 and the Summary dated 31/05/2019, numbered 2019/165 regarding the entry-exit control of the members of the data controllers providing the gym service by processing biometric data", published on the website of our Authority. It should be noted that the Board may make different decisions in different situations, to the extent required by the concrete case and in accordance with the Law.

In order to clarify the issues of biometric data processing, this Resolution on Guideline has been prepared regarding the issues to be considered in the processing of biometric data, which is considered as special quality personal data in Article 6 of the Law.

BIOMETRIC DATA PROCESSING PRINCIPLES

1. The data controller will only be able to process biometric data in accordance with the general principles set forth in Article 4 of the Law and the conditions set forth in Article 6, only in line with the principles set forth below.

a) Not to touch the essence of fundamental rights and freedoms: Since the right to protect personal data is one of the fundamental rights and freedoms regulated in the Constitution of the Republic of Türkiye (Constitution), it is clear that biometric data processing activities should also be subject to fundamental guarantees in terms of fundamental rights and freedoms stipulated in the Constitution, and at this point, the issue of proportionality is of great importance.

b) The method used is suitable for achieving the purpose of processing, the data processing activity is suitable for the purpose to be achieved: With this principle, it is stated that the method to be used by the data controller in terms of the purpose the data controller wants to achieve is suitable. In the decision of the Constitutional Court dated 28.09.2017 and numbered E.2016/125, K.2017/143, eligibility is defined as "the rule that is brought is suitable for the purpose to be achieved". The biometric data processing activity must be suitable for the purpose to be achieved, and if the desired result can be approached with the help of the tool, that tool will be considered suitable[6].

c) The necessity of biometric data processing method in terms of the aim to be achieved: as emphasized in the decision of the Constitutional Court dated 28.09.2017 and numbered E.2016/125, K.2017/143; The principle of necessity is that when there is more than one tool that allows the same goal to be achieved, the least intrusive tool is chosen among them[7].

6 Metin, Yüksel, (2017) Limitation of Fundamental Rights and Proportionality. SDÜHFD, Vol:7, Issue:1, p. 8-9
7 Metin, Y. s.11

If the same or better result can be achieved with a less restrictive intervention, the tool used in this context will be against the principle of necessity[8]. In other words, if there is any alternative to biometric data processing, the biometric data will not be processed, since it will not be necessary to process the biometric data. With the Decision of the Personal Data Protection Board (Board) dated 25/03/2019 and numbered 2019/81 and its decision dated 31/05/2019 and numbered 2019/165, this has been expressed as: *"(...) While it is possible to control the entrance and exit of the sports club and to provide the entrance control for the people who want to benefit from the club services by alternative means, it has been stated that the receipt of palm print data, which is in the nature of biometric data, does not comply with the principle of "being relevant, limited and proportionate to the purposes for which they are processed" in paragraph (2) of Article 4 of the Law on the Protection of Personal Data No. 6698. (...)".*As stated in the aforementioned Board Decision, the processing of biometric data will not be proportional if there is any alternative.

In this context, to explain the situation of finding an alternative with two examples; in the Decision made by the Board, it is foreseen that the gym will use a system for the same purpose with different means instead of receiving biometric data at the entrances and exits; biometric systems can be used, which is a more convenient and necessary method for Nuclear Power Plant entrance and exit, which requires a high level of security. Except for these two obvious examples, in every concrete case, interpretation should be made by looking at the purpose, the data controller who processes biometric data should clearly state why he is processing the data and prove that he has to process it.

ç) <u>Finding a proportion between the purpose and the tool to be achieved by data processing:</u> In the decision of the Constitutional Court dated 28.09.2017 and numbered E.2016/125, K.2017/143, proportionality was defined as *"the measure*

8 Metin, Y. s.11

that should be between the rule introduced and the aim to be achieved". The proportionality principle is the situation in which there is a measured proportion between the means and the purpose[9]. The tool used should not be disproportionate to the aim to be achieved. At the point of biometric data processing, there should be proportionality between the severity of the intervention and the reasons justifying the intervention; that is, disproportionate interventions should not be made to the persons involved as a result of the vehicle used[10]. In the case of more than one vehicle, choosing the most suitable vehicle means proportionality.

Let's say that in a company researching dangerous viruses, the lab is secured with doors that open only after successful fingerprint and iris scan verification. If this method is implemented to ensure that only persons trained in procedures familiar with the particular risks and deemed trustworthy by the company can test these hazardous materials, the company's legitimate interest in ensuring that only authorized persons can access it to ensure that the security risks associated with accessing that restricted area can be mitigated will significantly invalidate the request not to process the biometric data of the data subjects.

d) Obtaining it for as long as necessary, and destroying the said data without delay/immediately after the necessity disappears.

e) Limited in line with the purpose of processing; data controllers fulfill their obligation to inform in accordance with Article 10 of the Law: As it is known, in addition to Article 10 of the Law regarding the fulfillment of the obligation to inform, the *"Communiqué on the Procedures and Principles to be Complied with in Fulfilling the Obligation to Inform"* was published in the Official Gazette on 10.03.2018 and entered into force.

9 Metin, Y. s.13
10 Metin, Y. s.14

As well as the provisions of the aforementioned legislation are complied with, data controllers who will process biometric data due to the importance of biometric data are also concerned about which biometric data is collected for which legal reason and for what purpose, the importance of these data, the consequences that may arise in case of violation (risks for the processing of biometric data) should also inform data subjects.

f) If explicit consent is required, the explicit consent of the data subjects has been obtained in accordance with the Law: : In subparagraph (a) of the first paragraph of Article 3 of the Law titled "Definitions", explicit consent is defined as "freely given, specific and informed consent". In order for the explicit consent given for data processing to be valid, the explicit consent must first be given on a specific subject and limited to that subject. However, since explicit consent is a declaration of will, one must also know what one is consenting to in order to consent freely. The person must have full knowledge not only of the subject matter, but also of the consequences of his/her consent[11]. . For this reason, information must be provided in a clear and understandable manner on all matters related to data processing and must be made before the data is processed.

On the other hand, in order for explicit consent to be valid, the person must be conscious of his/her behavior and make his/her own decision. Since explicit consent must be disclosed with free will, the presentation of any product and/or service (or benefiting from any product and/or service) should not be conditional on explicit consent by the data subject, in cases where the parties are not in an equal position or one of the parties has an effect on the other, it should be carefully evaluated whether the consent is given freely[12]. *F*or example, in the employee-employer relationship, in cases where the possibility of not giving consent to the worker is not effectively offered or where non-consensibility will cause a possible negative situation for the worker, it cannot be accepted that the consent is based on free will[13].

11 Personal Data Protection Authority. "Explicit Consent", s.510 Metin, Y. s.14
12 Personal Data Protection Authority. "Explicit Consent", s.6
13 Personal Data Protection Authority. "Explicit Consent", s.6a

2. The fact that all the above-mentioned principles are met should be recorded and documented by the data controller.

3. Unless necessary, genetic data (blood, saliva, etc.) should not be obtained while biometric data is being obtained.

4. In the selection of the type or types of biometrics (iris, fingerprint, vascular network of the hand, etc.), justifications and documentation should be provided as to why the preferred type or types of biometric data were chosen over others.

5. In accordance with the principle of keeping for the period required for the purpose for which they are processed or stipulated in the relevant legislation in subparagraph (d) of the first paragraph of Article 4 of the Law, the maximum period for the processing of personal data should be determined. In this framework, there may be periods arising from the legislation in determining the periods, or there may be periods that are not due to the legislation but to be determined by the data controllers. However, all variants of the biometric feature (raw and derived records, etc.) must be processed for the required time; the reasons for how long the said data will be kept should be explained by the data controller in the personal data retention and destruction policy.

BIOMETRIC DATA SECURITY

Data controllers who process biometric data are required to pay attention to the personal data security issues included in laws, regulations, communiqués and board decisions. In this framework, in the processing of special categories of personal data; it is obligatory to take the measures specified in the Board's decision dated 31/01/2018 and numbered 2018/10 on *"Adequate Precautions to be Taken by Data Controllers in the Processing of Special Categories of Personal Data"*. However, appropriate measures should be taken into account in the guide documents prepared by the Personal Data Protection Authority in order to guide data controllers. In this context, the data controller should take the necessary technical and organizational measures in order to ensure the security of the data regarding the nature of the data and the possible risks that the data processing may pose for the data subject. In addition to the data security measures in the aforementioned legislation and guides, data controllers should also take the following measures regarding biometric data processing.

1. Technical Measures:

a) Biometric data should only be stored in cloud systems using cryptographic methods.

b) Derived biometric data should be stored in a way that does not allow the recovery of the original biometric feature.

c) Biometric data and its templates should be encrypted in accordance with current technology, with cryptographic methods that will provide adequate security. The encryption and key management policy should be clearly defined.

ç) Before installing the system and after any changes, the data controller should test the system through synthetic data (not real) in the test environments to be created.

d) The data controller should limit the use of biometric data to what is necessary in the studies to be carried out for testing purposes. All data should be deleted at the end of the tests at the latest.

e) The data controller should implement measures that warn the system administrator and/or delete and report biometric data in case of unauthorized access to the system.

f) The data controller should use certified equipment, licensed and up-to-date software in the system, prefer open source software first and make the necessary updates in the system in a timely manner.

g) The lifetime of devices that process biometric data should be traceable.

ğ) The data controller should be able to monitor and limit user actions on the software that processes biometric data.

h) Hardware and software tests of the biometric data system should be performed periodically.

2. Organizational Measures:

a) An alternative system should be provided without any restrictions or additional costs for the persons who cannot use the biometric solution (biometric data is impossible to record or read, handicap situation that makes it difficult to use, etc.) or who do not have explicit consent to use it.

b) A plan of action should be established in case of failure of authentication by biometric methods (failure to verify an identity, lack of authorization to enter a secure area, etc.).

c) Access mechanism to biometric data systems of authorized persons should be established, managed and those responsible should be identified and documented.

ç) Personnel involved in the biometric data processing process should receive special training on the processing of biometric data and such training should be documented.

d) A formal reporting procedure should be established so that employees can report possible security vulnerabilities in systems and services and threats that may arise as a result of such vulnerabilities.

e) The data controller should establish an emergency procedure to be implemented in the event of a data breach and announce it to everyone concerned.

REFERENCES

- Satapathy S. C. & Joshi A. (2017). Information and Communication Technology for Intelligent Systems (ICTIS 2017), Bhatnagar S. Cooperative Multimodal
- Approach for Identification – (Volume 1)
  Metin, Yüksel, (2017) Limitation of Fundamental Rights and Proportionality. SDUHFD, Volume: 7, Issue: 1
- Personal Data Protection Authority, “Explicit Consent”

Nasuh Akar Mahallesi 1407. Sokak No: 4 Balgat-Çankaya/ANKARA

0 (312) 216 50 00 // www.kvkk.gov.tr