# DATA PROTECTION IN TÜRKİYE

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

# DATA PROTECTION IN TÜRKİYE

54

**DATA PROTECTION IN TÜRKİYE**

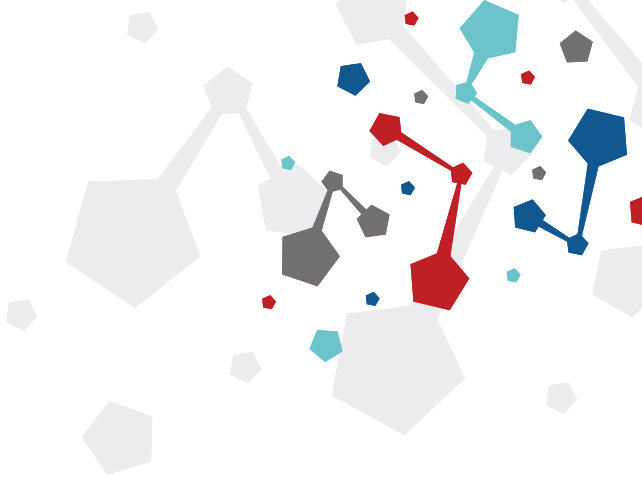
KVKK Yayınları No: 54

Mart 2025, Ankara

**KİŞİSEL VERİLERI KORUMA KURUMU**

Adres: Nasuh Akar Mahallesi 1407. Sokak No: 4 Çankaya/ANKARA
Telefon: 0 312 216 50 00

Web: www.kvkk.gov.tr



# CONTENT

# DATA PROTECTION IN TÜRKİYE

# DATA PROTECTION IN TÜRKİYE

The Personal Data Protection Law No. 6698 came into force after its publication in the Official Gazette No. 29677 on 7 April 2016. Turkish Data Protection Authority was established under the same Law and is located in Ankara.

Personal Data Protection Authority, which is a public legal entity and possesses administrative and financial autonomy, has been established to carry out duties conferred on it under the Law No. 6698. The Authority is composed of the Personal Data Protection Board and the Presidency.

Personal Data Protection Board consists of nine members. Five members of the Board are elected by the Grand National Assembly of Türkiye, two members by the President of the Republic and two members by the Council of Ministers.[1] The selection and appointment process of the Board members was completed at the end of 2016 and the Board started its duty on 12 January 2017 after the members took the oath before the First Presidency Board of the Court of Cassation.

[1] According to Article 163 of the Decree Law no: 703 (02/07/2018), the amendment of the paragraph 2 of article 21 shall come into force. Five members of the Board are elected by Grand National Assembly of Türkiye, four members by the President of the Republic.

The mission of the Authority is to ensure the protection of personal data and develop awareness in this respect in the public eye in line with the fundamental rights related with privacy and freedom stipulated in the Constitution, as well as to establish an environment to enhance the capability of competition of the public and private organizations in the data-driven world. Our vision is to be a globally recognized competent authority which is influential in the protection of personal data and to raise the public awareness in this regard.

## What is Personal Data?

Personal Data is any information relating to an identified or identifiable natural person such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Basically, two criteria are used to distinguish between personal data and non-personal data. Accordingly, to identify any data as a personal data, the data must be relevant to a person and this person must be identified or identifiable.

## Special categories of personal data

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.

Special categories of personal data, if obtained by others, can leave the data subject open to discrimination or unfair treatment. For this reason, sensitive personal data merits specific protection than other personal data.

## Who is Data Subject?

Only data of the natural persons is protected under the Law. Therefore, the term *"data subject"* is used in the Law to refer to natural person whose personal data is being processed. As expressly stated in the definitions of the Law, the person to be protected is *"natural person"*.

## Who is Data Controller?

Data controller is the natural or legal person who determines the purposes and means of the processing of personal data and is responsible for the establishment and management of the data filing system.

Legal persons are themselves *"controllers"* in processing of personal data; therefore, the responsibility specified in the relevant regulations belong to the legal persons themselves. There is no difference between public legal entity and private legal persons in this regard.

In other words, according to the Law data controller determines the purposes for which and the means by which personal data is processed. So, it is the person who decides 'why' and 'how' the personal data should be processed.

## What is Processing of Personal Data?

Processing of personal data is any operation performed on personal data, wholly or partially by automated means or

non-automated means which provided that form part of a data filing system, such as collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization, preventing the use thereof.

## General Principles in Processing of Personal Data

The procedures and principles for the processing of personal data in the Law are regulated in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108 and the European Union Data Protection Directive 95/46/EC. The following general principles set out in the Law shall be complied with while processing personal data:

- Lawfulness and fairness
- Being accurate and kept up to date where necessary.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

The principles regarding the processing of personal data should be at the core of all personal data processing activities and all personal data processing activities must be carried out in accordance with these principles.

## Conditions for Personal Data Processing

### *a) Conditions for Personal Data*

Personal Data is any information relating to an identified or identifiable natural person.

Personal data shall not be processed without explicit consent of the data subject.

Personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:

- It is expressly provided for by the laws.
- It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.
- Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract.
- It is necessary for compliance with a legal obligation to which the data controller is subject.
- Personal data have been made public by the data subject himself/herself.
- Data processing is necessary for the establishment, exercise or protection of any right.
- Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing

does not violate the fundamental rights and freedoms of the data subject.

Conditions regarding the processing of personal data are limited under the Law and cannot be extended. It is not necessary to obtain explicit consent in cases where data processing is based on the conditions which are referred to in the Law other than explicit consent. Obtaining explicit consent when there is another legal basis to process the data is misleading and deemed as a violation of rights by the data controller. In case data subject withdraws his/her explicit consent, the continuation of processing data, which is based on the other legal basis, by the data controller is deemed as processing against the rule of the lawfulness and fairness.

Therefore, it is necessary to determine whether the purpose of the processing of personal data by the data controller is based on one of the processing conditions other than explicit consent. If this purpose is not based on at least one of the conditions which are referred to in the Law other than explicit consent, it is necessary to obtain explicit consent of the data subjects for data processing.

***b) Conditions for Special Categories of Personal Data (Sensitive Personal Data)***

Sensitive Personal Data, if obtained by others, can make the data subject vulnerable to discrimination or unfair treatment. For this reason, sensitive personal data needs to be protected more strictly than the other personal data. Sensitive personal data can only be processed with the explicit consent of the data subjects or with any of the conditions set out by the Law.

Sensitive data is explicitly defined in the Law. 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 is deemed to be sensitive data. These are limited by the Law, so it is not possible to extend them by comparison.

Special categories of personal data may be processed only in cases where one of the following conditions is met:

- There is explicit consent of the data subject.
- It is expressly provided for by the laws.
- It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.
- It is related to personal data have been made public by the data subject and is in accordance with the will to make public.
- It is necessary for the establishment, exercise or protection of any right.
- It is necessary 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 by the persons subject to secrecy obligation or competent public institutions and organizations.


KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

- It is necessary to fulfill legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance.
- It is carried out in accordance with legislation they are subject to or their purposes and limited to the areas of their activities by a foundation, association or any other not-for-profit organization or formation with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members and companions of the organization or formation or to persons who have regular contact with them and that the personal data are not disclosed outside that organization or formation.

Adequate measures determined by the Board shall be also taken while processing the special categories of personal data.

## Key Points on Explicit Consent

Explicit consent is defined as the consent that relates to a specified issue, declared by free will and based on information.

Under the Law, explicit consent means giving consent to the processing of personal data by free will or upon other party's request. The data subjects actually express decision on their legal value to the data controller with explicit consent. The statement of explicit consent will also enable the data subjects to determine the limits, scope and manner in which the data is allowed to be processed.

In this sense, explicit consent must include *"positive declaration of intention"* of the data subject who consents. Without

prejudice to the regulations in the other legislation, it is not necessary to obtain explicit consent in writing. It is also possible to obtain explicit consent through other methods such as electronic media and call center etc. The controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Under the definition of explicit consent set out in Article 3 of the Law, explicit consent has 3 elements which are as follows:

- Related to a specified issue,
- Based on information,
- Declared by free will.

General explicit consent, which is not restricted to a specified issue and the relevant transaction, is accepted as "*blanket consent*" and is considered legally invalid. For example; consent statements which do not indicate a specified issue or activity, such as "*all kinds of commercial transactions, banking transactions and data processing activities*" can be deemed blanket consents.

Explicit consent is a strictly personal right of the individual. Therefore, since data subjects have the right to determine the future of their personal data, they can withdraw their consent at any time.

However, as withdrawal of explicit consent will have forward-looking results; all transactions carried out on the basis of explicit consent must be stopped by the data controller as soon as it receives the withdrawal statement.

## Transfer Of Personal Data

### *a) Transfer of Personal Data in Türkiye*

Article 8 of the Personal Data Protection Law stipulates that personal data which is obtained within the framework of the general principles specified in the Law can only be transferred in the conditions set out in Articles 5 and 6 of the Law to the third parties. On the other hand, processing of personal data lawfully in Türkiye does not mean that the data can be directly transferred to the third parties. Conditions set out in Articles 5 and 6 of the Law are also required for the transfer of personal data. Under Article 8 of the Law, transferring personal data in Türkiye may take place in case one of the following conditions is met:

- Explicit consent of the data subject,
- It is expressly provided for by the laws.
- It is necessary for the protection of life or physical integrity of the person himself/ herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.
- Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract.
- It is necessary for compliance with a legal obligation to which the data controller is subject.
- Personal data have been made public by the data subject himself/herself.

- Data processing is necessary for the establishment, exercise or protection of any right.
- Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

The Provisions of other laws relating to transfer of personal data are reserved.

If transfer of sensitive personal data is to take place, one of the following conditions must be met:

- There is explicit consent of the data subject.
- It is expressly provided for by the laws.
- It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.
- It is related to personal data have been made public by the data subject and is in accordance with the will to make public.
- It is necessary for the establishment, exercise or protection of any right.
- It is necessary 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 by the persons subject to secrecy obligation or competent public institutions and organizations.

- It is necessary to fulfill legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance.
- It is carried out in accordance with legislation they are subject to or their purposes and limited to the areas of their activities by a foundation, association or any other not-for-profit organization or formation with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members and companions of the organization or formation or to persons who have regular contact with them and that the personal data are not disclosed outside that organization or formation.

Personal data is the information relating to only the natural person. However, *"data controller"* and *"data processor"* can be both natural person and legal person. Any natural or legal person who carries out a transaction on personal data is either a data controller or a data processor according to the purpose and method relating to the data processing. In this context, it is necessary to comply with the Article 8 of the Data Protection Law for all kinds of data transfer between these persons.

***b) Transfer of Personal Data Abroad***

Under Article 9 of the Law, a cross-border transfer may take place in cases where one of the following conditions is met:

- Personal data may be transferred abroad by data controllers and data processors upon the existence of one of the conditions referred to in Article 5(2) and Article 6(3) of the Law and

there is an adequacy decision about the country, industries in the country or international organizations that personal data are to be transferred.

- Adequacy decisions are made by the Board and these decisions are published in the Official Gazette. Where necessary, the Board receive the opinions of relevant institutions and organizations. The adequacy decision is re-evaluated at least every four years. According to the results of the evaluation and to the extent necessary, the Board may repeal, amend or suspend the adequacy decision without retro-active effect.

When making an adequacy decision, the issues below are taken into account:

a) the state of reciprocity relating to the transfer of personal data between the country, industries in the country or international organizations that personal data are to be transferred and Türkiye.

b) the relevant legislation and its implementation in the country and the rules governing the international organization to which the personal data are to be transferred.

c) the existence of an independent and effective data protection authority and the availability of administrative and judicial remedies in the country to which the personal data are to be transferred.

ç) the status of the country or international organization to which the personal data are to be transferred about being

a party to international agreements on the protection of personal data or a member of international organizations.

d) the status of the country or international organization to which the personal data are to be transferred about being a member of global or regional organizations which Türkiye is a member.

e) the international agreements to which Türkiye is a party,

- If adequate protection is not provided, upon the existence of one of the conditions referred to in Article 5(2) and Article 6(3) of the Law and on condition that enforceable data subject rights and effective legal remedies for data subjects are available, data controllers or data processors may transfer personal data to abroad only if one of the conditions that are listed below are available:

  a) The existence of an agreement that is not an international agreement between public institutions or organizations abroad or international organizations and public institutions or organizations in Türkiye and the authorization of the Board for the transfer.

  b) The existence of approved binding corporate rules by the Board that include provisions with respect to personal data protection and companies within the enterprise group engaged in a joint economic activity are obliged to comply with.

  c) The existence of a standard contractual clause that is announced by the Board and contains matters like data categories, purposes of data transfers, recipient and re-

cipient groups, technical and organizational measures to be taken by data importer and additional measures to be taken for sensitive personal data.

ç) The existence of a written commitment that includes provisions providing adequate protection.

- The standard contract clause is notified to the Authority by data controller or data processor within five weekdays after it is signed.
- If there is neither an adequacy decision nor one of the conditions above, data controllers and data processors may transfer personal data abroad extrinsically if one of the conditions below are available:

a) Explicit consent of data subject is available provided that he or she is informed about possible risks.

b) The transfer is necessary for the performance of a contract between data subject and data controller or the implementation of precontractual measures that is taken by the request of data subject.

c) The transfer is necessary for the establishment or performance of a contract that will be signed between data controller and the other natural or legal person on behalf of data subject.

ç) the transfer is necessary for important reasons of public interest;

d) the transfer is necessary for the establishment, exercise or protection of any right.

e) the transfer is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.

f) the transfer is made from a register which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by relevant legislation for consultation are fulfilled and the being of request of the person who has legitimate interest.

- Subparagraphs of (a), (b) and (c) do not apply for the activities of public institutions or organizations on condition that these activities are subject to public law.
- The conditions laid down and provisions of this article in this Law are complied with by the data controller and the data processor, including for onward transfers of personal data transferred abroad before and transfers to an international organization.
- Without prejudice to the provisions of international agreements, in cases where interest of Türkiye or the data subject will seriously get harmed, personal data, may only be transferred abroad upon the authorization to be given by the Board after receiving the opinions of relevant public institutions and organizations.
- The Provisions of other laws relating to the transfer of personal data abroad are reserved.

- The procedures and principles regarding the implementation of this article shall be laid down through by-law.

## Rights of the Data Subject

Data Subjects have the right to;

- Make a request to the data controller
- Lodge a complaint with the Board

***a) Right to Make a Request***

Pursuant to Article 13 of the Law, data subjects can submit his/her request relating to the implementation of the Law to the data controller.

Natural persons whose personal data is processed have right to request to data controllers within the scope of their rights specified in Article 11 of the Law. This right consists of the following:

- to learn whether his/her personal data are processed or not,
- to demand for information as to if his/her personal data have been processed,
- to learn the purpose of processing of his/her data and whether these personal data are used in compliance with this purpose,
- to know the third parties to whom his/ her personal data are transferred in country or abroad,
- to request the rectification of the incomplete or inaccurate data, if any, to request erasure or destruction of his/her personal data, under the conditions referred to in Article 7,

- to request reporting of the operations carried out pursuant to sub-paragraphs (d) and (e) to third parties to whom his/her personal data have been transferred,
- to object to the occurrence of a result against the person himself/herself by analyzing the data processed solely through automated systems,
- to claim compensation for the damage arising from the unlawful processing of his/her personal data.

Data subjects shall make a request to data controllers within the scope of their rights specified in Article 11 of the Law, in writing or by registered electronic mail (KEP) address, secured electronic signature, mobile signature or by the e-mail address which has been previously entered into the data controllers' system or through a software or application designed for purposes of this request.

The data controller is obliged to take necessary organizational and technical measures to conclude the requests to be made by data subjects within the scope of the Communiqué, effectively and complying with norms of lawfulness and fairness.

Data controller shall act on the requests or refuses them together with justified grounds. Data controller shall communicate its response to the data subjects in writing or by electronic means.

Data controllers shall conclude the demands in the request within the shortest time by taking into account the nature of the demand and at the latest within thirty days and free of

charge. However, if process requires additional costs, fees may be charged in the tariff specified in Article 7 of the Communiqué. If the request is caused due to the fault of the data controller, the fee is refunded to data subject.

***b) Right to Lodge a Complaint***

If the request is refused, the response of the controller is found insufficient or the request is not answered by the controller within 30 days, data subjects may lodge a complaint with the Board within thirty days as of they learn about the response of the data controller, or within sixty days as of the request date, in any case. Data subjects shall not contact to the Board before exhausting the remedy of the request to the data controller.

Article 15 of the Law provides for the procedures and principles of the examination to be made by the Board.

Accordingly, the Board shall make the necessary examination in the matters falling within its task upon complaint or ex officio, where it learns about the alleged infringement. This examination shall comply with alleged infringement upon complaint or ex officio. Complaints not meeting conditions laid down in Article 6 of the Law No. 3071 of 1/11/1984 on the Use of Right to Petition shall not be examined.

As the request is mandatory and the complaint is optional, a data subject whose request has been refused implicitly or explicitly may both lodge a complaint with the Board and resort directly to the judicial or administrative jurisdiction.

Article 15 of the Law determines the procedures and principles of the examination to be made by the Board.

The Board shall finalize the examination upon complaint and give an answer to data subjects. Upon complaint, The Board examines the demand and gives an answer to the data subjects. In case the request isn't responded in sixty days from the date of complaint the demand shall be deemed refused.

Except for the information and documents having the status of state secret, the controller shall send the information and documents demanded by the Board related to the subject of examination within fifteen days, and shall enable, where necessary, on-the-spot examination.

Following the examination made upon complaint or ex officio, in cases where it is understood that an infringement exists, the Board shall decide that the identified infringements shall be remedied by the relevant controller and notify this decision to relevant parties. This decision shall be implemented without delay and within thirty days at the latest after the notification. Following the examination made upon complaint or ex officio, in cases where it is determined that the infringement is widespread, the Board shall adopt and publish a resolution in this regard. Before adopting the resolution, the Board may also refer to the opinions of relevant institutions and organizations, if needed.

The Board may decide that processing of data or its transfer abroad should be stopped if such operation may lead to damages that are difficult or impossible to compensate for and if it is clearly unlawful.

It is possible for the interested parties to file an action at the administrative courts against decisions made by the Board.

## Obligations of the Data Controller

### *a) Obligation to Inform*

The Law gives data subjects the right to be informed about by whom, for what purposes and for which legal reasons/ basis their data is to be processed, for what purposes and to whom the data may be transferred, and these issues are addressed under the obligation to inform of the controller.

Under Article 10 of the Law, at the time when personal data is obtained, the controller or the person authorized by it is obliged to inform the data subjects about the following:

- the identity of the controller and of his representative, if any,
- the purpose of processing of personal data,
- to whom and for which purposes the processed personal data may be transferred,
- the methods and legal basis of collection of personal data,
- other rights referred to in Article 11.

The controller is obliged to inform to the data subjects when the data processing adheres to the explicit consent of the data subject or processing is carried out under another condition of the Law. That is, the data subjects should be informed in every situation where their personal data is processed.

The following procedures and principles must be followed at the time of the fulfilment of the obligation to inform by the data controller or the person authorized by it by using physical or electronic media such as oral or written statement, voice recording, call center.

- The obligation to inform shall be fulfilled in any cases where the data processing adheres to the explicit consent of the data subject or processing is carried out under another condition.
- In case the purpose of personal data processing changes, the obligation to inform shall be fulfilled for new purpose prior to start of data processing.
- Fulfilment of the obligation to inform does not depend on the request of data subject.

***b) Erasure, Destruction or Anonymization of Personal Data***

Pursuant to Article 7 of the Law, despite being processed under the provisions of the Law, personal data shall be erased, destructed or anonymized by the controller ex officio or upon the request of the data subject, in the event that all of the conditions for processing laid down in Articles 5 and Article 6 of the Law no longer exist.

Obligations of the controller are to erase, destruct or anonymize personal data in cases where the reason of processing no longer exists. It is not necessary for the data subjects to request for such operations. However, in the event of negligence of the controller, data subjects have the right to request that personal data shall be erased, destructed.

The controller, who prepared personal data storage and disposal policy, shall erase, destruct or anonymize personal data in the first periodic disposal process following the date on which the obligation to erase, destruct or anonymize personal data occurs within the framework of the By-Law on Erasure,

Destruction or Anonymization of Personal Data. Erasure of personal data is the process of rendering personal data inaccessible and non-reusable for the relevant users, by no means.

Destruction is the process of rendering personal data inaccessible, irretrievable or non-reusable by anyone, by no means.

Anonymization is the process of rendering personal data impossible to link with an identified or identifiable natural person, even matching them with other data.

The data controller is obliged to take any type of technical and organizational measures related to erasure, destruction or anonymization of personal data.

Data controllers who are obliged to register with Data Controllers' Registry system shall issue personal data storage and disposal policy in accordance with personal data processing inventory.

Data controllers, who have issued data storage and disposal policy pursuant to the By Law on Erasure, Destruction or Anonymization of Personal Data, shall erase, destruct or anonymize the personal data in the first periodic disposal process following the date for obligation of erasure, destruction or anonymization of personal data arises.

Data controllers must also describe the methods used for the erasure, destruction and anonymization operations of personal data in the relevant policies and procedures.

All operations relating to erasure, destruction and anonymization of personal data shall be recorded and those records

shall be stored for minimum three years excluding other legal obligations.

Unless otherwise decided by the Board, the data controller may choose one of the appropriate methods for periodic erasure, destruction or anonymization of personal data ex officio. Upon the request of data subject, data controller may choose appropriate method with justified grounds.

The Board issued By-Law on Erasure, Destruction or Anonymization of Personal Data to determine principles and procedures regarding erasure, destruction and anonymization of personal data processed wholly or partially by automated means or non-automated means which provided that form part of a data filing system.

In addition, a Guide on Erasure, Destruction or Anonymization of Personal Data (*"Guidelines"*) has been prepared by the Board to draw attention to various topics in order to clarify the implementation and how to create good practice examples based on the By-Law.

***c) Data Security Requirements***

According to Article 12 on data security of the Law, the controller is obliged to take all necessary technical and organizational measures to provide an appropriate level of security for the purposes of;

- preventing unlawful processing of personal data,
- preventing unlawful access to personal data,
- ensuring protection of personal data.

The Board has the power to take regulatory action in order to determine security requirements. Additional measures may be taken according to the nature of the sector-specific processed data by taking into account the minimum criteria determined by the Board.

In case the processing of personal data is carried out by another natural person or legal person on behalf of the data controller, the controller shall jointly be responsible with these persons for taking the necessary measures. Therefore, data processors are also obliged to take measures to ensure data security.

Accordingly, for example, if the records of the data controller's company are held by an accounting company (data processor), the controller shall jointly be responsible with the accounting company for taking the measures regarding the processing of the data.

The controller is also obliged to carry out the necessary audits, or have them made, in its own institution or organization, in order to ensure the implementation of the provisions of the Law. The controller can conduct this audit by itself or have them conducted through a third party.

The data controllers and the data processors shall not disclose the personal data that they have obtained to anyone contrary to the provisions of this Law and they shall not use such data for purposes other than that for which the personal data have been processed.

The controllers and processors shall remain responsible for this obligation even after the end of their term of office.

In case the processed data is obtained by others by unlawful means, the data controller shall communicate the breach to the data subject and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through other methods it deems appropriate.

The appropriate measures to be taken regarding data security shall comply with the structure, activities and risks of each data controller. For this reason, a single model of data security cannot be envisaged. In determining the appropriate measures, the nature of the data controller's task and the personal data to be protected are also important, as well as the size and balance sheet of the company.

Adequate measures determined by the Board shall be also taken while processing the special categories of personal data.

In this context, 'Personal Data Security Guide' has been prepared by the Personal Data Protection Authority in order to clarify the technical and organizational measures in practice to be taken by the controller and to form good practice examples during the processing of personal data.

***d) Obligation to Register to Data Controllers' Registry***

Pursuant to Article 16 of the Law natural or legal persons who process personal data shall register with the Data Controllers' Registry prior to the start of data processing.

The procedures and principles related to the Data Controllers' Registry have been determined by the *"By-Law on the Data Controllers' Registry"*.

### i. What is Data Controllers' Registry

Data Controllers' Registry (VERBİS) is an information system that is accessible on the Internet and established and managed by the Presidency under supervision of the Board. Data controllers will use this system for the registration with the Registry and other operations related to the Registry. The aim of the system is to announce who the data controllers are and to ensure exercise the right of personal data protection more effectively.

### ii. Exemptions from Registration Obligation

All data controllers are obliged to register with the Data Controller's Registry System (VERBİS) prior to the processing of data. However, Article 16 regarding the obligations of registration with the VERBİS shall not be applied in the cases set forth in the second paragraph of Article 28.

The Law authorizes the Board to provide derogation from obligation to register with the Data Controllers' Registry by taking into consideration the objective criteria set by the Board such as the nature and quantity of data processed, the purpose of processing of personal data, the field of activity where personal data is processed, whether data processing is laid down in the laws, group of persons subject to the data or categories of data, the annual number of employees or annual financial balance sheet of the data controller.

Aim of the obligation to register is to establish a safer and transparent environment in terms of clarification of personal data processing and to act in compliance with the legislation for controllers.

### iii. Information to be entered within the scope of the registration obligation

Data controllers shall provide the following information to register with Data Registry System (VERBIS):

- The information included in the application form determined by the Board relating to the identity and residential and business address of the data controller, representative of data controller, if any and contact person,
- The purposes for which the personal data will be processed,
- The explanations relating to group(s) of persons subject to the data and the data categories of these persons,
- The recipients or groups of recipients to whom personal data may be transferred,
- The personal data which is envisaged to be transferred abroad,
- Measures taken concerning the security of personal data as referred in Article 12 of the Law and in accordance with the criteria determined by the Board,
- Maximum storage period of personal data laid down by the legislation or for the purposes for which personal data is processed.

In case of any change in the Registry records, data controllers shall notify the Authority through VERBİS within seven days of the date of change.

***e) Obligation to Respond to the Request of Data Subject***

Pursuant to Article 13 of the Law, data subjects shall make the requests relating to the implementation of this Law to the data controller in writing or by other means to be determined by the Board. The data controller shall conclude the demands in the request within the shortest time by taking into account the nature of the demand and at the latest within thirty days and free of charge. However, if the action requires an extra cost, fees in the tariff may be charged determined by the Board.

The fee set by the Board is covered in the 'Communiqué on Procedures and Principles of the Application to Data Controllers'. The data controller shall act on the request or refuse it with justified grounds and communicate its response to the data subject in writing or electronic means (such as registered e-mail address, a secure electronic signature, a mobile signature or an e-mail). In case the demand in the request is accepted, it shall be fulfilled by the data controller.

However, if the action requires an extra cost, fees may be charged laid down in the tariff determined by the Board. If the request of the data subject is to be responded in writing, no fee will be charged up to ten pages. 1 Turkish lira may be charged per page over ten pages.

If the request is made due to fault of the data controller, the fee is refunded to data subject.

In cases where the request is responded by means of recording medium like CD, flash memory, fee to be charged by data controller cannot exceed the cost of the recording medium.

If the request is refused, the response is found insufficient or the request is not responded within the specified time period, the data subject may lodge a complaint with the Board within thirty days as of he/she learns about the response of the data controller, or within sixty days as of the request date, in any case.

***f) Obligation to Fulfil the Board Decisions***

As a result of the examination made upon complaint, or ex-officio in cases where it is understood that an infringement exists, the Board shall decide that the identified infringements shall be remedied by the relevant data controller and notify this decision to the relevant parties. This decision shall be implemented without delay and within thirty days at the latest after the notification.

**The Guidelines which we have published so far:**

- The Guideline Regarding Good Practices for Personal Data Protection in the Banking Sector
- Guideline on the Cookie Practices
- Right to be Forgotten (Evaluation of the Right to be Forgotten in Terms of Search Engines)
- Considerations for the Processing of Biometric Data
- Recommendations on the Protection of Personal Data in the Field of AI
- Considerations for Protection of Children's Personal Data
- Guide on the Preparation of Personal Data Processing Inventory

- Guide on the Fulfilment of the Obligation to Inform
- The Personal Data Protection Law in 100 Questions
- Implementation Guideline on the Protection of Personal Data Law
- Personal Data Security Guidelines (Technical and Organizational Measures)
- Guideline on Erasure, Destruction or Anonymization of Personal Data
- Frequently Asked Questions About the Personal Data Protection Law
- Right to Request the Protection of Personal Data as a Constitutional Right
- Data Controller and Data Processor
- Data Controllers' Registry
- Methods for Seeking Rights of Data Subject
- Rights and Obligations Under the Law
- Processing Conditions for Personal Data
- Key Principles Regarding the Processing of Personal Data
- Explicit Consent
- Basic Concepts in the Law No. 6698
- Terms in the Law No. 6698
- Purpose and Scope of the Personal Data Protection Law No. 6698

- International and National Regulations for the Protection of Personal Data
- The Need for the Protection of Personal Data Protection Law
- Processing Conditions for Sensitive Personal Data
- Transfer of Personal Data Abroad
- Structure and Duties of Personal Data Protection Board


%
5
^
6
&
7
*
8
T
Y
U
F
K
V
M
C
10
15
20
5
25
0
30
35

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Adres: Nasuh Akar Mahallesi
1407. Sokak No: 4
Çankaya/ANKARA
Telefon: 0 312 216 50 00
Web: www.kvkk.gov.tr

kvkkurumu