



KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

DATA PROTECTION IN TURKEY

Nasuh Akar Mah. 1407. Sokak No:6 06520
Balgat-Çankaya/Ankara
Tel: 0 (312) 216 50 50 // www.kvkk.gov.tr



DATA PROTECTION
IN TURKEY

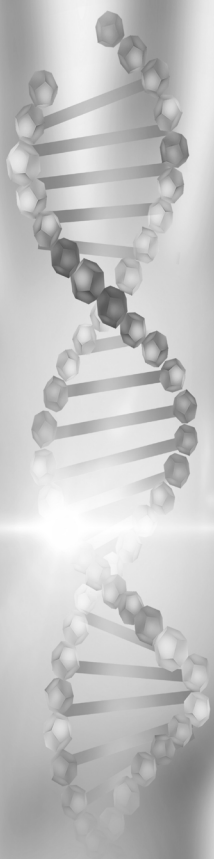
The Law on the Protection of Personal Data No. 6698 was published in the Official Gazette on 7 April 2016 and 29677 numbered entered into force. Turkish Data Protection Authority was established under the same Law in Ankara.

Turkish Data Protection Authority has been established as an independent regulatory authority having organisational and financial autonomy and having a public legal entity in order to fulfill the duties under the Law. 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 Grand National Assembly of Turkey, two members by the President of the Republic and two members by the Council of Ministers¹. The selection and appointment process of the Board members was completed at the end of 2016 and the Board started its duty on January 12, 2017 when the members took the oath in the Court of Cassation Board of First Presidency.

The mission of the Authority is to provide 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 stated in the Constitution, as well as to establish an environment to enhance the capability of competition of the public and private organizations in the world of data-driven economy. Our goal is to be influential in arising the public awareness related with personal data protection and to be a globally accepted authority in this area.

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



What is Personal Data?

Personal Data is any information relating to an identified or identifiable natural person. In this case, it can be said that basically two criteria are used to differentiate personal data from non-personal data. Accordingly, in order that any data is defined as personal data, the data must be related to a person and that person must be identified or identifiable.

PERSONAL
DATA

Who is Data Subject?

Data protection only applies to the data of the natural persons under the Law. Therefore, “data subject” is used in the Law to express natural person whose personal data is being processed. The person to be protected is “natural person” as stated in the definitions in the Regulation.

If personal data of a legal person identifies or makes identifiable a natural person, these data are protected under the Law as well. However, interest to be protected here belongs to the natural person, not legal person, since the Law does not cover the processing of personal data concerning legal persons.



DATA
SUBJECT



Who is Data Controller?

Data controller is the natural or legal person who determines the purposes for which and means by which personal data is processed and is responsible for establishing and managing the data registry system. Legal persons are themselves “controllers” while processing personal data, liabilities stated in the relevant regulations shall belong to the legal persons. There is no difference between public legal persons and private legal persons.

According to the law, controller is the person who determines the purposes for which and means by which personal data is processed. In other words, it is the person who shall answer the questions of “why” and “how” of the processing activities.

DATA
CONTROLLER

What is Processing of Personal Data ?

Processing of personal data is the series of operations that are carried out on personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or through non-automatic means only for the process which is a part of any data registry system set out in the Law.



PERSONAL
DATA

Key Principles in Processing of Personal Data

The procedures and principles for the processing of personal data in Article 4 of the Law are regulated in parallel 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. Key principles set out in the Law which state that data must be:

- Processed lawfully and fairly.
- Accurate and where necessary, kept up-to-date.
- Processed for specified, explicit and legitimate purposes.
- Relevant, limited and proportionate to the purposes for which they are processed.
- Retained for the period of time determined by the relevant legislation or the period deemed necessary for the purpose of the processing.

All personal data processing must be carried out in accordance with these principles.



Requirements for Personal Data Processing

a) Personal Data

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

As per Article 5 of the Law, processing of personal data shall only be exercised in case of the existence of following provisions.

Personal data can be processed in case;

- The data subject has given his explicit consent,
- It is explicitly provided for by the laws,
- It is mandatory for the protection of life or to prevent the physical injury of a person, in cases where that person cannot express consent or whose consent is legally invalid due to physical disability,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the conclusion or fulfilment of that contract.
- It is mandatory for the controller to fulfil its legal obligations.
- The data is made manifestly public by the data subject.
- Data processing is mandatory for the establishment, exercise or protection of any right.
- It is mandatory for the legitimate interests of the controller, provided that such processing shall not violate the fundamental rights and freedoms of the data subjects.

Principles regarding processing of personal data are limited under the Law and cannot be extended.



PERSONAL DATA

It is not necessary to obtain explicit consent, in case data processing is based on the conditions which are referred to in the Law other than explicit consent. Obtaining explicit consent when there are other statutory justifications to process the data is misleading and deemed as an abuse of rights by data controller. In case of the withdrawal of explicit consent by data subject, continuing processing by data controller which is based on the other legal bases is deemed as processing against the rules of the Law and honesty.

Therefore, it is necessary to evaluate whether the purpose of the processing 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 take explicit consent of the data subject for data processing.

Key Points on Explicit Consent

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

Explicit consent means giving consent for his personal data to be processed upon his own request or other party's request under the Law. The data subject shall actually express the decision on his legal value to the data controller with his explicit consent. Explicit consent shall enable the data subject to determine the limits, scope, manner and time of the data which he consented to process.

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 take explicit consent in writing. It is also possible to take explicit consent through electronic media and call centre etc. The burden of proof here is on the data controller.

Under the definition of explicit consent set out in the Article 3 of the Law, explicit consent has 3 following elements:

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

General explicit consents which are not restricted to a specified issue and the relevant transaction are accepted as "blanket consents" and are deemed legally invalid. For example; consent statements which does 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

Giving explicit consent is strictly binding right for the individual, data subject can withdraw his explicit consent. Since the data subject has the right to determine the future of his personal data, he can withdraw his consent at any time.

However, withdrawal of explicit consent will have a forward-looking results, all transactions carried out on the basis of explicit consent must be stopped by data controller as of he learns the withdrawal.

b) Sensitive Personal Data

Sensitive Personal Data, if obtained by others, can leave the data subject open to discrimination or unfair treatment. For this reason, sensitive personal data need to be protected more strictly than other personal data. Sensitive personal data can only be processed with the explicit consent of data subject 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, sect or other belief, clothing, membership of associations, foundations or trade-unions, information relating to health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be sensitive data. These are limited by Law, so it is not possible to extend them by comparison.

The law also makes a distinction between sensitive data. Accordingly, the processing without explicit consent of personal data relating to health and sexual life and other sensitive data has been regulated differently.

Under the law, sensitive data can be processed without explicit consent of the data subject in the following cases:

- Sensitive data excluding those relating to health and sexual life can be processed only in the conditions set out by the Law,
- Personal data relating to health and sexual life may only be processed, without explicit consent of the data subject, by persons under an obligation of confidentiality or by authorised institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Additionally, Law provides that for the processing of sensitive data adequate measures as determined by the Board must be taken.

Transferring of Personal Data

a) Transferring Personal Data inside Turkey

Article 8 of the Data Protection Law provides that personal data which is obtained within the framework of the general principles specified in the Law can only be transferred with the explicit consent of the data subject. The Law stipulates the same conditions for processing data and transferring data inside Turkey. Article 8 also defines the conditions for transferring data to the third parties without explicit consent.

On the other hand, since personal data is processed legally in Turkey does not mean that the data can be directly transferred to the third parties. Conditions set out Article 5 and 6 of the Law are also stipulated for transferring of data.

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

- The data subject has given his explicit consent,
- It is explicitly provided for by the laws,
- It is mandatory for the protection of life or to prevent the physical injury of a person, in cases where that person cannot express consent or whose consent is legally invalid due to physical disability,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the conclusion or fulfilment of that contract.
- It is mandatory for the controller to fulfil its legal obligations.
- The data is made manifestly public by the data subject.
- Data processing is mandatory for the establishment, exercise or protection of any right.

- It is mandatory for the legitimate interests of the controller, provided that such processing shall not violate the fundamental rights and freedoms of the data subjects.

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

- The data subject has given his explicit consent,
- Sensitive data excluding those relating to health and sexual life is explicitly provided for by the Laws,
- Personal data relating to health and sexual life, by persons under an obligation of confidentiality or by authorised institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing,

Personal data is only the information relating to 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 data controller or 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.



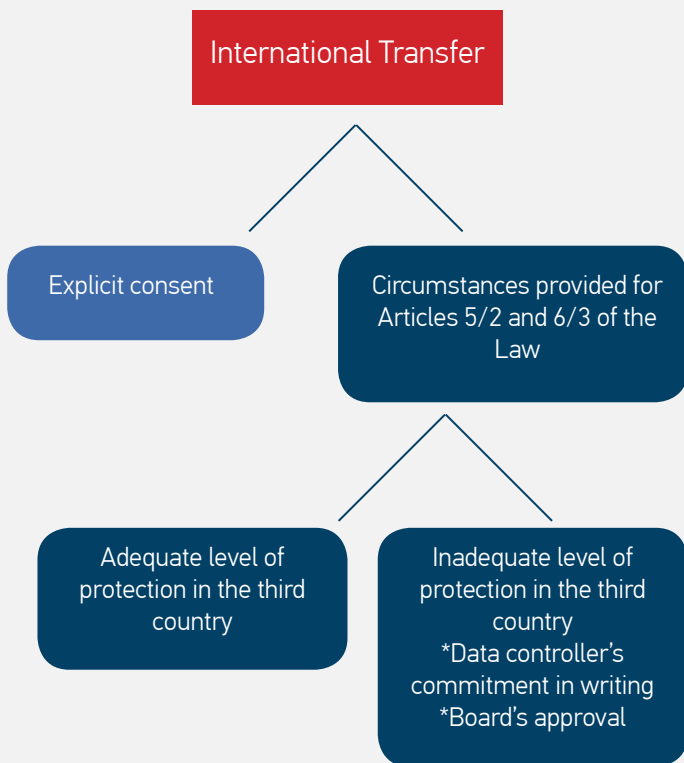
TRANSFER OF DATA

b) International Transfer of Personal Data

As required under Article 9 of the Law, a cross-border transfer may take place in one of the following cases that;

- The data subject has given his explicit consent,
- The country is approved by Board as “Adequate Country” and existence of the circumstances provided for in second paragraph of Article 5 and third paragraph of Article 6 of the Law,
- If the country is not approved by Board as “Adequate Country”, then data controllers in Turkey and abroad commit in writing to provide an adequate level of protection and the Board has authorized this transfer where existence of the circumstances referred to in second paragraph of Article 5 and third paragraph of Article 6 of the Law),

The Law has the same conditions/requirements for processing personal data and transferring personal data abroad.



* The list of approved countries shall be determined and announced by the Board.

Rights of Data Subject

Pursuant to Article 11 of the Law, by applying to the data controller data subject is entitled to:

- Learn whether or not personal data is being processed,
- Request further information about processing if personal data relating to him is being processed,
- Learn the purpose of processing of personal data and whether personal data is being used consistently with the purpose,
- Know the third parties in the country or abroad to whom personal data is transferred,
- Request rectification of personal data if processed incompletely or inaccurately,
- Request erasure or destruction of personal data,
- Request notification of the rectification, erasure or destruction to the third parties to whom personal data has been transferred,
- Object to the processing, exclusively by automatic means of his personal data, which leads to an unfavourable consequence for the data subject,
- Request compensation for the damage arising from the unlawful processing of his personal data.

Methods for Seeking Rights of Data Subject

a) Right to Apply

Data subject has the right to apply to the data controller to learn whether his personal data is processed or not, to request information if his personal data is processed, to request the rectification of the incomplete or inaccurate data, if any, to request the erasure or destruction of his personal data if it is unlawful, to request notification of the operations carried out in compliance with this to the third parties to whom his personal data has been transferred and to request compensation for the damage arising from the unlawful processing of his personal data.

Data subject shall submit his request relating to the enforcement of the Law to the data controller. The Law provides for a gradual application procedure for the requests relating to data personal data protection. Data subject cannot make a complaint to the Board before exhausting the application process to the data controller.

The right to compensation under the general provisions of those whose personal rights are violated is reserved in the Law.



There are two basic provisions relating to the means of applications which shall be made to the data controller in the Law. One of these means is written application. Written application is deemed as the application made with the document containing handwritten signature in accordance with the general provisions. In addition, the documents with the secure electronic signature shall meet the conditions of written form.

Personal Data Protection Board has been authorised to determine other means of application except written application in the Law. The Board has determined means of applications to be made to the data controller with secondary legislation.

a) Right to Complain

If the request (SAR) as per Article 13 of the Law is refused, the response of the controller is found unsatisfactory or the response is not given by the controller within 30 days, the data subject may file a complaint. Data subject shall not contact to the Board before exhausting all process.

The data subject may file a complaint with the Board within thirty days as of he learns about the response of the controller, or within sixty days as of the application date, in any case.

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 scope of work upon complaint or ex officio, where it learnt about the alleged violation. This examination shall comply with alleged violation upon

complaint or ex officio.

The notices and complaints not meeting the requirements laid down in Article 6 of the Law on the Use of Right to Petition shall not be examined. Except for the information and documents having the status of state secret, the controller shall be obliged to communicate with the Board within fifteen days the information and documents requested and shall enable, where necessary, on-the-spot examination.

The Board shall finalize the examination upon complaint and give an answer to data subjects. In case the Board fails to answer the data subject's application in sixty days as of the application date, it is deemed rejected. Accordingly, the period of filing a lawsuit in the administrative judiciary will begin with the passage of sixty days as of the date of the complaint.

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 all it may concern. This decision shall be implemented without delay and within thirty days after the notification at the latest. 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 related 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 recover 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 Data Controller

a) Obligation to Inform

The law gives data subject a right to be informed about by whom, for what purposes and for which legal reasons/basis their data are 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 when collecting personal data, the controller or the person authorised by him is obliged to inform the data subjects about the following:

- the identity of the controller and of his representative, if any,
- the purpose of data processing,
- the recipients to whom the data can be transferred, and the purpose of the transfer,
- the methods and legal reasons of collection of personal data,
- other rights referred to in Article 11.

The controller is obliged to inform to the data subject 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 subject should be informed in every situation where his personal data is processed.



b) Erasure, Destruction or Anonymisation of Personal Data

Despite being processed under the provisions of the Law, personal data shall be erased, destroyed or anonymised by the controller, ex officio or upon demand by the data subject, upon disappearance of reasons which require the process.

Obligations of the controller are to erase, destroy or anonymise personal data in cases where the reason of processing disappears. It is not necessary for the data subject to apply for this. However, in the event of negligence of the controller, data subject has the right to request that personal data shall be erased, destroyed or anonymised.

Controller, who prepared personal data storage and extermination policy, shall erase, destroy or anonymise personal data in the first periodic extermination process following the date on which the obligation to erase, destroy

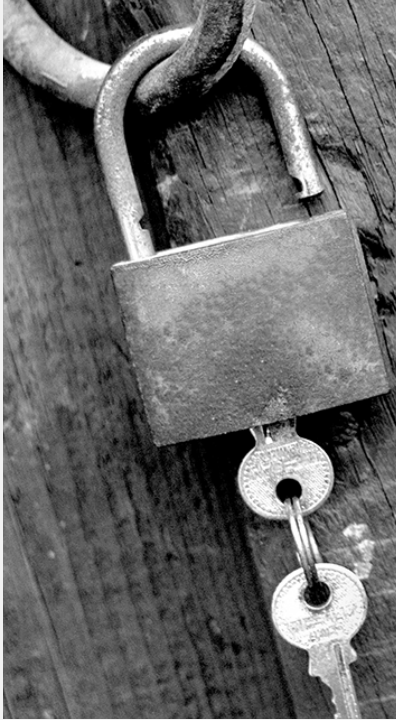
or anonymise personal data occurs within the framework of the Regulation on Erasure, Destruction or Anonymisation of Personal Data.

Erasure of personal data is the process of rendering personal data inaccessible and unusable for all relevant users. Controllers are liable for taking any technical and organisational measures to ensure that the erased personal data can be inaccessible and unusable for all relevant users.

Destruction of personal data is the process of rendering personal data inaccessible and unusable for any person. Controllers are liable for taking any technical and organisational measures required for destruction of personal data.

Anonymisation of personal data is defined as rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data. For personal data to be anonymised, personal data must be made irrelevant to identified or identifiable natural person in spite of the use of appropriate techniques in terms of the registry medium and the relevant field of activity such as retrieving and matching personal data with another data by controller, receiver or receiver groups. Controllers are liable for taking any technical and organisational measures for anonymisation of personal data.

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



c) Data Security Requirements

According to the Article 12 on data security of the Law, the controller is obliged to;

- prevent unlawful processing of personal data,
- prevent unlawful access to personal data,
- ensure the retention of personal data.

The controller shall take all necessary technical and organisational measures for providing an appropriate level of security in order to fulfil these obligations. The Board has power to take regulatory action in order to determine security requirements. Besides that, 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 of the processing of personal data by a natural or legal person on behalf of the 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), controller shall jointly be responsible with the accounting company for taking the measures laid down in the first paragraph regarding the processing of the data.

The controller shall also be obliged to be audited regarding to data security under the Law. The controller shall be obliged to conduct necessary audits or have them conducted in his own institution or organization, with the aim of implementing the provisions of this Law. The controller can conduct this audit by himself or through a third party.

The controllers and processors shall not disclose the personal data they obtained/collected to third parties and their purposes shall not be incompatible with the original purposes for collecting the data against the provisions of this Law. The controllers and processors shall remain responsible for this obligation even after the termination of their task.

In case the processed data are obtained unlawfully by other parties, the controller shall notify the data subject and the Board within undue delay. Where necessary, the Board may announce such breach at its official website or through other methods it deems appropriate.

The 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 provided for. The nature of the data controller's task and the personal data to be protected is also important as well as the size and turnover of the company.

In this context, a Personal Data Security Guide has been prepared by the Personal Data Protection Authority in order to clarify the technical and organisational 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

1) What's Data Controllers' Registry

Data Controllers' Registry (VERBIS) is a registration system where data controllers shall be registered to and record the data processing activities they are engaged with. Data controllers must register with the Registry which is held by the Authority under the supervision of the Board. Therefore, it is aimed to announce who data controllers are and to exercise the right of personal data protection more effectively.

The procedures and principles related to the Registry are determined in the Regulation on the Data Controllers' Registry.

2) Exemptions of Enrolling in the Registry of Data Controllers

All data controllers are obliged to register with the Data Controller's Registry System (VERBIS) before processing data.

However, Article 16 regarding the obligations of registering with the VERBIS shall not be applied in the cases set forth in the second paragraph of Article 28.

The Board has also the authorization to bring an exemption to the obligation to register according to the Law. In the implementation of the exemption, objective criteria determined by the Board such as the nature and the number of the processed personal data, legal requirements for data processing, or data transfer to the third parties shall be considered.

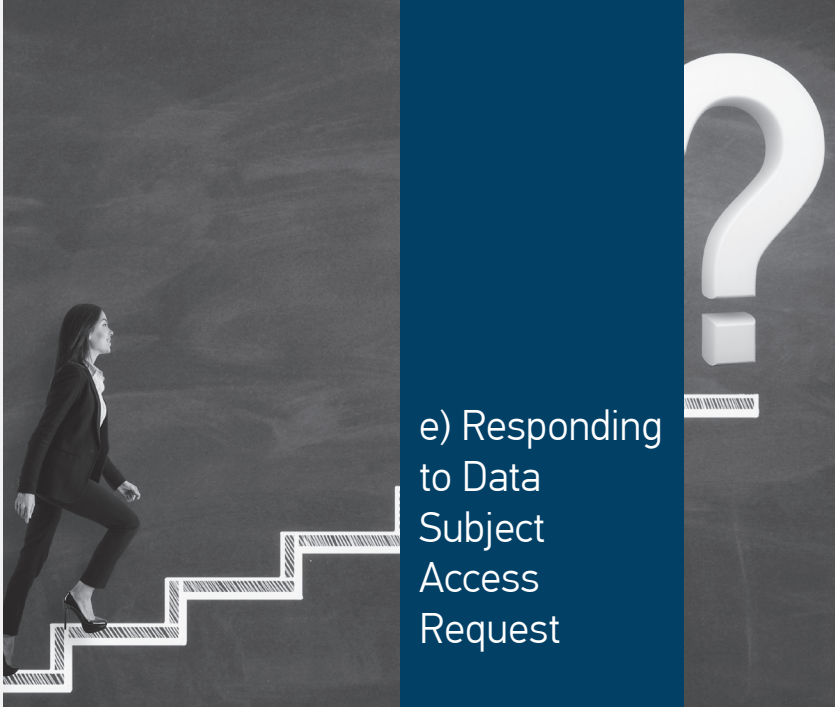
Obligation to register with VERBIS has the aim of the establishment of a safer and transparent environment in terms of clarification of personal data processing and to act in compliance with the legislation for controllers.

3) Data Controllers' Registry Requirements

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

- Identifying information (including the address of the data controller or its representative).
- The purpose of the data processing.
- The data subject groups and data categories (data processing inventory).
- Recipient or recipient groups to which the data may be transferred.
- Any personal data which may be transferred abroad.
- The data security measures taken.
- The maximum time for processing personal data (which must be in accordance with the purpose of the data processing).

In case of any change in the information listed above, such change shall be notified to the Authority. Thus, it is aimed to keep the record up to date.




e) Responding to Data Subject Access Request

The data controller is obliged to respond to the request (SAR) which is made by the data subject in writing and by other means determined by the Board within the thirty days of the receipt at the latest and free of charge. However, data controller may charge a fee set by the Board from the requestor if the request necessitates responding fee.

The fee set by the Board is included in the Communiqué on Procedures and Principles of the Application to Data Controllers. The data controller shall accept the request or refuse it with justified grounds and inform to data subject in written or electronically (registered e-mail address, a secure electronic signature, a mobile signature or an e-mail). If the request is accepted, data controller shall fulfil the data subject's request. If a fee was charged, such fee must be repaid to the data subject when the request is made due to the fault of the data controller.

Rejection of the application, insufficiency of the answer or the failure to respond to the application within an appropriate time period; the data subject becomes entitled to file a complaint to the Board within 30 days following the date the data subject become aware of the data controller's response and 60 days of receipt at most.

A grayscale photograph showing a person's hands writing on a notepad with a pen. The person is wearing dark trousers. The background is blurred, suggesting an office or meeting environment.

f) Requirements of Decision Notice to be Fulfilled

If the Board determines the existence of a data breach upon the complaint or ex officio, Board shall notify the decision notice to all concerned including that the data breach shall be settled by the relevant controller. The data controller shall fulfil decision notice without undue delay and within thirty days of receipt.

The Guidelines which we have published so far are as follows:

- Law on the Protection of Personal Data in 100 Questions
- Implementation Guideline on the Law on the Protection of Personal Data
- Personal Data Security Guidelines (Technical and Organisational Measures)
- Guideline on Erasure, Destruction or Anonymisation of Personal Data
- Frequently Asked Questions About the Law on the Protection of Personal Data
- Right to Request Protection of Personal Data as a Constitutional Right
- Data Controller and Data Processor
- Data Controller's Registry
- Methods for Seeking Rights of Data Subject
- Rights and Obligations Under the Law
- Processing Conditions of Personal Data
- Key Principles Regarding to Processing of Personal Data
- Explicit Consent
- Basic Concepts in the Law No. 6698
- Terms in the Law No. 6698
- The Purpose and Scope of the Law No. 6698 on the Protection of Personal Data
- International and National Regulations for the Protection of Personal Data
- The Need for the Law on the Protection of Personal Data
- Processing Conditions of Sensitive Personal Data
- International Transfer of Personal Data
- Structure and Duties of Personal Data Protection Board





Nasuh Akar Mah. 1407. Sokak No:6 06520
Balgat-Çankaya/Ankara
Tel: 0 (312) 216 50 50 // www.kvkk.gov.tr