PROTECTION OF PERSONAL DATA — HANDBOOK

1. How is our personal data protected in Turkey? What amendments have been made?

In 2010, the constitutional guarantee of personal data was bound. According to the Constitution: 'Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with foreseen objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be enacted in law.'

'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' was signed by the Council of Europe on 28 January 1981 and signed by Turkey in order to protect personal data in all member countries under the same standards and to establish cross-border data flow policies. The Convention was published in the Official Gazette dated March 17, 2016 and numbered 29656 and was included in domestic law. According to Article 4 of the Convention No. 108, it is compulsory to make

legal arrangements for the protection of personal data in domestic law. In this context, Law No. 6698 on Protection of Personal Data (Law) dated March 24, 2016 was issued and entered into force on 7 April 2016.

2. What is the purpose and scope of the Law on Protection of Personal Data?

The purpose of the Law is to regulate the procedures and principles in which personal rights and freedoms, including the confidentiality of private life, protection of personal data, and the obligations of natural person and legal entities that process personal data.

Natural person and legal entities whose personal data are processed and those that are totally or partially automatic, or in a non-automatic way, are part of any data recording system, are included in the scope of the Law. At the same time the Law will be applied to the data controllers, who operates in Turkey but a resident abroad.

3. What is personal data?

Personal data is defined as; any information relating to an identified or identifiable natural person.[1] To be able to talk about personal data, it has to be related to a natural person[2], and this person has to be specific or identifiable. Such names shall be considered as personal data if the names and nicknames are alone or in combination with other sources to enable the identification of the person.

4. What are the Special Categories of Personal Data?

Special categories of personal data are the ones bearing the risk of causing discrimination against the owners in case they are processed. For this reason, they need to be protected much more strictly than other personal data. Special categories of personal data includes data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics.

According to the Law, it is prohibited to process special categories of personal data without obtaining the explicit consent of the data subject.

5. What is the personal health data and in which cases can it be processed?

Personal health data refers to any kind of health data relating to the identity of the individual or of the identifiable natural person. For example; all kinds of assays, the diseases the person has, the drugs they use, and so on. Personal health data is considered as a private

[1] Any information is extremely broad, however it can be defined as a natural person's name, surname, date of birth and place of birth; phone number, motor vehicle license plate, social security number, passport number, resume, picture, image and sound recordings, fingerprints, IP address, e-mail address, mobile phone, preferences, interacted persons, group memberships, family information, health information.

[2] Those which are counted as legal entities' data, are considered outside of the definition of the personal data.

personal data. Therefore, it is subject to the conditions for processing of special categories of personal data.

Individuals engaged in personal health data processing activities may only process personal health data in the presence of one of the following conditions:

- If at least one of the following personal health services is provided by persons under the confidentiality obligation or by authorities, it may be processed without the explicit consent of the personal data owner: public health protection, preventive medicine, medical diagnosis, treatment and care services, financing planning and management.
- In the case that the person concerned is informed in detail, the written consent is received, and the relevant consent is maintained, the health data of the person concerned can be processed and transmitted in consent.

6. What is explicit consent and what are the provisions?

According to the Law, there are three elements of explicit consent:

- Being related to a specific topic
- Based on enlightenment
- Being explained with free will

No form conditions are required for explicit consent, but when explicit consent is written, consent texts must be made clear and simple. At the same time explicit consent can be withdrawn.

Personal data may be processed without obtaining the explicit consent of the data subject if one of the below conditions exists:

- It is expressly permitted by any law;
- It is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent;
- It is necessary to process the personal data of parties of a contract, provided that the processing is directly related to the execution or performance of the contract;
- It is necessary for compliance with a legal obligation which the controller is subject to;
- The relevant information is revealed to the public by the data subject herself/himself;
- It is necessary for the institution, usage, or protection of a right;
- It is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

Personal data that is processed before the date of publication of the Law shall be rendered compliant within two years following the date of publication of this Law. Personal data that is determined to be contrary to the provisions of the Law shall be immediately deleted, destroyed, or anonymised. However, the consents that are lawfully obtained before the date of publication of the Law shall be deemed lawful in terms of the Law , provided that no declaration of intention to the contrary is made within one year.

7. Who is data controller?

Data controller is a natural or legal entity who determines the purposes and means of the processing of personal data, and who is responsible for establishment and management of the filing system. These persons can be natural person or legal entities such as public institutions, companies, associations or foundations. In this context, the data controller is the entity itself; the obligations arising out of this Law shall be fulfilled by the authorized bodies or persons representing and binding the legal entity.

8. Who is data processor?

Data processor is a natural or legal entity who processes personal data based on the authority granted by and on behalf of the data controller. These persons may also be a separate natural or legal entity for whom the data authority authorises to process personal data.

The Data Controller is jointly responsible with these persons for taking such measures in the case that the personal data is processed by another natural or legal person on his behalf.

9. What are the general principles of processing personal data?

- Being in conformity with the law and good faith;
- Being accurate and if necessary, up to date;
- Being processed for specified, explicit, and legitimate purposes;
- Being relevant, limited and proportionate to the purposes for which data are processed;
- Being stored only for the time designated by relevant legislation or necessitated by the purpose for which data are collected: Personal data must only be retained for the period required for the purposes for which they are prescribed in the applicable legislation or for the purposes for which they are handled. According to this, the data controllers shall comply with this period if there is a period foreseen to keep the data in the relevant legislation; otherwise, the data may be retained only for the time required for the purpose for which it is being processed. If there is no valid reason for further storage of a data, the data will be deleted or made anonymous. Data will not be stored due to the possibility of future use. When filing for register entry, the data controller must report the maximum time required for the purpose for which personal data is processed.

Principles for the processing of personal data must be at the core of all personal data processing activities and all personal data processing activities must be performed in accordance with these principles.

10. What are the conditions for processing of personal data?

In Article 5 of the Law, data processing conditions are established. In this respect, it is possible to process personal data, but only if

there is a explicit consent of the data owner or the presence of one of the conditions on the sixth question.

11. What are the full and partial exceptions in the law? In which cases will the law not be enforced or be applied in a limited manner?

Provisions of this Law shall not be applied in the following cases:

- Processing of personal data by natural persons in the course of a purely personal or household activity, provided that obligations relating to data security are complied with and data are not transferred to third parties.
- Processing of personal data for the purposes of official statistics and, through anonymization, research, planning, statistics and similar.
- Processing of personal data for the purposes of art, history, and literature or science, or within the scope of freedom of expression, provided that national defence, national security, public safety, public order, economic safety, privacy of personal life or personal rights are not violated.
- Processing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organisations who are assigned and authorized for providing national defence, national security, public safety, public order or economic safety.
- Processing of personal data by judicial authorities and execution agencies with regard to investigation, prosecution, adjudication or execution procedures.

On the condition of being relevant and proportionate to the purpose and general principles of this Law, article 10 which regulates the obligation of the data controller to inform; except for right to request compensation, article 11 which regulates the rights of the data subject; and article 16 which regulates the obligation to register with the Data Controllers' Registry shall not apply in the following cases:

- Processing of personal data is necessary for prevention of crime or investigation of a crime.
- Processing of personal data revealed to the public by the data subject herself/himself.
- Processing of personal data is necessary, deriving from the performance of supervision or regulatory duties, or disciplinary investigation or prosecution by assigned and authorized public institutions and organisations and professional organisations with public institution status.
- Processing of personal data is necessary for the protection of economic and financial interests of the state related to budget, tax, and financial matters.

12. What are the rights of the data subject?

- Learn whether or not her/his personal data have been processed;
- Request information as to processing if her/his data have been processed;

- Learn the purpose of processing of the personal data and whether data are used in accordance with their purpose;
- Know the third parties in the country or abroad to whom personal data have been transferred;
- Request rectification in case personal data are processed incompletely or inaccurately;
- Request deletion or destruction of personal data;
- Request notification of the operations made as per indents (d) and (e) to third parties to whom personal data have been transferred;
- Object to occurrence of any result that is to her/his detriment by means of analysis of personal data exclusively through automated systems;
- Request compensation for the damages in case the person incurs damages due to unlawful processing of personal data by applying to the data controller.[3]

Data claims by data owners should be free of charge. However, if the transaction also requires a cost, it may be charged according to the tariff to be determined by the Personal Data Protection Board (Board).

In cases where the data owner's application is dismissed with respect to his rights or the answer is found to be inadequate, within thirty days from the date of the receipt of the response and presumably within sixty days from the date of the application, the data owner can make a complaint to the Board.

13. What does it mean to delete, destroy and anonymise personal data? Under what conditions should personal data be deleted, destroyed or anonymised?

Deletion of personal data; is the process by which the personal data is inaccessible and irrevocable by the respective users. The data controller assumes all necessary technical and administrative measures to ensure that deleted personal data can not be accessed and reused by the relevant users.

Destruction means that all physical recording media suitable for storing data stored in the information can not be retrieved and used again. Data controllers shall take all necessary technical and administrative measures concerning the destruction of personal data.

Anonymisation of personal data is the making of personal data unlikely to be associated with an identifiable or identifiable real person even when matched with other data. In this context, it is not possible to assume that the data is anonymised if it is possible to know who the data belongs to after the data is traced and the other data is matched and supported. Anonymised data will no longer be subject to the provisions of the Law as it will no longer have personal data attributes.

After the processing of the personal data has been completed, the data is deleted, destroyed

[3] Data owners who have been breached have the right to compensation according to general provisions.

or made anonymous on the request of the person or the person concerned (the data owner). The procedures and principles regarding the deletion, destruction and anonymization of personal data shall be determined by the Board in accordance with Article 7 of the Law.

14. What are the terms and conditions of domestic and foreign transfers of personal data?

Personal data shall not be transferred abroad without obtaining the explicit consent of the data subject.

Personal data may be transferred abroad without obtaining the explicit consent of the data subject if one of the conditions set forth in the second paragraph of article 5 or third paragraph of article 6[4] is present and,

- If the foreign country to whom personal data will be transferred has an adequate level of protection,
- In case there is not an adequate level of protection[5], if the data controllers in Turkey and abroad commit, in writing, to provide an adequate level of protection and the permission of the Board exists.

15. What is the scope of the data controllers liability to inform and how will it be fulfilled?

Data controller or the person it authorized is obligated to inform the data subjects while collecting the personal data with regard to:

- The identity of the data controller and if any, its representative,
- The purposes for which personal data will be processed,
- The persons to whom processed personal data might be transferred and the purposes for the same,
- The method and legal cause of collection of personal data,
- The rights set forth under article 11.

There is no form requirement for fulfilment of the disclosure obligation and it is not subject to the approval of the interested person (data holder). The obligation to disclosure can be fulfilled by a unilateral declaration.

16. What are the responsibilities of data controllers to ensure data security?

Data controller shall take all necessary technical and organisational measures for

[4] Conditions permitting the processing of personalised personal data without the relevant person's explicit consent

[5] Whether or not there is adequate protection in foreign countries shall be determined and announced by the Board. The Board shall decide whether there is adequate level of protection in a foreign country and whether approval will be granted in terms of indent by evaluating:

- The international agreements to which Turkey is a party,
- Reciprocality regarding transfer of personal data between the country requesting personal data and Turkey,
- With regard to each present transfer of personal data, nature of personal data and purpose of processing and retention,
- Relevant legislation and practice of the country to whom personal data will be transferred,
- Measures committed by the data controller in the country to whom personal data will be transferred
- If it requires, by obtaining the opinion of relevant public institutions and organisations.

providing an appropriate level of security in order to;

- Prevent unlawful processing of personal data,
- Prevent unlawful access to personal data,
- Safeguard personal data.

In addition to that;

- The data controller is obligated to carry out or have carried out necessary inspections within his institution and organisation in order to ensure implementation of the provisions of the Law.
- Data controller and persons who process data shall not disclose and misuse personal data they learned contrary to the provisions of the Law. This obligation shall continue after resigning from office.
- In case processed personal data are acquired by others through unlawful means, the data controller shall notify the data subject and the Board of such situation as soon as possible. The Board, if necessary, may declare such situation on its website or by other means which it deems appropriate.

17. What are the procedures and principles of application to data controller?

The data controller shall conclude the requests included in the application free of charge and as soon as possible considering the nature of the request and within 30 days at the latest. However, in case the operation necessitates a separate cost, the fee in the tariff designated by the Board may be collected. The data controller shall accept the request or reject it by explaining the reason and notify the data subject of its reply in writing or electronically. In case the request included in the application is accepted, it shall be fulfilled by the data controller accordingly. In case the request is resulted from the fault of the data controller, the collected fee shall be returned to the data subject.

18. What is the Data Controllers' Registry, is it mandatory to register? How to register at the registry?

Under the supervision of the Board, Data Controllers' Registry shall be kept by the Presidency in a publicly available manner.

Natural or legal persons who process personal data shall register with the Data Controllers' Registry prior to commencing processing. However, considering objective criteria that shall be designated by the Board such as the characteristics and the number of data to be processed, whether or not data processing is based on any law, or whether data will be transferred to third parties, the Board may set forth exemptions to the obligation to register with the Data Controllers' Registry.

The fact that the enforcement date of the Regulation on Data Controllers' Registry has been determined as 01.01.2018 does not mean that the obligation to register in the Registry has started. Accordingly, the obligation to register will commence after the Board declares the exceptional decision, the Data

Accounts Register Information System (VERBIS) is opened to the service, and the Board sets a starting date for registration in the Registry and is shared with the public.

If the data controller is a legal entity resident in Turkey, it has to designate a contact person and contact information of the person who has to save the Registry to assign records during a VERBIS. The contact person is responsible for ensuring communication between the data controller and the person concerned or the Personal Data Protection Authority. Responsibility in terms of liabilities and sanctions under the Law is not on the contact person but on the body representing the legal entity. Assignment made as a contact person does not remove the responsibility of the data controller in accordance with the provisions of the Law.

Registry application to the Data Controllers' Registry shall be made with a notification including the following matters:

- Identity and address information of the data controller and of the representative thereof, if any,
- The purposes for which personal data will be processed,
- The group or groups of persons subject to the data and explanations regarding data categories belonging to these persons,
- Recipient or groups of recipients to whom personal data may be transferred,
- Personal data which is envisaged to be transferred abroad,
- Measures taken for the security of personal data,
- The maximum period of time necessitated by the purposes for which personal data are processed.

19. How will the orientation process of the Personal Data Protection Law be?

Personal data processed before the date of publication of the Law shall be made compatible with the provisions of the Law within two years from the date of publication, in other words until April 7, 2018 the preparations should be completed.

Any personal data found to be inconsistent with the provisions of the law shall be immediately deleted, destroyed or made anonymous. However, the requests received in accordance with the law before the date of publication of the Law, which is 7 April 2016, shall be deemed to comply with the Law if a declaration of will is not made within a year.

In this context, the following actions must be taken by employers:

- Preparing personal data processing inventory[6]
- Identification of cases requiring explicit consent and preparation of consent texts, required legal information texts for this purpose and preparation of all contract

[6] Personal data processing inventory refers to personal data processing activities that data controllers are performing based on business processes; data category and quality, data processing purposes, data retention locations and durations associated with the recipient group and detailing the data.

texts which result in the transfer of personal data

- Data collection, storage, replacement, etc. creation of data processing policies and processes for processing activities
- Issues such as information security and the company's risk management structure, security policies, information security organisation, human resources security, information asset management, access control security, physical and environmental security, information technology operations and communication security should be addressed.
- In addition, in the framework of the principles stated above, the data that is not needed should be destroyed, the assigned personnel should be educated, and continuous audits should be performed to check that the workplace organisation is operating in compliance with the relevant legislation.

For more information please contact with:
info@gurpinarlaw.com

LAW NO OR REGULATION NAME	OFFICIAL GAZETTE - ENFORCEMENT DATE
Law No. 6698 on the **Protection of Personal Data** (Articles 1,2,3,4,5,6,7,10,12,19 and after)	07.04.2016 - 07.04.2016
Law No. 6698 on **Protection of Personal Data** (Articles 8,9,11,13,14,15,16,17,18)	07.04.2016 – 07.10.2016
Regulation on Deletion, Destruction or Anonymization of Personal Data	28.10.2017 – 01.01.2018
Regulation on the Data Controllers' Registry	30.12.2017 - 01.01.2018
Communiqué on Procedures and Principles for Application to Data Officers **Communiqué Pertaining to the Procedures and Principles to be Obeyed in the Fulfilment of the Lighting Obligations**	10.03.2018 - 10.03.2018

CRIMES	IMPRISONMENT
(Article 135 of the Turkish Criminal Code) **Recording personal data contrary to law**	1-3 YEARS
(Article 136 of the TCC) **Unlawful delivery or acquisition of data**	2-4 YEARS
(Article 138 of the TCC) **In case of failure to destroy the data within a defined system despite expiry of legally prescribed period**	1-2 YEARS
(Article 17 of the Law on Protection of Personal Data) **To do not delete personal data or make it un-anonymous**	1-2 YEARS

MISDEMEANOURS	ADMINISTRATIVE FINE (MIN-MAX)
Violation of disclosure obligation	5.000 TL - 100.000 TL
Violation of data security obligation	15.000 TL - 1.000.000 TL
Failure to comply with decisions made by the Board	25.000 TL - 1.000.000 TL
Failure to comply with the requirement to register in the Data Controllers' Registry	20.000 TL - 1.000.000 TL