GURULKAN ÇAKIR

PROTECTION OF PERSONAL DATA IN TURKEY

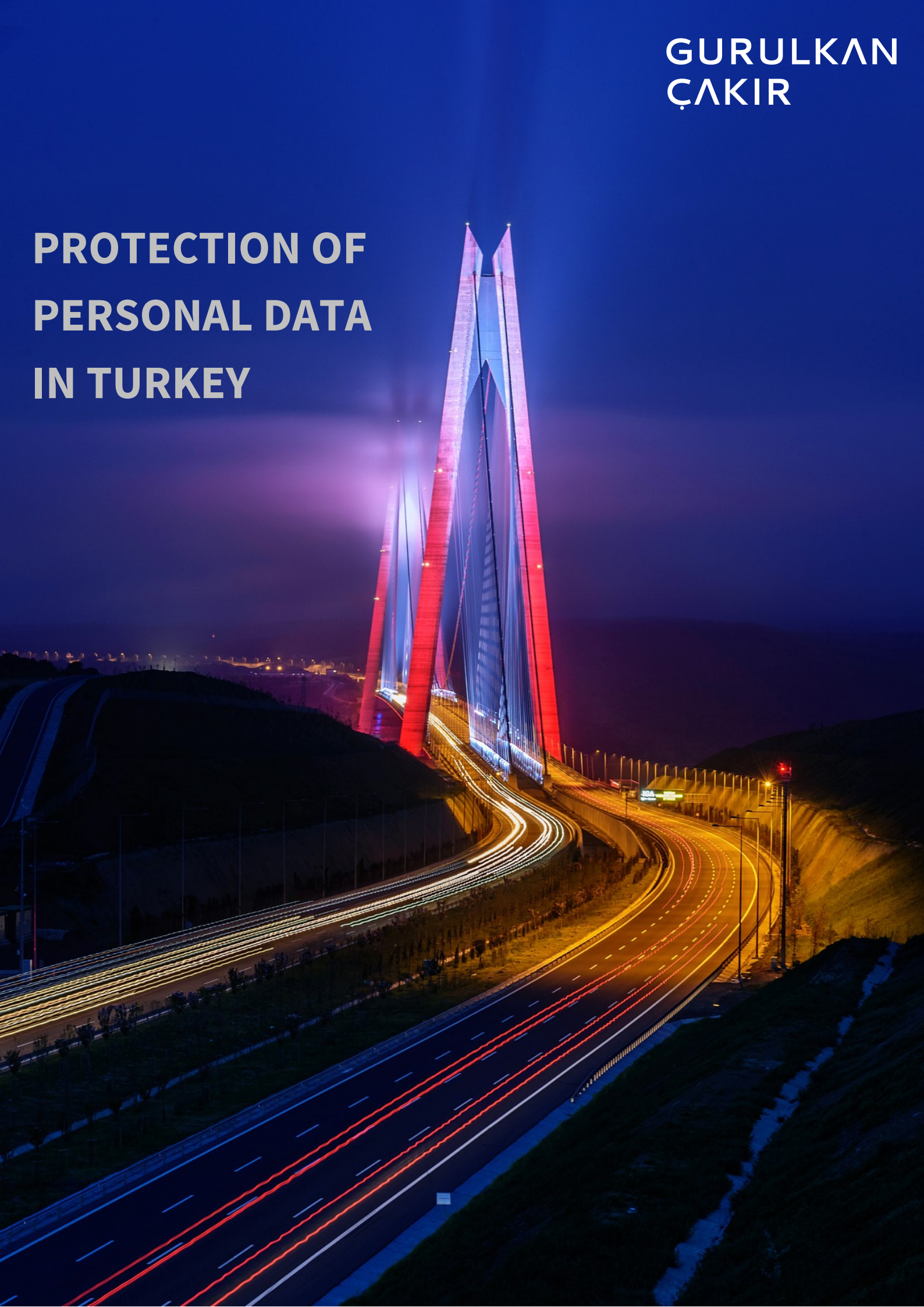

TABLE OF CONTENTS

PROTECTION OF PERSONAL DATA IN TURKEY

Introduction

With the enactment of the Law no. 6698 ("**Code**") in April, 2016, "The right to the protection of personal data", which has been set out in the Constitution of Turkey with the constitutional amendments in 2010[1], has finally become a statutory right in Turkey. The Code, which was modelled on the Directive 95/46/EC of the European Union ("EU"), lays out the framework for rules, principles, limits and criteria of processing of personal data.

All natural or legal persons who process personal data, or "data controllers", now have many responsibilities towards "data subjects" and are accountable to the new Turkish Data Protection Agency ("**Agency**") which has been established by Art. 19 of the Code. As is the practice in Europe, in order to ensure the compliance, data controllers will have to register with The Agency, which has the authority to hold audits, give administrative fines to data controllers and issue regulations and decisions on data protection matters.

I. Personal Data

Definitions are found in the Art. 3 of the Code. According to this article, **personal data** is: "*any information relating to an identified or identifiable natural person*".

Examples of personal data:

- ID Number
- Phone Number
- E-mail address
- Pictures
- IP address or Cookie information on a web browser

[1] Turkish Constitution Art. 20/3: "*Everyone has the right to request the protection of his or her personal data...*"

- Information on the physical traits of a person
- Information relating to the financial status and credibility
- CV information
- Information on union or party memberships

Processing of personal data is:

Any set of operations which is performed upon personal data, whether or not by automatic means, such as

- *collection,*
- *recording,*
- *retention,*
- *storage,*
- *alteration,*
- *reformation,*
- *disclosure,*
- *transfer,*
- *acquisition,*
- *categorization,*
- *usage, or*
- *blocking*

of personal data.

Information relating to legal persons is not personal data and therefore is not in the scope of this Code and is not protected in the context of personal data.

For information to be classified as personal, it does not need to relate to an identified person. If the information in question can be combined with additional information and become related to an identified person, it is considered personal information by virtue of this article. In other words, if an individual is described in a way which makes it possible to find out who the data subject is by conducting further research, the information in question is personal data.[2]

II. Sensitive Personal Data

Special categories of personal data (or sensitive personal data) are provided in the Art.6 of the Code.

[2] Turkish Constitutional Court rendered a decision on a controversial subject and ruled that an IP address is indeed a personal data: file n. 2014/149, decision no. 2014/151. Also, CJEU has ruled that dynamic IP addresses can be personal data under certain circumstances: Patrick Brayer vs. Germany, 2016.

Information relating to

- *health,*
- *sex life,*
- *union memberships,*
- *political opinions,*
- *racial or ethnic origin*

are deemed sensitive personal data, and have heavier conditions for processing.

III. Data Controller and Data Processor

Data controller is:

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

While public institutions and private companies can be data controllers as legal persons, individuals such as general practitioners, pharmacists, politicians and sole traders etc. are some examples of data controllers as natural persons, where these individuals keep personal information about their patients, clients, constituents etc.

Data processor is:

➔ Any natural or legal person body which processes personal data on behalf of the controller.

In that sense, data processors process data only within the limits and for the purposes determined by the data controller, most commonly as a service. Third party payroll companies, marketing and research companies or cloud companies are some examples of data processors.

Data processors do not hold control over the personal data; therefore are not responsible for the lawfulness of data processing as long as they are only acting as instructed by the data controller. Where a data processor surpasses the limits of processing activity drawn by the data controller, he becomes responsible in the same degree as a data controller within the scope of the Code.

It is important to determine whether a company is a data controller or a data processor. The Code focuses on the data controller to ensure compliance. Almost all obligations and responsibilities belong to the data controller; whereas data processor is only jointly responsible with the data controller for taking security measures. Because legal responsibilities provided by the Code mostly falls onto the controllers, it is crucial for controllers to well define the sharing of responsibilities regarding data protection issues in their contracts with data processors.

The legal status of a natural or legal person can be both data controller and data processor at the same time, depending on its data processing activities. In that regard, it is also important for a person to categorize and keep track of its processing activities.

IV. Principals Relating to Data Quality

According to the Art. 4 of the Code, personal data can be processed only in compliance with the principals relating to data quality. These principals are as follows:

- Lawfulness and fairness,
- Accuracy and up-to-dateness,
- To process data for specified, explicit and legitimate purposes,
- The processing to be relevant and not excessive in relation to the purposes of the processing,
- Not to retain data for longer than necessary for the purposes for which they are collected.

1. Lawful and Fair

For the processing to be lawful, it must have one of the legal grounds stated in the Art. 5 of the Code. However, having a legal ground for processing personal data does not automatically make it fair as well. If the processing of personal data is having negative effects on the data subject which cannot be foreseen by the data subject, it might be unfair. Also, fairness requires the data controller to be as transparent, clear and open about the processing as possible. Especially in contractual relationships, for the data subject to be able to make more informed decisions and better assess the terms of the contract,

transparency and clarity on the processing activities is necessary for it to be deemed fair.

2. Accurate and Up-to-date

Inaccurate or out-of-date information may have adverse effects on data subjects. For example, if the address of a customer of a seller is out-of-date, a delivery may never find the customer. Or, if there is misleading or erroneous information in the database of a bank on the credibility of its clients, this may adversely affect the financial conditions of the client. For that reason, it is provided by the Code that personal data must be kept accurate and up-to-date.

3. Specified, Explicit and Legitimate Purposes

Data controllers must specify the purposes of processing so as to keep them compatible with the purposes for which they collect the data. This is important for the transparency of data controllers towards data subjects as well. Data subjects need to be well informed about the purposes of the processing, so that they are able to well exercise their rights on the protection of their personal data.

Also, the purposes of processing can often change during the processing activity due to unexpected reasons or due to the nature of the processing activity. This may lead to an incompatibility between the collection and the processing of personal data. In these cases, data controllers must seek new legal grounds for the new purposes for the processing of personal data, and keep data subjects informed about the new processing activities.

4. Relevant and Not Excessive

The purposes of processing of personal data derives from its legal grounds, which are stated in the Art. 5. Although the collection of data may be lawful and in accordance with the Art. 5, if the further processing of data is excessive in relation to the purposes of the collection of the data, it contradicts with this principal. For that reason, processing must not exceed what is necessary to achieve its purposes. For example, for the identification of persons who enter into a workplace, whereas an ID card control is sufficient, fingerprint

control would be excessive as it involves processing of sensitive personal information; therefore illegal in terms of the Code.

5. Retention

Processing of personal data is legal only as long as it serves the purpose for which they are collected; and therefore, it must be kept no longer than necessary for the those purposes, as retention is also considered a processing activity. In practice, companies do not always keep track of which data they collect and retain; which can cause legal problems in terms of data protection principals. Data controllers should keep track of the personal data they process, and the best way to do that is to have data retention policies, which also shows effort for compliance before data protection agencies.

V. Grounds for Processing of Personal Data

According to the Code, personal data cannot be processed unless one of the requirements from the Art. 5 is met. These requirements are as follows:

- Processing is required by the law,
- It is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent,
- It is necessary for the contractual relationship between the data controller and the data subject,
- It is necessary for the data controller to perform his legal obligations,
- The data to be processed is expressly made public by the data subject,
- It is obligatory for the establishment, exercise or defence of a legal claim,
- It is necessary for the legitimate interest of the data controller, provided that it does not infringe fundamental rights of the data subject,
- Explicit consent given by the data subject.

1. Requirement by the Law

In certain cases, processing of personal data may be required by the law. For employers, keeping employee's personnel files in accordance with the Art. 75 of the Labour Code and for banks, keeping the documents of the clients for 10 years as required by the Art. 42 of the Banking Code are some of the examples of this situation. In these cases, data controllers undertake the responsibility of compliance with the data protection rules as a requirement by the law.

2. Vital Interests

In some cases, data processing may be necessary where the data subject may not be in a capacity to give his or her consent. This may especially be the case where the health, or even the life of the data subject or another person is at stake. Where the data subject is incapable of giving his consent and yet data processing is imperative for the vital interests of the data subject or another person, consent is not required.

3. Performance of a Contract

Contractual relationships in many cases require processing of personal data. This typically is the case in contracts between companies and their clients. Personal information such as contact information, ID information, address or certain preferences of clients or users may be indispensable for the performance of a contract. In such cases, data controller needs no other legal basis for the processing of personal data than the contract itself. However, the personal data which can be processed on this legal basis is limited to the amount which is indispensable for the performance of the contract. If the data controller wishes to further process the data in question for other purposes, consent may be required.

4. Publicization by the Data Subject

Where a person makes his personal information publicly available, it can be processed without his consent or any other legal basis mentioned in the Article 5/2, as is the case for sharing information about oneself on social media. However, it is accepted that the

processing activity must be in compliance with the purpose of publicization by the data controller. For example, expressing hobbies and interests on the social media does not make it legal to use such information for marketing purposes.

5. Necessity for a Legal Claim

Processing of personal data may be necessary for the establishment, exercise or the defence of a legal claim of the data controller. Such is the case with merger & acquisition processes where clientele and employee information needs to be shared in bulk with another company. Such processing would otherwise require the consent of data subjects; however, that would unreasonably inconvenience these processes. Therefore, depending on the situation, necessity for the processing of personal information for abovementioned reasons can be a legal basis by itself.

6. Legitimate Interests

The legitimate interests of the data controller alone can also justify the processing of personal data, without the consent of the data subject of any other legal basis abovementioned. The purpose of this provision is to prevent the over-reliance on strict legal grounds which could have unintended results in this field. However, it should not be automatically chosen, or its use unduly extended on the basis of a perception that it is less constraining than the other grounds. Overuse of this legal basis can be ultimately interpreted as unfair and constraining for the rights of the data subjects.

Also, in order to rely on legitimate interest grounds, the data controller has to implement a balancing test between his own interests and those of the data subject in order to ensure, by assessing the risks of processing, that the fundamental rights of the data subject are not infringed and by taking into account different factors, that the processing is actually necessary for the legitimate interest, as this implies processing to the detriment of the data subject.

7. Explicit Consent

According to the Art. 5/1 of the Code, personal data can be processed if the data subject has given his explicit consent. The definition of "explicit consent" is given in the definitions in the Art. 3/1-a.

Explicit consent is:

- Informed,
- relating to a specific matter, and
- freely given

consent of the data subject.

VI. Grounds for the Processing of Sensitive Data

Provided in the Art. 6 of the Code as special categories of personal data, grounds for the processing of sensitive data are much more limited compared to the processing of personal data. This is because unlawful processing of sensitive data has a much bigger potential of having negative effects on the public order and on the data subject such as social discrimination or identity theft.

Sensitive personal data (other than those relating to health and sex life) can only be processed if there are provisions in other laws which allow the processing of sensitive data. The only other legal ground is the explicit consent of the data subject.

Sensitive data relating to health and sex life can be processed only with the explicit consent of the data subject or by health professionals under confidentiality obligation, with the purposes of the protection of public health, preventive medicine, medical diagnosis, medical treatment or the planning of healthcare and its financing.

VII. Transfer of Data

Classified as a type of processing activity, transfer of data has the same conditions as other types of processing. However, the transfer of sensitive data and the transfer of any personal data have exceptional conditions.

Transfer of sensitive personal data requires additional physical and technical security measures. Although the Data Protection Board has

the authority to determine the minimum standards for these security measures, these standards have not yet been determined as of date.

The transfer of any personal data to third countries has additional conditions. Data controllers must ensure that:

- The third country to which the data is transferred has adequate level of protection, or;
- The data controllers in the third countries to which the data is transferred guarantee an adequate level of protection and the Data Protection Board approves the transfer.

If the transfer takes place on the grounds of explicit consent of the data subject, the abovementioned conditions are not required to be met.

VIII. Information to be given to Data Subjects

In accordance with the Art. 10 of the Code, data controllers must provide data subjects with a list of information about the processing activity. The scope of the information to be given to the data subjects is as follows:

- Identity of the data controller,
- The purposes of the processing,
- The identity of the third parties to whom data may be transferred and for what purposes,
- The means of collection of personal data and its legal basis,
- The rights of the data subject provided in the Art. 11 of the Code.

IX. Rights of the Data Subject

Every data subject has the right to obtain information from the data controller on;

- Whether or not his personal information is being processed or has been processed in the past,
- The processing activities relating to his personal data,
- The purposes of processing and whether or not it is being processed legally,

- The third parties to whom data has been transferred to,
- Rectification of the data if it is incomplete or erroneous,
- Erasure, destruction or rectification of the data.

Data subjects also have the right to object to data processing activities if the processing creates negative effects on the data subject; or ask for compensation if damages occurred due to the processing activities.

Data subjects have the right to contact data controllers in a written form or by means specified by The Board. Data controllers have the obligation to reply to request as soon as possible and in no longer than 30 days. Because replying and keeping track of requests is a workload for data controllers, data controllers can charge a small fee in exchange, in line with the list of tariffs which will be provided by The Board.

X. Erasure, Destruction or Anonymization of Data

When the purposes of processing of personal data disappear or come to an end, it is no longer legal to store the personal data. In that case, data controllers need to either erase, destroy or anonymise the personal data. Erasure or destruction of the data implies irrecoverable deletion of the data, which requires a certain level of technical expertise. The standards for the erasure or destruction of data will be set by the Board. However, although the Draft Regulation on the Erasure, Destruction and Anonymization of Data has been announced for the public opinion and suggestions, it has not yet been enacted.

Personal data relates to natural persons. However, if the links between the data and persons are irreversibly removed, data ceases to be personal. This process is called "anonymization". By anonymising personal data, data controllers can keep the data, even though the purposes for processing of personal data have disappeared, in order to use it for other purposes such as planning, research or statistics.

XI. Data Security, Sanctions and Liability

The liability of data controllers in the Code is open to broad interpretation as according to the Art. 12 of the Code, data controllers must implement "*all technical and administrative measures*" to

ensure data security, as opposed to the provision of the Directive 95/46 of the European Union which holds data controllers responsible only for all appropriate measures.[3] For that reason, data controllers must be very cautious while implementing security measures for data protection.

The scope of the data controller's responsibilities is as follows:

- To prevent illegal processing of personal data,
- To prevent unauthorized access to data,
- To ensure safe retention of data.

As a preventive approach, to ensure the lawfulness of the processing, data controllers should adopt internal policies relating to the internal operations of their companies such as privacy policies, and make the data available only to authorized personnel.

Sanctions for non-compliance in the Code can be categorized as administrative fines and penal sanctions. For criminal sanctions, the Code refers to Art. 135 – 140 of the Turkish Penal Code. These fines and penal sanctions are presented in the table below:

Unlawful processing of personal data	1-3 years of imprisonment
Unlawful disclosure, dissemination or obtainment of personal data	2-4 years of imprisonment
Failure to erase or destroy personal data	1-2 years of imprisonment
Failure to inform data subject	5.000 ₺ - 100.000 ₺
Non-compliance with the provisions of the Code relating to data security	15.000 ₺ - 1.000.000 ₺
Non-compliance with the decisions of the Data Protection Board	25.000 ₺ - 1.000.000 ₺
Failure to register with the Data Protection Agency	20.000 ₺ - 1.000.000 ₺

Legal person data controllers such as companies are responsible for the acts of the natural persons who act in their names, such as employees, and therefore the administrative sanctions are applied to

[3] Directive 95/46/EC Art. 17/1.

the legal persons themselves, not to their employees. Penal sanctions on the other hand can be applied to both the employees and the members of the board of directors who make the decisions that cause the unlawful processing of personal data.

Because the imprisonment sanctions cannot be applied to legal persons such as companies, in accordance with the Art. 140 of The Turkish Penal Code, legal persons may face criminal sanctions proper to legal persons. In worst case scenario, this may be the revoking of their operating licences.

XII. Register of Data Controllers

Data controllers will be accountable to the Data Protection Agency, which has the authority to fine and sanction data controllers within the framework of the Code. In order to make inspections and tracking of data controllers effective, The Code establishes a "Register of Data Controllers" and makes it obligatory for data controllers to register with the Data Protection Agency. Rules and procedures relating to the Register will be determined by the Data Protection Board. The Draft Regulation on the Register of Data Controllers has also been announced for the public's opinions and suggestions, but has not yet been enacted as of date.

XIII. Derogations from the Code

Certain processing activities do not fall under the scope of the Code, which are stated in the Art. 28. These derogations are as follows:

- Processing activities relating to purely personal or household activities,
- Processing for research, planning or statistical purposes by anonymization,
- Processing for national defence, national security, establishing public order,
- Processing for the purposes of art, history, literature, scientific research or within the context of freedom of expression, provided that it does not infringe fundamental rights and liberties.

- Processing carried out by judicial or enforcement authorities for the purposes of investigation and prosecution purposes.

GURULKAN ÇAKIR

GURULKAN ÇAKIR AVUKATLIK ORTAKLIĞI

Polat İş Merkezi, Offices 28-29
Mecidiyeköy 34387
Istanbul, TURKEY

T +90 212 215 30 00
M info@gurulkan.com
W www.gurulkan.com