GURULKAN ÇAKIR

Erasure, Destruction and Anonymization of Personal Data

Introduction

The codification of personal data protection in Turkish law is relatively a recent development. On 07.04.2016, the Code of Personal Data Protection numbered 6698 ("Code"), which is regulating the protection of personal data as well as imposing several liabilities on those dealing with personal data, has been enacted. Following the enactment of the Code, a number of regulations have been put into force for the purpose of providing an in-depth regulation and organization of the protection of personal data. The Regulation on the Erasure, Destruction or Anonymization of Personal Data ("Regulation"), being the main subject of this article, has been enacted on 28.10.2017. After the enactment of the Regulation, Turkish Data Protection Authority ("TDPA") has published the Guidelines on the Erasure, Destruction or Anonymization of Personal Data ("Guidelines") on its official website.

Policy

The Code allows the processing of personal data on the condition that there is a legal purpose for processing such data. The Code defined those persons and legal entities processing personal data and having the responsibility of establishing and managing a data recording system as "Data Controllers". Data Controllers are obliged to register in the Data Controllers Registry before they commence processing any personal data. Additionally, Data Controllers must

create a personal data processing inventory which contains and indicates the purpose of processing of personal data, category of data, maximum periods required for the actualization of the purpose of processing of personal data, types of personal data to be transmitted abroad, and lastly, precautions taken for the security of personal data.

The Regulation stipulates that Data Controllers must draw up, in accordance with the personal data processing inventory, a personal data storage and destruction policy. However, the mere fact that a personal data storage and destruction policy has been created does not mean that the personal data is stored, erased, destructed and anonymized in compliance with the provisions of the Code and Regulation.

The said policy must, at least, include the information pertaining to; (i) the purpose of the policy, (ii) recording mediums, regulated with the policy, for the storage and destruction of personal data, (iii) definitions of the legal and technical terms incorporated into the policy, (iv) elucidation as regards the legal, technical or other reasons requiring the personal data to be stored and destructed, (v) technical and administrative precautions taken for the purpose of preventing the unlawful processing of and access to the personal data, (vi) technical and administrative precautions taken for the destruction of the personal data in accordance with the law, (vii) titles, departments and work definitions of those persons partaking within the processes of storage and destruction of the personal data, (viii) the table indicating the periods of storage and destruction, (ix) periodical destruction intervals, and (x) if any update has been made within then-existing personal data storage and destruction policy, the explanation of such an update.

Background of Erasure, Destruction and Anonymization

Once all conditions for processing of personal data, which are defined explicitly in the Code, become obsolete, then Data Controllers, *ex officio* or upon the relevant person's request, are obliged to erase, destruct or anonymize the personal data. Within the process of the erasure, destruction or anonymization of the personal data, it is mandatory to comply with the general principles, and technical and administrative precautions defined in the Code,

as well as the provisions of relevant laws, decisions of the TDPA, and the personal data storage and destruction policy.

All operations executed in connection with the erasure, destruction and anonymization of the personal data must be recorded and preserved at least for 3 years. In this respect, Data Controllers are also obliged to explain, in the policy and the procedures, the methods they apply to the process of the erasure, destruction and anonymization of the personal data. In this regard, Guidelines provide implementable methods for the erasure, destruction and anonymization of the personal data, for the purpose of enlightening Data Controllers on how the said process should be conducted in compliance with laws.

Erasure

Both in the Regulation and the Guidelines, the erasure of personal data is defined as "the process of rendering the personal data inaccessible and unusable for the relevant users." It is also set forth that Data Controllers are liable for taking any technical and administrative precautions to ensure that the erased personal data cannot be accessed or used again.

The process of the erasure of the personal data is divided into four steps. These steps are set forth in the Guidelines as follows:

- Determination of the personal data to be erased,
- Ascertainment, by means of an access authorization and control matrix or a similar system, of the relevant users for each personal data,
- Ascertainment of the authorizations and methods, such as access, restoration and reuse, of the relevant users,
- Closure and abolishment of these authorizations and methods of the relevant users.

Destruction

The Regulation and the Guidelines define the destruction of the personal data as "the process of rendering personal data inaccessible, irretrievable and unusable for any person." As is the case with the erasure of the personal data, Data Controllers are also

liable for taking any technical and administrative precautions required for the destruction of the personal data.

It is stipulated that each copy of the personal data must be ascertained, and that one or more of the methods set forth within the Guidelines should be implemented for the purpose of destructing the personal data. The methods described within the Guidelines variate depending on the type of the medium the personal data is stored in. These mediums are ramified as local systems, circumferential systems, paper and microfiche systems, and cloud. For example, physical destruction of the medium is displayed as a method for the destruction of the personal data where the data is stored into a local system. Naturally, physical destruction method cannot be applied to the process of destruction of personal data where the data is stored in a cloud system. In this case, system-specific methods should be implemented for the destruction of the data in the cloud.

Anonymization

The anonymization of the personal data is defined as "rendering the personal data unidentifiable with a person whose identification is definite or ascertainable." With the anonymization of the personal data it is targeted that the linkage between the personal data and the relevant person is broken.

The methods of the anonymization of the personal data, within the Guidelines, are divided into three different sections. The first method set forth is the anonymization techniques that do not create value irregularity. When this technique is applied, no alteration, addition or exclusion is made within the values of the data; instead, alterations are made in the whole rows and columns in which the data is stored. By this way, individual values of the data are preserved, but the overall data goes through a shift. Some specific methods used within this technique are also displayed within the Guidelines as the sub-sections of the first technique of the anonymization.

Second method of the anonymization of the personal data is the anonymization techniques that create value irregularity. On the contrary to the previous method, by this method a value irregularity

is created within the data. When this method is implemented, it is important to determine the benefit to be obtained from the personal data; because the values carried by personal data records are altered. Even when the individual values of the personal data are altered, the benefit expected to be obtained from the data can be secured by way of preventing the disruption of the overall statistics. As is the case with the first method of anonymization, this method is also divided into specific methods as the sub-sections in the Guidelines.

Last method of the anonymization of the personal data is the statistical techniques that strengthen anonymization. It is possible that some values in the anonymized personal data may be identified with the relevant persons as a result of an aggregation with individual scenarios. For the purpose of avoiding such situation, a number of statistical methods can be used for strengthening the anonymization of the personal data by minimizing the individuality of the data records. The purpose of this method is to keep the benefit to be obtained from the data at a reasonable level while minimizing the risk of the disruption of the anonymization.

Data Controllers should decide which method is to be applied for the anonymization of the personal data based on several factors such as; the kind of data, the size of data, the structure of data, the benefit expected to be obtained from the data, the purpose of processing the data, the level of damage that may occur in case the anonymization of the data is disrupted.

Data Controllers must meet three requirements set forth within the Guidelines for being able to choose anonymization of the personal data instead of the erasure or the destruction thereof. These conditions are as follows:

- The anonymization cannot be disrupted by way of aggregating an anonymized data set with another data set,
- One or more values cannot constitute a meaningful aggregate that could enable the de-anonymization of a specific record,

- The values in the anonymized data set cannot be aggregated in such a way that allow data users to make assumptions and conclusions.

Time Periods

Data Controllers having created a personal data storage and destruction policy must erase, destroy or anonymize the personal data within the first periodical destruction process following the occurrence of the liability of erasing, destructing or anonymizing the personal data. The interval in which the periodical destruction process is to be executed should be determined within the personal data storage and destruction policy. The Regulation sets forth that this interval cannot exceed 6 months. Additionally, within the Regulation, the TDPA is authorized to shorten the relevant time periods in case damages that are unrepairable or extremely difficult to be compensated occur, or in case there is an explicit contradiction to law.

Upon the receipt of a request by a relevant person, if all conditions of processing of personal data have ceased, then the Data Controller must conclude the said request within thirty days and inform the relevant person. Where all conditions of processing of personal data have ceased but the personal data in question had been transferred to third parties, the Data Controller must notify the third party of the issue and ensure that the process stipulated within the Regulation is accordingly executed. If all conditions of processing the personal data have not ceased, the request of the relevant person may be explicitly denied by the Data Controller, and this denial must be communicated to the relevant person within 30 days in writing or electronically.

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