Turkish DPA's Guidelines on the Erasure, Destruction or Anonymization of Personal Data

Authors: Gönenç Gürkaynak, Esq., İlay Yılmaz and Burak Yeşilaltay, ELIG, Attorneys-at-Law

I. Introduction

The Regulation on the Erasure, Destruction or Anonymization of Personal Data ("Regulation") was published on the Official Gazette of October 28, 2017, as the first phase of the belated secondary legislation. Although the Regulation provided more specific and explicit provisions pertaining to the erasure, destruction or anonymization of personal data in comparison to the Law No. 6698 on the Protection of Personal Data, the practical uncertainty regarding the implementation of these provisions was unfortunately not resolved and the technical methods that could be used to fulfill the obligations set forth under these provisions still remained unclear.

Hence, a pressing need for guidance emerged with respect to the methods that could be used to comply with the legislation in terms of the erasure, destruction or anonymization of personal data. Accordingly, the Turkish Data Protection Authority ("DPA") published the Guidelines on the Erasure, Destruction or Anonymization of Personal Data[1] ("Guidelines") on its official website, to satisfy this apparent need.

The Guidelines explain and recommend acceptable methods that could be used for the erasure, destruction or anonymization of personal data in accordance with the legislation, by providing various examples that could be used by the data controllers. The Guidelines are based on the Regulation.

The purpose of the Guidelines is to provide clarity regarding the proper implementation of the relevant provisions of the legislation, and to present "best practices" examples to data controllers regarding the erasure, destruction or anonymization of personal data. As explained, the Guidelines explain the technical methods and tools that should be used for erasure, destruction or anonymization. Furthermore, a key part of the Guidelines elaborates on the approved tools and techniques that could be used for anonymization by offering various examples relating to each anonymization technique presented in the Guidelines. Please find more detailed explanations regarding each of these data protection processes in the sections below.

[1] The original text of the Guidelines is available at http://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20S%C4%B0L%C4%B0NMES%C4%B0,%20YOK%20ED%C4%B0LMES%C4%B0%20VEYA%20ANON%C4%B0M%20HALE%20GET%C4%B0R%C4%B0LMES%C4%B0%20REHBER%C4%B0.pdf

II. Erasure

The Guidelines define "erasure" as "the process of making it impossible for the relevant users to access or reuse personal data," in line with the Regulation.

The first step in erasing data is the identification of the particular piece of personal data to be erased. Thereafter, the relevant users should be determined, the means of access open to such users should be established, and, as a final step, the data should be erased, which means that access to the personal data in question should be prevented.

The Guidelines state that the specific erasure method that will be used by the data controller should be chosen in accordance with the particular storage platforms on which personal data is saved, and also offer examples of acceptable erasure methods by referring to the distinctions between various storage platforms. The Guidelines proceed to provide and explain separate techniques for erasing personal data on cloud systems, on paper, on office files in central servers, on portable media, and on databases.

III. Destruction

Destruction is defined in the Guidelines as "the process of making it impossible for personal data to be accessed, retrieved or reused by any person or by any means." This definition has apparently been taken directly from the Regulation.

The Guidelines clearly state that all copies of data must be identified, and that one or more of the methods described should be applied in order to destruct and destroy personal data, as required by the legislation. The Guidelines make an important distinction between various destruction methods and this distinction is based on where the personal data in question is held, such as local systems, circumferential systems, paper and microfiche systems, and cloud. Additionally, the Guidelines provide guidance for devices under maintenance and repair, by setting forth specific methods that can be employed by data controllers before sending such devices away for maintenance and repair services. These methods include taking certain measures in order to prevent technical personnel who are responsible for maintenance or repair services from copying or removing the data from the organization (i.e., taking data out of the premises or storage facilities of the data controller.)

IV. Anonymization

i. General

The last major topic addressed by the Guidelines (and also the most extensively discussed and elaborated issue) is anonymization, which is defined as "making it impossible to associate personal

data with an identifiable person, even if such data is matched with other data." This definition is also in line with the Regulation.

The main goal and purpose of anonymization is to break the connection between a piece of data and the person identified through that data. The Guidelines set out certain approved anonymization techniques, by dividing them into three categories:

(a) Anonymization techniques that do not create irregular values, such as removing variables, removing recordings, top- and bottom-limit coding, local suppression or sampling. When these techniques are used, anonymization is achieved by changing the rows and columns of the data scheme, instead of making any amendments or removals to the data. That way, the data are changed in general, but the values in the relevant fields remain unchanged and are maintained in their original form.[2]

(b) Anonymization techniques that do create irregular values, including micro-aggregation, data-swapping, and post-randomization techniques (such as adding noise to the data or resampling). In these techniques, the values are changed and the value scheme is also altered. Even so, it will still be possible to use and benefit from such anonymized data by protecting the overall statistics from distortion.

(c) Techniques that strengthen anonymization, such as k-anonymity, l-diversity and t-closeness. These techniques aim to minimize the risk of tarnishing the anonymization, while also enabling users to benefit from the anonymized data scheme.

ii. Determination of Methods to Apply to Personal Data

According to the Guidelines, the data controllers should determine which techniques they will use by evaluating the circumstances related to the personal data they possess. This evaluation should take into account the type of data in question, the purpose or expected benefit of processing personal data, the effort required for anonymization, and the storage platform used for the personal data, among others. The choice of the method used for the erasure, destruction or anonymization of personal data is left up to the data controllers' discretion. However, the Guidelines set out certain criteria for the data controllers to opt for the anonymization of personal data, instead of erasure or destruction. The Guidelines declare that data controllers should choose to anonymize personal data only if the following conditions are fulfilled:

[2] *See* http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=18A77E8D59ACD49F27B5F132F0FAEFCF?doi=10.1.1.403.4581&rep=rep1&type=pdf

- The anonymization cannot be defeated/overcome by combining or aggregating the anonymized data scheme with another data scheme,
- One or more input values cannot be combined or aggregated to create a substantive or meaningful grouping that could enable the isolation and de-anonymization of a specific record,
- The values in the anonymized data scheme cannot be combined or aggregated in such a way as to allow data users to create assumptions or reach conclusions.

iii. Reverse Anonymization

Anonymized data may still become personally identifiable information if reverse anonymization techniques are used (e.g., by employing several intervention methods), and such reverse anonymization attacks can be made by numerous different parties with varying motivations. As a result of such interventions and interferences, the identity of the real person whose data was anonymized may be revealed, specific information related to the real person may be divulged, or hypothetical information related to the real person may be exposed, and each one of these three results may lead to certain data protection risks. Therefore, the Guidelines suggest that data controllers should examine their anonymization techniques and investigate whether any such risks related to reverse anonymization exist for the techniques they use, and take the necessary precautions as a result of their investigations.

V. Conclusion

The Guidelines certainly bring clarity to this vital issue and provide more specific information regarding the methods that could be used by data controllers in order to comply with the legislation and fulfill their obligations regarding the erasure, destruction and anonymization of personal data. The Guidelines achieve this goal by setting forth various "best practice" methods and demonstrating how to implement these methods by offering illustrative real-world examples.

Although the Guidelines offer various methods for implementing each technique, and even though these methods and techniques are clearly explained through examples based on internationally recognized "best practices," there are some issues regarding the implementation of these techniques that still remain unclear and unresolved. For instance, one vital shortcoming of the guidance is that the pros and cons of the techniques set forth in the Guidelines are not sufficiently explained. The Information Commissioner's Office, which is the equivalent of the DPA in the United Kingdom, provides a "pros and cons" table,[3] which, if adopted in Turkey, would help data controllers and data processors to determine which methods best fit their purposes, whilst explaining the methods and techniques that they are allowed to use. Likewise, the option of outsourcing such techniques to a

[3] *See* https://ico.org.uk/for-the-public/online/deleting-your-data.aspx

service provider, and the conditions and requirements of this option, the distribution of liability in such cases, and its potential consequences have not been taken into consideration by the Guidelines either.

Furthermore, the Guidelines also do not include any indications, suggestions or guidance as to the scope of the disclosure (i.e., disclosure to the public, to the DPA or to the data subjects) that should be made by data controllers or as to the methods and techniques that should be used for such disclosure. In the "Guidance on Personal Data Erasure and Anonymization," which was published by the Office of the Privacy Commissioner for Personal Data in Hong Kong,[4] the correlation between retention and erasure policies is clearly set out, which also ensures that data controllers present evidence that they comply with the legislation provisions regarding erasure. However, the Guidelines fail to provide any correlation with the data retention and destruction policy required by the Regulation.

Since the Guidelines do not constitute a mandatory legal instrument that must be followed or adopted by the data controllers, and since this document only provides recommendations regarding the technical tools and methods that could be used by the data controllers to comply with the relevant legislation, the data controllers are not limited to the techniques and methods set forth under the Guidelines. However, in terms of laying out the "best practices," which are mainly based on Article 29 Data Protection Working Party Opinion 05/2014 on Anonymization Techniques,[5] and used on a global scale, it still leaves certain issues to the discretion of the data controllers.

Therefore, data controllers will need to conduct internal assessments to decide on the specific techniques, methods and practices that they could use (separately or in combination) to comply with the relevant legislation, based on the specific needs pertaining to their business and operations, and they would not be able to rely merely on the Guidelines issued by the DPA. In other words, abiding by the Guidelines (or adopting the techniques recommended by the Guidelines) will not always be sufficient on its own to ensure a data controller's compliance with its legal requirements and responsibilities as to the erasure, destruction and anonymization of personal data.

Article contact: Gönenç Gürkaynak, Esq. Email: gonenc.gurkaynak@elig.com

(First published in Mondaq on November 29, 2017)

[4] *See* https://www.pcpd.org.hk/english/publications/files/erasure_e.pdf
[5] *See* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf