Latest Developments in Turkish Data Protection Practice and Regulation

Authors: Gönenç Gürkaynak, Esq., Ceren Yıldız, Berna Aytaç and Ece Terziahmetoğlu, ELIG Gürkaynak Attorneys-at-Law

Recently, there have been certain significant developments regarding the data protection practice and some important guidelines have been published by the Turkish Personal Data Protection Authority. Below is an overview on the important points of the relevant developments.

I. Draft Guideline on Processing of Personal Data in Loyalty Programs

The Turkish Personal Data Protection Authority ("DPA") has published a Draft Guideline on Processing of Personal Data in Loyalty Programs ("Loyalty Programs Guideline") on June 16, 2022. The Loyalty Programs Guideline was not published yet and was open to public consultation until July 16, 2022. The draft version is not accessible currently and may change depending on the public consultation.

The Loyalty Programs Guideline mainly provides detailed information on the categories of personal data processed within the scope of loyalty applications, legal grounds for the processing of personal data, the discussion of the personal data processed within the framework of loyalty programs in the context of general principles, issues to be considered within the scope of loyalty practices in fulfilling the obligation of providing information by data controllers, as well as practice cases.

The Loyalty Programs Guideline classifies loyalty programs as: (i) programs rewarding regular customers based on consistency, (ii) programs enabling rewards in an interface where the identity of the customer is determined and their demographic/payment records are directed to the business database, (iii) programs targeting a limited and privileged customer base in return of a subscription fee, (iv) programs targeting many customers with easy and free subscription, (v) programs based on rewarding points in return for purchases, visits, likes on social media pages, downloading application, enlisting to e-mail subscription, etc. (vi) layered loyalty programs based on the spending thresholds that a customer reaches, (vii) paid/VIP loyalty programs, (viii) programs enabling refunds on payments, (ix) programs targeting ethical values such as donations in return for purchases, (x) programs enabling partnership, (xi) loyalty programs provided within a game application, and (xii) combined programs with mixed rewards.

In the Loyalty Programs Guideline, data controllers within the scope of loyalty programs are determined as loyalty program implementers. On the other hand, the Loyalty Programs Guideline, only considers real person customers as a data subject.

The Loyalty Programs Guideline remarks the personal data processed within the scope of loyalty programs, although it varies from application to application. The annexes of the Loyalty Programs Guideline provide a detailed practice example of personal data processed within loyalty programs through Radio Frequency Identification Technology (RFID), as well as categories of personal data.

Within the scope of loyalty programs, it is stated that the legal reason should be determined according to the purpose of processing personal data. If the purpose of the loyalty program is to provide only points/gifts/advantages to the customer in return for shopping within the framework of the determined criteria, the processing of the personal data of the customer in order to obtain this advantage/points/gift may be considered within the scope of the processing of the personal data of the parties to the agreement, provided that it is directly related to the establishment and performance of the agreement. However, in the processing of personal data belonging to the parties of the agreement, which are not directly related to the performance of the agreement, the data controller should evaluate in each case whether it can rely on another legal reason.

In the Loyalty Programs Guideline, the DPA also refers to profiling activities. The DPA states that data processing activities carried out for profiling are not mandatory within the scope of the performance of the agreement and that data controllers cannot rely on the legal reason for the performance of the agreement for such transactions.

The Loyalty Programs Guideline clarifies an approach that is followed in practice and adopted by the DPA. If an explicit consent is not provided, the goods/services may still be provided, however the additional benefits may not be provided. In order to accept that the explicit consent is not provided as a condition of the goods/services offered within the scope of the loyalty program and to be able to talk about the legality of the explicit consent given in this context, the data controller must ensure that the advantage provided with the loyalty program is reasonable and that the data subject does not suffer a significant disadvantage and their free will is not affected

The Loyalty Programs Guideline states that it is known that the contact information, which is in the nature of personal data processed for loyalty programs, is processed within the scope of sending commercial messages to individuals as part of the marketing strategies of the companies and that the consent of the person must be obtained in order to send electronical commercial messages and process personal data in the context of the provisions of the Regulation on Commercial Electronic Messages on the protection of personal data.

The Loyalty Programs Guideline underlines that the processing of personal data for the recognition of the customer for loyalty programs and the “purpose of processing” for the processing of the personal data of the customer in order to send electronical commercial messages are different from each other. In this context, the data controller should carefully evaluate whether the contact information of the loyalty program member can be used to send electronical commercial messages.

II. Guideline on Use of Cookies

The DPA has published the final version of Guidelines on the Use of Cookies [1](“Cookie Guidelines) on June 20, 2022. The Cookie Guidelines aim to provide a guidance for and practical advice for all data controllers who operate a website. The Cookie Guidelines cover the processing of personal data through cookies, and notes that those cookies that are not used for processing personal data are not in the scope of the Cookie Guidelines applicable to desktop and mobile websites or web applications.

The Cookie Guideline defines cookies as *“a type of text file placed on the user's device by the website operators and is transferred as part of the HTTP (Hyper Text Transfer Protocol) query”*. Cookies are classified according to the (i) duration of use, (ii) their purpose and (iii) their parties. With regard to their duration, cookies are classified as session or persistent cookies. As for their purpose, cookies are classified as strictly necessary cookies, functional cookies, performance - analytic cookies and ad/marketing cookies. Lastly, in terms of their parties, cookies are classified as first party cookies and third party cookies.

Within the scope of Law No. 6698 on the Protection of Personal Data (“Law No. 6698”), data controllers are advised to consider the following criteria when processing personal data through cookies:
- Criterion A: The use of cookies for the sole purpose of transmission of a communication over an electronic communication network,
- Criterion B: The use of cookies that are strictly necessary for providing the information society services that are explicitly requested by the subscriber or user.
As for cases that do not fall under the scope of these two criteria, the below conditions will be applicable for the use of the cookies. The conditions for processing of personal data regarding the cookies within the Scope of the Law No. 6698 are as follows:
- Explicit consent, or
- As a result of the assessment made by the data controller regarding the data processing activity through cookies, other data processing conditions set forth in Articles 5 and 6 of the Law should also be taken into consideration.

Explicit consent needs to be obtained through an active affirmative action, by specifically and separately informing the data subject on processing of personal data. Non-specific statements or consents that are not based on an active action by a data subject cannot be considered as valid explicit consent. Accordingly, merely visiting a website cannot be considered as giving explicit consent for cookie practices. It is important that an explicit consent is specific, informed and freely given. In this regard, besides the elements of explicit consent set forth under the Law, explicit consent must be obtained as an applicable legal ground for processing, before implementation of cookies.

The Cookie Guidelines list each cookie type and assesses them based on the above criteria.

Per the Cookie Guidelines, in cases where the issue of consent to cookies by placing a cookie wall for accessing the website is imposed on the data subject as a prerequisite for the service, the cookie wall may injure the free will of the data subject, and in this case, the explicit consent obtained will not be a valid explicit consent. In cases where third-party cookies are placed on the website, it is emphasized that both the website owner and the third party are obliged to ensure that users are clearly informed about cookies and to obtain their explicit consent when necessary.

[1] https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf (Last accessed on October 17, 2022)

In the event that websites operating in Turkey transfer data abroad by using cookies through companies located abroad, this activity must comply with the provisions of the Law No. 6698 on the transfer of personal data abroad. In this context, it is necessary to obtain explicit consent from the data subject or to have adequate protection in the country to which the transfer will be made, or to submit a letter of undertaking to the DPA.

The Cookie Guidelines also provide illustrative examples of "good practices" and "bad practices" for data controllers to obtain explicit consent when processing personal data through the use of cookies.

III. Guideline on Protection of Personal Data in the Banking Sector

The DPA and the Banks Association of Turkey, published the Guideline on Protection of Personal Data in the Banking Sector[2] ("Banking Guideline") on 5 August 2022.

The Banking Guideline states that banks are data controllers for the transactions they carry out within the scope of Article 4 (Operating Subjects) of the Banking Law No. 5411 ("Banking Law"). In addition, the Banking Guideline states that the characteristics of the case will be evaluated in order to determine whether a bank qualifies as a data controller or data processor for operations they conduct as an agency and intermediary organization regarding insurance, private pensions, investment instruments, international fast money transfers and payment for invoices, taxes and fees. The Banking Guideline also states that banks can be a joint data controller.

The Banking Guideline includes guidance on the issues that should be included in the data processing agreements to be made between the data controller and the data processor. Separate referrals are also made for the support services of banks, agreements made with companies and their affiliates, open banking and situations where banks act as agency.

Since the explicit consent to be obtained from the data subjects does not have to be "written", the bank does not have to provide a written and signed text, but the data controller is responsible for proving that explicit consent has been obtained. In the case of the branch, approval can be obtained for explicit consent texts from the data subjects, by ink signature or other methods (digital signature, e-signature, etc.) prescribed by the legislation to replace it. If the explicit consent is requested from the data subjects from the ATM, the consent for the explicit consent text can be obtained after the person logs into the ATM. When it comes to Internet/mobile banking, boxes/buttons and similar methods that can be ticked by people can be used in order to obtain explicit consent from the data subjects. In the selections made with this box/button and similar methods, the options should not be selected beforehand.

Pursuant to Article 73 (Keeping Secrets) of the Banking Law, information that constitutes a customer secret cannot be transferred in the country or abroad without the customer's request or instruction, even with the explicit consent of the data subject, except in cases of exception from the obligation to keep secrets. In the Banking Guideline, it is stated that the competent authorities may request information and documents from the banks in cases stipulated by the Law No. 6698, and that providing information within the scope of these requests is limited to answering the questions asked by the authorities on related issues in accordance with Article

[2] https://kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf (Last accessed on October 17, 2022)

73 and 159 of the Banking Law. In this context, banks will be able to transfer data to the competent authorities, provided that it is limited to the answers to information requests.

In terms of data transfers abroad, the Banking Guideline refers to the conditions stipulated in paragraph 6 of Article 9 of the Law No. 6698 and reminds that the provisions of other laws are reserved. The Banking Guideline also underlines that the provisions of the Banking Law regarding the transfer of customer secret data have special provisions according to Law No. 6698. These may not necessarily mean that cross-border personal data transfer is free of cross-border transfer conditions under the Law No. 6698 as long as it is allowed under the Banking Law. While assessing a cross-border transfer situation, both laws should be carefully assessed and applied together, when possible.

In the Banking Guideline it is also stated that the each bank will be able to create its own notice texts in accordance with its own operation and systems, within the scope of personal data categories, data collection method, processing purposes and legal justifications, and the parties to which personal data is transferred. On the other hand, the information to be given to the data subject within the framework of the obligation to notify must be compatible with the information disclosed in the Data Controllers Registry Information System (VERBIS). Since the bank has a large number of data processing purposes, it would be appropriate for banks to prepare the notice texts themselves. The Banking Guideline assesses specific situations banks may encounter and guides the banks on how to perform their transparency obligation. The Banking Guideline, considering, the banking practice, gives general advice on certain acceptable transparency methods such as providing a layered transparency notice i.e. first providing a summary explanation by directing the data subjects to a more detailed compliant transparency notice or by informing that their personal data are collected by providing an explanation as character limits in the banking technologies e.g. internet banking, ATMs allow.

On the other hand, banks are obliged to notify the real persons (staff, visitors, etc.) whose data they process. It is recommended in the Banking Guideline that additional information should be provided to the data subject at the stages of obtaining personal data within the scope of banking activities. For instance, specific notice can be made on issues such as the use of biometric data in identity verification or products/processes that may affect large audiences and where new technologies are used, or participation in contests/lottery. As a rule, the obligation to notify must be fulfilled by the data controller at the stage of obtaining personal data.

The obligation of deletion, destruction and anonymization of personal data in the Banking Guideline is processed under three headings: (i) storage of banking information, (ii) elimination of the purpose of processing and (iii) destruction methods. Banks are responsible for preparing inventory and keeping it up to date. Within the scope of these obligations, the Banking Guideline included guidance for banks by referring to the legislative items regarding the retention periods of data. In addition, there are guiding tables on the destruction methods of banks in the Banking Guideline. Banks must comply with both the data security obligations listed in the banking legislation and the data security obligations stipulated in accordance with the Law No. 6698. The Guide explains in detail the data security obligations of banks, which they are subject to in their legislation, and in which legislation they are included. Each bank also determines its storage and disposal policies in accordance with its assessment.

IV. Draft Guideline Regarding the Issues to be Considered in the Processing of Genetic Data

DPA has published the Draft Guidelines Regarding the Issues to be considered in the Processing of Genetic Data ("Genetic Data Guideline") for the execution of the processing activities of genetic data, which is considered as special categories of personal data, in accordance with the Law No. 6698. The Guidelines was open to public consultation from August 24, 2022 to September 24, 2022. Genetic Data Guideline has not been published yet and may change depending on the consultation.

Genetic Data Guideline indicates that for genetic data to be definable or informative, it must be analyzed. First, DNA and RNA output is created, then this DNA/RNA sample is processed based on the targeted study and raw data become analyzable. However, the Genetic Guideline emphasizes that raw data is still valuable and meaningful before analysis and have the potential to make an individual identifiable and if a DNA/RNA sample is requested, entire genomic data of the individual can be accessed, provided that sample was preserved properly. Therefore, all data controllers collecting biological samples must maintain all administrative and technical measures to provide security to the samples.

Genetic Data Guideline also refers to anonymization issue of the genetic data. Genetic Data Guideline emphasizes that whichever method is used, DNA samples provide a unique data about a data subject, hence it is impossible to sever the link between the data subject and the collected data. Therefore, instead of "anonymization", the term "de-identification" is used. Generally, genetic data is "de-identified" after process, through re-tagging with unique identifiers (x, y, z etc.) that are different from the assigned identifiers e.g. birthdate, location etc. when they were collected, then encrypted in a way to make it impossible to link the data subjects to their genetic material without the required key, however, people who have the relevant decryption, this link can be reformed (re-identification)

Genetic Data Guideline emphasizes that genetic data is only health data when they are processed for medical diagnosis and treatment and when they are not health data, they may be processed when there is an applicable processing condition under the Law No. 6698.

Genetic Data Guideline indicates that genetic data can be sent abroad voluntarily or when it is mandatory such as performing of a limited number of tests that are not available in Turkiye e.g. advanced cancer profiling, MRD. Genetic Data Guideline.

Genetic Data Guideline states that all individuals and legal entities that Genetic Disease Evaluation Centers are in relation with e.g. Ministry, university, legal entity etc. are data controllers. In a similar sense, cloud systems, where the genetic data are stored might be considered as data processors.

Genetic Data Guideline reiterates the explicit consent rules under the Law No. 6698 with a focus on genetic data and emphasizes that explicit consent must not be precondition for providing a service e.g. making food intolerance test mandatory to provide a nutritionist service. Genetic Data Guideline also indicates that sometimes, genetic data can be processed commercially, without a purpose of medical diagnosis and treatment such as identification of lineage, determining inclination to sportive activities or certain talents. In such cases, when the personal data will be processed with explicit consent, data subject must be properly informed not by indicating the risks that data subjects may encounter but also the risks involving the persons who are tied to their parentage.

Genetic Data Guideline also focuses on the matter of processing for scientific purposes and indicates that Regulation on Processing Personal Health Data underlines the conditions for using health data on scientific purposes. Genetic Data Guideline emphasizes that for a singular genetic data to be unassociated with an identifiable individual is only possible when such data is transformed into cumulative variant frequency lists achieved through combining multiple data of the same kind belonging to other individuals (genome aggregation data). Processing such data is only possible after obtaining ethical board permissions within the scope of a scientific research and complying with the relevant laws. Doing this, data controllers must minimize the personal data risks by using methods de-identifying the person as much as possible with methods such as pseudonymisation.

Genetic Data Guideline further indicates data controller obligations under the Law No. 6698, suggests administrative and technical measures and finally provides a section of suggestions and recommendations directed to regulation and management of genetic data mostly directed at regulatory and health authorities.

Article Contact: Gönenç Gürkaynak, Esq. E-mail: gonenc.gurkaynak@elig.com

(First published by Mondaq on October 26, 2022)