

BİÇER GÜNER

Attorneys-at-Law

Bimonthly Data Protection and Privacy Bulletin

February 2024



Dear Readers,

As Biçer Güner Attorneys-at-Law, we are pleased to share with you our newsletter on the developments in the field of Personal Data Protection in Türkiye. In this newsletter, we provide content that will briefly inform you about the decision of the Constitutional Court regarding the legislation and practice, the guidelines published by the Personal Data Protection Authority, the decisions rendered by the Personal Data Protection Board, and the administrative fines to be applied in 2024.

Table Of Contents

1. <i>Constitutional Court Decision On The Rejection Of Objections Against The Decisions Of The Personal Data Protection Board Without Justification.....</i>	1
2. <i>The Guideline On Considerations In The Processing Of Genetic Data Published</i>	1
3. <i>Recommendations For The Protection Of Privacy In Mobile Applications Published.....</i>	2
4. <i>Guideline On The Processing Of Republic Of Türkiye Identity Numbers Published</i>	3
5. <i>Guideline On The Protection Of Personal Data In Election Activities Published</i>	3
6. <i>Decisions Published By The Board</i>	4
7. <i>Administrative Fines To Be Imposed In 2024 Under The Law</i>	6



1. Constitutional Court Decision on the Rejection of Objections Against the Decisions of the Personal Data Protection Board without Justification

With the "*M.I.I. Application Decision*" ("**Decision**") numbered 2020/7518 and dated October 12, 2023 and published in the Official Gazette dated 15.12.2023 and numbered 32400, the Constitutional Court ruled that the right to property of the applicant was violated as a result of the rejection of the objection to the administrative fine imposed on the applicant by the Personal Data Protection Board ("**Board**"), by the Criminal Judgeship of Peace without any evaluation, on the grounds that the necessary technical and administrative measures to ensure data security were not taken in accordance with the on Personal Data Protection Law No. 6698 ("**Law**").

In the case subject to the Decision, the Board imposed a total administrative fine of TRY 1,450,000 on the applicant on the grounds that the customer reservation and guest database of the accommodation company acquired by the applicant in 2016 was accessed without authorization, however, the applicant did not take the necessary technical and administrative measures to ensure data security in accordance with the relevant articles of the Law and did not comply with the obligation to notify the violation within the shortest time possible.

The applicant objected to the Decision with the request to abolish the administrative fine, claiming that the Board's decision regarding the administrative fine did not contain a sufficient justification, that the administrative fine was not applicable in terms of time, that fault liability is

essential in the protection of personal data, that it was unlawful to impose a fine despite taking all measures and having no fault, that the administrative fine was contrary to the principle of proportionality and the principle of equality when compared to the other events subject to the fine. The Criminal Judgeship of Peace ("**Judgeship**") dismissed the applicant's objection and rendered its final decision by declaring that the administrative sanction imposed was in compliance with the law and procedure, and the applicant's objection to the dismissal decision was dismissed again as the decision was in compliance with the law and there was no matter that needed to be modified.

The applicant made an individual application to the Constitutional Court with the allegations that the court of first instance decided to reject the objection without conducting a sufficient and necessary examination, that the imposition of an administrative fine at the maximum level was not proportionate, and violated his property right.

As a result of its examination, the Constitutional Court stated that imposing obligations on data controllers to protect and ensure data security and imposing sanctions in case of breach of these obligations is in the public interest and is a convenient tool to ensure the appropriate level of security. However, in the concrete case, the Constitutional Court concluded that the applicant's relevant claims were significant allegations that affected the entire judicial process that they had to be addressed and that no evaluation was made by the Judgeship on the applicant's objections, and therefore the procedural safeguards for the protection of the right to property were not fulfilled in the concrete case and the right to property was violated. The relevant Decision will be directed to the Istanbul Anadolu 1st Criminal Judgeship of Peace, which examined the applicant's objection to the administrative fine, and the Judgeship shall initiate retrial proceedings and establish a new decision that eliminates the reasons that led the Constitutional Court to the conclusion of violation.

The decision emphasized the importance of explaining the justifications for the administrative fines imposed by the Board in a legally necessary and sufficient manner and stated that the decisions and the appeal processes against these decisions should be fully and in detail justified without prejudice to constitutional rights.

2. The Guideline on Considerations in the Processing of Genetic Data Published

The Guideline on Considerations in the Processing of Genetic Data ("**Genetic Data Processing Guideline**") was published by the Personal Data Protection Authority ("**Authority**") on its official website on October 13, 2023. The Genetic Data Processing Guideline regulates the areas of use and processing conditions of genetic data, which are accepted as special categories of personal data under the Law, genetic data controllers, data subjects, and their obligations, genetic data security, and finally the recommendations and suggestions of the Authority.

Within the scope of the Genetic Data Processing Guideline, genetic data is defined as *all or part of the information derived from all DNA, RNA, and protein sequences encoded from the genome, cell nucleus, or mitochondria of a living being*. Biometric and genetic data of individuals are also defined as special categories of personal data in Article 6 of the Law. Accordingly, the data controllers are required to process genetic data in the light of the general principles of personal data processing stipulated in the Law, based on the appropriate legal grounds and to fulfill their obligations in accordance with the Law on the determination of lineal descendant and genetic predisposition in the processing of genetic data used in genetic analyses for purposes. In addition, within the scope of the principles of convenience, necessity, and proportionality, in order to realize the result targeted by the processing of genetic data, only the data aimed at achieving the purpose

in question should be processed, and in this direction, tools/methods that require the least intervention (i.e., data minimization), which ensures the processing of less amount and type of personal data, should be used. The data controller is also obliged to explain the genetic data processing activities and their consequences to the **data subject** whose genetic data is processed in a clear and comprehensible manner and should not exceed the scope of consent.

On the other hand, in order for genetic data to be transferred abroad, either **(i)** the explicit consent of the data subject must be obtained, or **(ii)** in cases where explicit consent is not required, there must be adequate protection in the foreign country to which the genetic data will be transferred (*the list of foreign countries with adequate protection has not yet been published by the Authority*); or **(iii)** in the absence of adequate protection, the data controllers in Türkiye and in the relevant foreign country must obtain the Board's permission by undertaking in writing to provide adequate protection. Furthermore, the Genetic Data Processing Guideline also states that, without prejudice to the provisions of international agreements, in cases where the interests of the data subject or Türkiye may be seriously harmed, transfers may be made abroad with the permission of the Board, provided that the opinion of the relevant public institution is obtained.

Due to the sensitivity of genetic data, data controllers are recommended to take the technical and administrative measures under the Genetic Data Processing Guideline, as well as the *Adequate Measures to be Taken by Data Controllers in the Processing of Sensitive Personal Data* as set out in the [Board's Decision No. 2018/10 dated January 31, 2018](#), in order to ensure the security of the data. Accordingly, if genetic data is to be stored in the cloud systems, a record of the data stored in the cloud should be kept, backups should be taken outside the cloud, and a two-step authentication control should be applied for remote access. In addition, access to systems to be encrypted with cryptographic methods should be limited to authorized personnel. In cases such as maintenance, repair, and return of the devices used during data processing, it should be ensured that there is no personal data on the devices and servers, and a written commitment should be obtained from the owner of the device. For the data processing system, certified devices and up-to-date software should be used, patch management should be provided, and open-source software should be preferred and first tested by using synthetic data. In addition, hardware and software security tests of the systems should be performed periodically. By adopting the principle of "Privacy by design", which envisages compliance with data protection rules from the design stage of genetic data privacy, personal data protection rules and privacy should be taken into account from the construction stage of software and appropriate systems should be integrated. Also, genetic data should be stored by authorized and knowledgeable individuals with whom a confidentiality agreement has been executed. These principles and criteria set out in the Genetic Data Processing Guideline must be recorded and documented by the data controller and disclosed to the public.

3. Recommendations for the Protection of Privacy in Mobile Applications Published

Recommendations for the Protection of Privacy in Mobile Applications ("**Recommendation**") was published by the Personal Data Protection Authority on its official website on December 22, 2023. The Recommendation addressed the existing and potential risks regarding the protection of privacy in mobile applications used especially on smartphones and tablets through examples and provided general recommendations for data subjects and data controllers in terms of the processing of general and sensitive personal data within the scope of the Law No. 6698 on the Protection of Personal Data through mobile applications.



The Recommendation indicates that many actors such as the application provider, application developer, advertising network, application store organization, operating system provider, library provider, and device manufacturer may be responsible for the processing and protection of personal data in mobile applications. Accordingly, although it varies according to the functionality and design of the application and the permissions given by the user, recommendations were made to both application users and persons who may be considered as data controllers and/or data processors in order to protect the privacy of individuals in the processing of personal data such as the *user's identity information, membership information, contact information, financial information, user interactions, location information, online identifiers, phone book or friend lists, sensitive personal data include biometric data and health data* in applications and to ensure that the data processing activities carried out through applications comply with the principles set out in the Law.

⇒ Recommendations for Users:

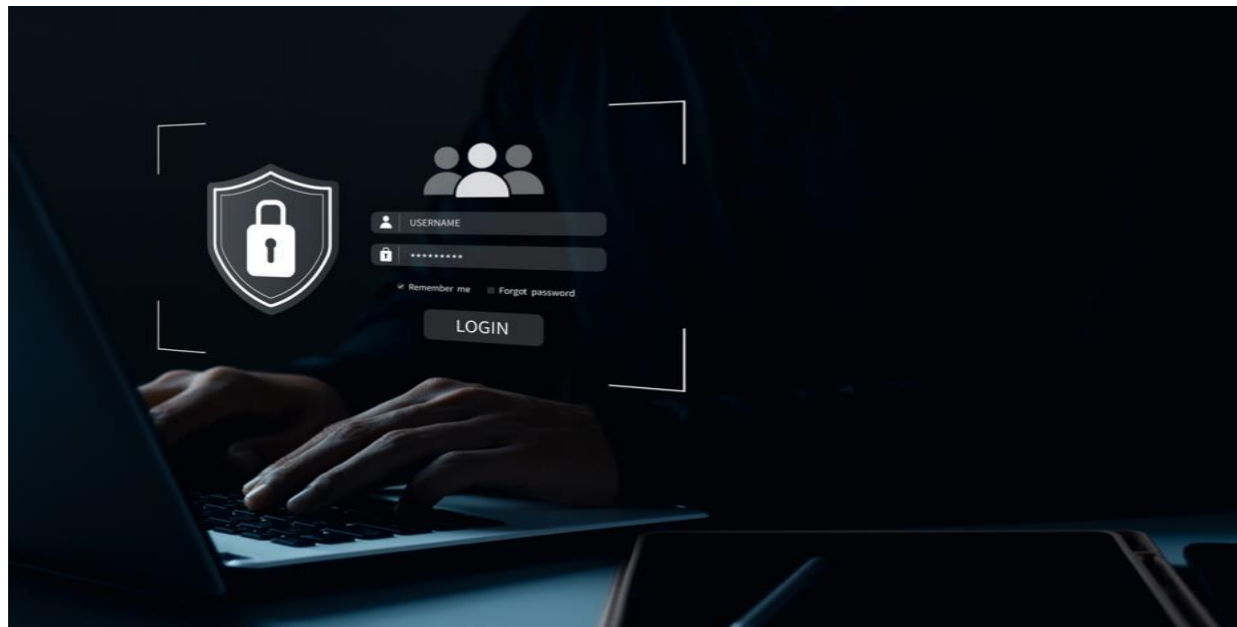
According to the Recommendation, apps should be downloaded from sources that are considered to be reliable, such as official app stores like AppStore or GooglePlay, or the official website of the mobile app provider, after receiving information about the developer of the app and ensuring that the app name is correct. Although high app ratings and positive reviews do not necessarily guarantee that an app is reliable, reviews and ratings should be evaluated to get an idea of the functionality and reliability of the app. In particular, the privacy policy of the app to be downloaded should be reviewed and it should be checked which data it requests access to. If there is a concern about the protection of privacy in access permissions such as location, audio, video, etc. requested by the application, access requests should be rejected and an alternative application should be searched for, if necessary. When creating passwords to be used in applications, strong combinations should be preferred as much as possible, different passwords should be created for each account and two-factor authentication should be enabled. In addition, the use of social media accounts should be avoided when logging in to applications as this will lead to the application collecting information from the social network account.

⇒ Recommendations for Parties Processing Personal Data:

Personal data processing activity must be carried out in accordance with the Law in the processes of development, launch and use of mobile applications by the relevant persons. In this context, personal data should be processed in accordance with the law and in good faith, accurately and up-to-date, within the framework of specific, clear and legitimate purposes, in a limited and measured manner, and should be kept in accordance with the legal retention periods. In this context, it has been recommended that application developers and providers should be honest and transparent in their personal data processing activities, and in this direction, in accordance with the obligation to disclose, facilitate access to the privacy notice and privacy policy, if prepared separately, and use a user-friendly interface for privacy settings and updates, by taking into account the rights and interests of users. In addition, it is essential to determine the processing conditions that will form the basis for processing personal data through mobile applications and to set forth their justifications. In carrying out the data processing activity, the data controller should first assess whether any of the other data processing conditions other than explicit consent can be relied upon, and if none of these are available, it should ensure that the user's explicit consent is obtained.

The Recommendation also raised as a problem the fact that the software does not provide the opportunity to give permission to the application and third parties integrated into the application separately and stated that while obtaining user permissions, it should be transparent regarding the third-party transactions utilized in the application and that this service should not be used in the application unless there is a legal reason for processing personal data through the third-party service integrated into the application.

On the other hand, users should be given the opportunity to correct personal data to ensure that it is accurate and up-to-date in order to ensure currency in applications and to prevent identity theft in terms of outdated personal data. In addition, the processed data must be suitable for the realization of the purposes determined by the use of the application. What is important here is to collect the least possible type and number of personal data to achieve the purpose within the framework of data minimization and proportionality principles and to avoid data processing that is not necessary for the purpose.



Finally, in terms of ensuring data security, the Recommendation recommends that mobile applications should be designed in compliance with the privacy by design and privacy by default principles, which ensure compliance with data protection rules, that multi-factor authentication methods should be used on devices to prevent unauthorized access to devices using the applications, that regular patch management and software updates be performed and that methods such as CAPTCHA be included in user logins as a precaution against bot attacks, and that personal data be encrypted through an adequate encryption layer and secure management of relevant encryption keys for effective storage and transmission.

4. Guideline on the Processing of Republic of Türkiye Identity Numbers Published

The Authority published Guidelines on the Processing of Republic of Türkiye Identity Numbers ("**TRIN Guideline**") on 16.01.2024. The purpose of the TRIN Guideline is to highlight the legislative provisions envisaging the processing of the Republic of Türkiye identification number ("**TRIN**") and to guide data controllers on how to carry out TRIN processing activities in accordance with the Law.

According to the TRIN Guideline the important issues in the processing of the TRIN are as follows: (i) to consider whether methods that interfere less with the right of data subjects to protect their personal data are possible, (ii) to carry out the data processing activity in accordance with the law, (iii) to take the necessary technical and administrative measures by the data controllers, and (iv) to ensure that the TRIN is processed in accordance with the Law and its secondary legislation.

On the other hand, the TRIN Guideline provides examples of circumstances where the processing of the TRIN is envisaged and the relevant legislation provisions. The examples of these circumstances and legislative provisions given by the TRIN Guidelines can be summarized as follows:

- issuing invoices for the exchange of goods and services,
- order and cargo delivery,
- Sending commercial electronic messages by tradesmen,
- registration in the trade registry and obtaining a registration certificate,
- legal transactions conducted at notary publics,
- filing of lawsuits,
- prevention of laundering proceeds of crime.
- cases where documents containing TRIN or identity information are presented, shown, or notified to the competent authorities for identification and other purposes.

5. Guideline on the Protection of Personal Data in Election Activities Published

The Authority published the Guideline on the Protection of Personal Data in Election Activities ("**Election Guideline**") on 24.01.2024. The purpose of the Election Guideline is to remind their obligations under the Law to the public administrations, political parties, candidates, and electors who are involved in election activities as well as their rights under the Law. You may see below a summary of the highlights of the Electoral Guideline:

- The Election Guideline states that each of the Supreme Board of Elections ("SBE"), political parties, and independent candidates are considered to be data controllers in terms of the data processing activities that they carry out within the scope of election activities.
- As per Article 28 of the Law, the provisions regulating the obligation to inform data subjects, the rights of data subjects (except the right to claim compensation for damages) and the obligation to register with the Data Controllers Registry will not apply to the SBE, which is responsible for the management and supervision of elections. On the other hand, it is emphasized that political parties and independent candidates are obliged to inform the data subjects and to ensure that data subjects can exercise their rights during personal data processing activities.
- It is stated that special categories of personal data including health data such as disability data can be transferred by the SBE without obtaining the explicit consent of the data subjects based on the provision regulated in Article 8 Paragraph 3 of the Law stating that "Provisions in other laws regarding the transfer of personal data are reserved", by citing Article 6 of Law No. 7062 and Articles 36 and 74 of Law No. 298 as examples.
- It is stated that political parties may process communication data in order to send audio, video, or written messages to their members; however, it will not be possible for them to conduct propaganda by sending messages to the e-mail addresses of citizens, or by sending audio, video or written messages to their phones.
- The Election Guideline emphasizes that independent candidates should not send audio, video, or text messages to citizens and should not process citizens' personal data for this purpose.

6. Decisions Published by the Board

⇒ Decision No: 2023/567

Subject: Regarding the obligation to save credit/debit card information in order to shop from an e-commerce site

Assessment: The registration and storage of a credit card or debit card in any system on an online shopping platform shall not be mandatory, and such registration may only be made with the explicit consent of the data subject without impairing their free will.

⇒ Decision No: 2023/695

Subject: Unlawful access to the data of the data subject in the e-pulse system by a private medical center

Assessment: If the unlawful data processing activities carried out by the employees at their own discretion occur within the data controller's space, the data controller will be responsible for this violation.



⇒ Decision No: 2023/845

Subject: Unlawful processing of personal data by a cargo company employee through sending a text message to the data subject's phone after the delivery of the cargo

Assessment: All persons working on behalf of the data controller even through sub-contracting, or a similar relationship should be provided with personal data protection training by the data controller. This obligation, which is considered within the scope of administrative measures, is not limited to the data controller's own employees.

⇒ Decision No: 2023/924

Subject: Unlawful processing of personal data of the data subject by the parking lot operator data controller and failure to fulfill the obligation to disclose

Assessment: The decision indicates that it is possible to process personal data to be submitted as evidence. However, it should not be forgotten by the data controllers that the data subjects should be informed about this matter. Otherwise, as in the decision, even if the data processing activity is lawful, data controllers may be penalized for failure to fulfill the obligation to disclose.

⇒ Decision No: 2023/1041

Subject: On the failure of the data controller to duly fulfill the disclosure obligation on its website and to oblige the service it provides to be conditional on explicit consent

Assessment: In the Decision, it was held that if alternative sales channels are offered to users, the data transfer abroad in sales conducted through the Internet may be subject to the condition of explicit consent.

⇒ **Decision No: 2023/1130**

Subject: Disclosure of the report and medication records of the data subject by the pharmacy to the former spouse

Assessment: In its assessment within the scope of the decision, the Board determined that since the Ministry of Health is responsible for the establishment and management of the Medula system, pharmacists are data processors in terms of the data entered into this system. On the other hand, in the case subject to the decision, as the pharmacist went beyond entering the information into Medula (printing out the report and medication list of the data subject and sharing it with a third party), the pharmacist was considered as a data controller. Accordingly, it has been stated that data processors shall be considered as separate data controllers if they exceed the instructions given by the data controller.

⇒ **Decision No: 2023/1234**

Subject: Processing of personal data by a car rental company upon requesting a Findeks report from the data subject

Assessment: E-marketplaces acting as intermediary service providers do not have the title of data controller in terms of processing activities carried out exclusively by sellers. Providing Findeks reports, which are requested subject to explicit consent, as a condition for the provision of the service, will be deemed invalid since it contradicts the principle that explicit consent is based on free will.

⇒ **Decision No: 2023/1309**

Subject: Unlawful disclosure of personal data of the data subject by an airline company to third parties

Assessment: The decision states that the data controller must immediately notify the data breach upon receiving a data breach notification, even within the scope of the data subject application.

```

40 .myphoto{
41   width: 500px;
42   margin-top: 15%;
43   clip-path: polygon(25% 0%, 100% 0%, 75% 100%, 0% 100%);
44 }
45 .myphoto2{
46   display: none;
47 }
48 .intro{
49   font-weight: 600;
50   font-family: Montserrat, Sans;
51   line-height: 2.2;
52   font-size: 70%;
53   /* margin-right: 50px; */
54 }
55 .intro1{
56   padding-top: 10px;
57   padding-bottom: 10px;
58   font-size: 157%;
59   color: #65159a;
60 }
61 .intro2{
62   margin-top: 20px;
63   margin-bottom: 20px;
64   font-size: 90%;
65 }

```

⇒ **Decision No: 2023/1310**

Subject: Processing of personal data through processing facial data when assigning a digital password in a bank's mobile application

Assessment: Within the scope of the Decision, biometric data in mobile banking may be processed with explicit consent in the presence of a legitimate reason such as identity verification.

⇒ **Decision No: 2023/1321**

Subject: Continuation of the processing of the e-mail data of the data subject by the data controller company of which the data subject was previously a partner

Assessment: E-mail accounts belonging to data subjects, the employees or former partners, should be set up in such a way that they will not receive new e-mails after leaving their jobs, in other words, after the end of their relationship with the data controller, the relevant e-mail accounts should be closed.

⇒ **Decision No: 2023/ 1356**

Subject: An employer's submission of footage of a person praying in a masjid in a reinstatement case

Assessment: The decision states that it is possible to record footage in the workplace for certain purposes. However, as stated in the decision, the privacy expectations of individuals should also be taken into consideration in determining the recording areas, and recording should not be made in areas such as prayer rooms and rest rooms. As a matter of fact, evidence obtained by exceeding these criteria and presented to the courts should be considered unlawful and should not qualify as evidence.

⇒ **Decision No: 2023/1414**

Subject: Disclosure of sensitive personal data of the data subject by the lawyer to the court

Assessment: In the decision, it is stated that DNA test results can be used by each person who possesses this common data as it is the common data of more than one person. As a matter of fact, the Code of Civil Procedure may constitute a legal basis for the submission of sensitive personal data to the courts as evidence, and when submitting personal data to the courts as evidence, the legal reason for the establishment / protection and exercise of a right may be relied upon.

⇒ **Decision No: 2023/1461**

Subject: Use of security cameras with audio recording capability

Assessment: In the decision, recording and processing video footage with security cameras is considered lawful, while recording and processing audio footage is considered unlawful, except in exceptional circumstances.

⇒ **Decision No: 2023/1465**

Subject: Display of personal data of a third-party during user login on the website of the data controller

Assessment: In the case subject to the decision, a user who logged in to the website of the car rental company with his/her own username and e-mail address was directed to the account of another user due to a system error. The Board stated that only the viewability of this data is considered as a data processing activity and no data breach notification was made despite the fact that the data of four people were affected by the technical error in question, that an ex officio investigation was initiated as a result of the notification of the person who was provided with unauthorized access, that the personal data of the whistleblower does not need to be affected by the incident in order to make a notification. Furthermore, as a result of the investigation, it was determined that the data controller did not take the necessary security measures and that a data breach notification should have been made due to this unauthorized access.

Consequently, it is obligatory to provide a data breach notification even if a single data subject is affected by a data breach.

⇒ **Decision No: 2023/1548**

Subject: Audio recording, disclosure and submission to the court file without the explicit consent of the person concerned

Assessment: The decision states that in certain circumstances, audio recordings may be used as evidence in lawsuits between the employee and the employer. In line with the established jurisprudence of the Supreme Court of Appeals, these certain circumstances are the cases where the employer does not have the possibility of proving the termination of the employment contract for just cause by other evidence, or where there is an aim to prevent the loss of evidence that would be possibly lost. In such cases, the data controller employer will be able to rely on the legal ground for the establishment/protection and exercise of a right.

⇒ **Decision No: 2023/1578**

Subject: Transfer of sensitive personal data of the data subject in the patient file to the court

Assessment: The decision states that the data controllers who responded and submitted documents within the scope that are specified in the court orders acted in accordance with the law.

7. Administrative Fines to be Imposed in 2024 under the Law

Obligations	2024 Lower Limit (TRY)	2024 Upper Limit (TRY)
Breach of Disclosure Obligation	47,303₺	946,308₺
Breach of Data Obligation	141,934₺	9,463,213₺
Failure to Fulfill Board Decision	263,557₺	9,463,213₺
Violation of VERBIS Registration and Notification Obligation	189,245₺	9,463,213₺

Should you have any queries on the above, please contact us.

Contact

Burçak Kurt Biçer
Managing Partner
burcak.bicer@bicerguner.com

Uğurkan Şeber
Senior Associate
ugurkan.seber@bicerguner.com

İrem Efe
Associate
irem.efeb@bicerguner.com

BİÇER GÜNER

Attorneys-at-Law

Bimonthly Data Protection and Privacy Bulletin

Şubat 2024



Değerli Okuyucularımız,

Biçer Güner Avukatlık Ortaklığı olarak, Türkiye'deki Kişisel Verilerin Korunması alanında meydana gelen gelişmelere dair hazırladığımız bülteni sizlerle paylaşmaktan memnuniyet duyuyoruz. Bu bültenimizde, Anayasa Mahkemesi'nin mevzuat ve uygulamaya ilişkin kararı, Kişisel Verileri Koruma Kurumu tarafından yayımlanan rehberler, Kişisel Verileri Koruma Kurulu tarafından verilen kararlar ve 2024 yılında uygulanacak idari para cezaları hakkında siz değerli okuyucularımızı kısaca bilgilendirecek içeriklere yer veriyoruz.

İçindekiler

1. *Kişisel Verileri Koruma Kurulu Kararlarına Karşı İtirazların Gereksiz Reddedilmesi Hakkında Anayasa Mahkemesi Kararı* 1
2. *Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber Yayımlandı* 1
3. *Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler Yayımlandı*..... 2
4. *Türkiye Cumhuriyeti Kimlik Numaralarının İşlenmesine İlişkin Rehber Yayımlandı* 3
5. *Seçim Faaliyetlerinde Kişisel Verilerin Korunması Rehberi Yayımlandı* 3
6. *Kurul Tarafından Yayınlanan Kararlar* 4
7. *Kanun Kapsamında 2024 Yılında Uygulanacak İdari Para Cezaları* 6



1. Kişisel Verileri Koruma Kurulu Kararlarına Karşı İtirazların Gereksiz Reddedilmesi Hakkında Anayasa Mahkemesi Kararı

Anayasa Mahkemesi (“AYM”), 15.12.2023 tarih ve 32400 sayılı Resmî Gazete’de yayımlanan 2020/7518 numaralı ve 12.10.2023 tarihli “M.I.I. Başvurusu Kararı” (“Karar”) ile, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) uyarınca veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirlerin alınmadığından bahisle Kişisel Verileri Koruma Kurulu (“Kurul”) tarafından Başvurucuya uygulanan idari para cezasına itirazın Sulh Ceza Hakimliği tarafından hiçbir değerlendirme yapılmadan reddedilmiş olması sebebiyle Başvurucunun mülkiyet hakkının ihlal edildiğine karar vermiştir.

Karara konu olayda Kurul, Başvurucunun 2016 yılında devraldığı konaklama şirketindeki müşteri rezervasyon ve misafir veri tabanında yetkisiz erişim gerçekleştiği ancak Kanun’un ilgili maddeleri uyarınca veri güvenliğinin sağlanmasına yönelik gerekli teknik ve idari tedbirlerin alınmadığı ve ihlalin en kısa sürede bildirilmesi yükümlülüğüne uyulmadığı gerekçeleriyle Başvurucu hakkında toplam 1.450.000 TL idari para cezası uygulanmasına karar vermiştir.

Başvurucu, idari para cezasına ilişkin Kurul kararının yeterli bir gerekçe içermediğini, idari para cezasının zaman bakımından uygulanabilir olmadığını, kişisel verilerin korunmasında kusur sorumluluğunun esas olduğunu, tüm tedbirleri almasına ve kusuru olmamasına rağmen ceza verilmesinin hukuka aykırı olduğunu, idari para cezasının ölçülülük ilkesine ve diğer cezaya konu edilen olaylar ile karşılaştırıldığında eşitlik ilkesine aykırı olduğunu iddia ederek idari para cezasının kaldırılması talebiyle karara itirazda bulunmuştur. Sulh Ceza Hakimliği (“Hakimlik”) tarafından ise uygulanan idari yaptırım yasa ve usule uygun bulunarak Başvurucunun itirazı reddedilmiş, red kararına yapılan itiraz ise kararın uygunluğundan ve değiştirilecek bir husus bulunmadığından kesinleştirilmiştir.

Başvurucu ilk derece mahkemesi tarafından yeterli ve gerekli inceleme yapılmaksızın itirazın reddine karar verildiği, en üst haddeden idari para cezası uygulanmasının orantılı olmadığı ve mülkiyet hakkını ihlal edildiği iddialarıyla Anayasa Mahkemesine bireysel başvuruda bulunmuştur.

Yaptığı inceleme sonucunda AYM, veri sorumlularına veri güvenliğinin korunması ve sağlanması için yükümlülükler getirilmesinin ve bu yükümlülüklerin ihlali hâlinde yaptırım uygulanmasının kamu yararına yönelik olduğunu ve uygun güvenlik düzeyini temin etmeye yönelik elverişli bir araç olduğunu belirtmiştir. Ancak, somut olay nezdinde AYM, Başvurucunun ilgili iddialarının yargılama sürecinin bütününe etkileyen önemli ve karşılanması gereken iddialar olduğunu belirterek, Başvurucunun bu itirazları hakkında Hâkimlik tarafından hiçbir değerlendirme yapılmadığı, bu sebeple mülkiyet hakkının korunmasına yönelik usule ilişkin güvencelerin somut olayda yerine getirilmediği ve mülkiyet hakkının ihlal edildiği sonucuna varmıştır. Kararın, Başvurucunun idari para cezasına itirazını inceleyen İstanbul Anadolu 1. Sulh Ceza Hakimliği’ne gönderilerek Hakimlik tarafından yeniden yargılama işlemlerinin başlatılması ve Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren yeni bir karar tesis edilmesi gerekecektir.

Karar ile, Kurul tarafından uygulanan idari para cezalarının gerekçelerinin hukuken gerekli ve yeterli bir şekilde açıklanmasının önemi vurgulanarak, verilen kararların ve bu kararlara itiraz süreçlerinin Anayasal haklara zeval vermeden bütünüyle ve detaylı olarak gerekçelendirmeleri gerektiği belirtilmiştir.

2. Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber Yayımlandı

Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber (“Genetik Veri Rehberi”), 13 Ekim 2023 tarihinde Kişisel Verileri Koruma Kurumu (“Kurum”) tarafından resmi internet sitesinde yayımlanmıştır. Söz konusu Genetik Veri Rehberi ile, Kanun’da özel nitelikli kişisel veri olarak kabul edilen genetik verilerin kullanım alanları ve işleme şartları, genetik veri sorumluları, ilgili kişiler ve yükümlülükleri, genetik veri güvenliği ve son olarak Kurum’un önerileri ve tavsiyeleri düzenlenmektedir.

Genetik Veri Rehberi kapsamında genetik veri, *canlıya ait genomdan, hücre çekirdeğinden ya da mitokondrisinden kodlanan tüm DNA, RNA ve protein diziliminden elde edilen bilgilerin tamamı ya da bir kısmı* olarak tanımlanmaktadır. Kanunun 6. maddesinde de kişilerin biyometrik ve genetik verileri, özel nitelikli kişisel veriler olarak nitelendirilmiştir. Bu doğrultuda, sağlık alanında yapılan genetik analizlerde kullanılan genetik verilerin işlenmesinde, veri sorumlularının Kanun’da öngörülen kişisel veri işleminin genel ilkeleri ışığında, ulaşılmak istenilen amaç için uygun ve gerekli olacak şekilde, doğru hukuki sebeplere dayalı olarak genetik veri işlemleri ve Kanun’a uygun şekilde yükümlülüklerini yerine getirmeleri gerekmektedir. Ayrıca, elverişlilik, gereklilik ve orantılılık ilkeleri kapsamında genetik verinin işlenmesiyle hedeflenen neticenin gerçekleşmesi için yalnızca söz konusu amacı gerçekleştirmeye yönelik verilerin işlenmesi, bu doğrultuda daha az miktar ve türde kişisel verinin işlenmesini sağlayan, en az müdahaleyi gerektiren araçlar/yöntemlerin kullanılması, yani veri minimizasyonu, önem arz etmektedir. Veri sorumlusu ayrıca, genetik verisi işlenen ilgili kişiye, genetik veri işleme faaliyetlerini ve sonuçlarını açık ve anlaşılır bir şekilde anlatmakla yükümlü olup, rıza kapsamının dışına çıkmamalıdır.

Öte yandan, genetik verilerin yurt dışına aktarımının söz konusu olabilmesi için, (i) ilgili kişinin açık rızası, (ii) açık rıza aranmayan durumlarda genetik verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunması (*yeterli koruma bulunan yabancı ülkelerin listesi henüz Kurum tarafından yayınlanmamıştır*); veya (iii) yeterli korumanın bulunmaması durumunda ise Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt ederek alacakları

Kurum izninden herhangi birinin bulunması gerekmektedir. Bununla birlikte Genetik Veri Rehberi, uluslararası sözleşme hükümleri saklı kalmak üzere, ilgili kişinin veya Türkiye'nin menfaatinin ciddi bir şekilde zarar görebileceği hallerde, ilgili kamu kurumunun görüşünün alınması kaydıyla, Kurul'un izniyle yurt dışına aktarım yapılabileceğini de belirtmektedir.

Veri sorumlularının, genetik verilerin hassasiyeti nedeniyle verilerin güvenliğini sağlamak amacıyla Kurul'un [2018/10 sayılı ve 31 Ocak 2018 tarihli Kararında](#) yer alan *Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemlerin* yanı sıra, Genetik Veri Rehberi'nde yer alan teknik ve idari tedbirleri alması tavsiye edilmektedir. Buna göre, genetik verilerin bulut sistemlerinden tutulması halinde, bulutta depolanan verilerin kaydı tutulmalı, bulut dışındaki yedekleri alınmalı ve uzaktan erişimi için iki kademli kimlik doğrulama kontrolü uygulanmalıdır. Ayrıca, kriptografik yöntemler ile şifrelenecek sistemlere erişim sadece yetki sahibi personel ile sınırlandırılmalıdır. Verilerin işlenmesi sırasında kullanılan cihazların bakım ve onarımı ile iadesi gibi durumlarda cihazlar ve sunucularda kişisel veri olmadığından emin olunup, cihaz sahibinden yazılı taahhütname alınmalıdır. Veri işleme sistemi sertifikalı cihazlar, güncel yazılımlar kullanılmalı, yama yönetimi sağlanmalı ve açık kaynak kodlu yazılımlar tercih edilmeli ve ilk olarak sentetik veriler kullanılarak test edilmelidir. Ayrıca, sistemlerin donanımsal ve yazılımsal güvenlik testleri periyodik olarak yapılmalıdır. Genetik veri mahremiyetinin tasarım aşamasından itibaren veri koruma kurallarına uygunluğu öngören "Mahremiyet Temelli Tasarım" (*Privacy by design*) ilkesi benimsenerek, bir yazılımın yapım aşamasından itibaren kişisel verilerin korunması kuralları ve gizliliğin göz önünde bulundurulması ve buna uygun sistemlerin entegre edilmesi gerekmektedir. Ayrıca genetik veriler, konu kapsamında yetkili ve bilgili ve kendisiyle gizlilik sözleşmesi akdedilmiş kişiler tarafından muhafaza edilmelidir. Genetik Veri Rehberi'nde yer verilen bu ilkelerin ve kriterlerin sağlandığı hususu ise veri sorumlusu tarafından kayıt altına alınıp belgelendirilmelidir ve kamuoyuna açıklanmalıdır.

3. Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler Yayımlandı

Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler ("**Tavsiye**"), 22 Aralık 2023 tarihinde Kişisel Verileri Koruma Kurumu tarafından resmi internet sitesinde yayımlanmıştır. Söz konusu Tavsiye ile, özellikle akıllı telefonlar ve tabletlerde kullanılan mobil uygulamalarda mahremiyetin korunmasına yönelik mevcut ve potansiyel riskler örnekler üzerinden ele alınarak, Kanun kapsamındaki genel ve özel nitelikli kişisel verilerin mobil uygulamalar aracılığıyla işlenmesi faaliyeti bakımından ilgili kişi ve veri sorumlusu niteliğini haiz aktörlere yönelik genel nitelikli tavsiyelerde bulunulmuştur.

Tavsiye, mobil uygulamalarda kişisel verilerin işlenmesi ve korunması süreçlerinde; uygulama sağlayıcısı, uygulama geliştiricisi, reklam ağı, uygulama mağazası kuruluşu, işletim sistemi sağlayıcısı, kütüphane sağlayıcısı ve cihaz üreticisi gibi birçok aktörün sorumlu olabileceğini belirtmiştir. Bu doğrultuda uygulamanın işlevselliğine, tasarımına ve kullanıcının verdiği izinlere göre değişkenlik gösterse de genel olarak mobil uygulamalar tarafından işlenen *kullanıcının kimlik bilgileri, üyelik bilgileri, iletişim bilgileri, finansal bilgiler, kullanıcı etkileşimleri, konum bilgisi, çevrimiçi tanımlayıcılar, telefon rehberi veya uygulamadaki arkadaş listeleri; özel nitelikteki kişisel verilere ise biyometrik veriler, sağlık verileri* gibi kişisel verilerin işlenmesinde bireylerin mahremiyetinin korunması ve uygulamalar üzerinden gerçekleştirilen veri işleme faaliyetinin Kanun'da belirtilen ilkelere uyumlu olması amacıyla hem uygulama kullanıcılarına hem de veri sorumlusu ve/veya veri işleyen olarak nitelendirilebilecek kişilere örnekler üzerinden tavsiyelerde bulunulmuştur.



⇒ Kullanıcılara Yönelik Tavsiyeler:

Tavsiye'ye göre söz konusu uygulamalar, güvenilir olduğu değerlendirilen AppStore veya GooglePlay gibi resmi uygulama mağazaları veya mobil uygulama sağlayıcısının resmi internet sitesi gibi kaynaklardan, uygulamanın geliştiricisi hakkında bilgi edinilerek ve uygulama adının doğruluğundan emin olunduktan sonra indirilmelidir. Her ne kadar yüksek uygulama puanı ve olumlu yorumlar bir uygulamanın mutlak surette güvenilir olacağını garanti etmese de uygulamanın işlevselliği ve güvenilirliği hakkında fikir edinmek adına uygulamaya yönelik yorum ve puanlar değerlendirilmelidir. İndirilecek uygulamanın özellikle gizlilik politikası gözden geçirilmeli, hangi verilere erişim izni istediği kontrol edilmelidir. Uygulama tarafından talep edilen konum, ses, görüntü vb. erişim izinlerde mahremiyetin korunmasına ilişkin endişe duyulması halinde erişim isteklerinin reddedilmesi ve gerekirse alternatif bir uygulama araştırılması gerekmektedir. Uygulamalarda kullanılacak şifreler oluşturulurken mümkün olduğunca güçlü kombinasyonlar tercih edilmeli, her hesap için farklı şifre oluşturulmalı ve çift faktörlü doğrulama etkin hale getirilmelidir. Ayrıca, uygulamanın sosyal ağ hesabından bilgi toplamasına yol açacağından, uygulamalara giriş yaparken sosyal medya hesaplarının kullanılmasından kaçınılmalıdır.

⇒ Kişisel Veri İşleyen Tarafra Yönelik Tavsiyeler:

Mobil uygulamaların geliştirilmesi, kullanıma sunulması ve ilgili kişiler tarafından kullanılması süreçlerinde kişisel veri işleme faaliyetinin Kanun'a uygun gerçekleştirilmesi gerekmektedir. Bu kapsamda kişisel veriler, hukuka ve dürüstlük kurallarına uygun bir şekilde, doğru ve güncel olarak belirli, açık ve meşru amaçlar çerçevesinde bu amaçlara bağlı, sınırlı ve ölçülü olacak şekilde işlenmeli; kanuni muhafaza sürelerine uygun olarak muhafaza edilmelidir. Bu kapsamda uygulama geliştiricileri ile sağlayıcılarının kişisel veri işleme faaliyetlerinde dürüst ve şeffaf olmaları ve bu doğrultuda aydınlatma yükümlülüğüne uygun olarak aydınlatma metni ve eğer ayrıca hazırlanmışsa gizlilik politikasına erişimi kolaylaştırılması, kullanıcıların hak ve menfaatlerini gözeterek gizlilik ayarları ve güncellemeler konusunda kullanıcı dostu ara yüz kullanılması tavsiye edilmiştir. Ayrıca, mobil uygulamalar aracılığıyla kişisel verileri işlemeye temel oluşturacak işleme koşullarının belirlenmesi ve gerekçeleri ile ortaya konulması elzemdir. Veri sorumlusu, veri işleme faaliyetinin gerçekleştirilmesinde öncelikle *açık rıza* dışındaki diğer veri işleme şartlarından birisine dayanılıp

dayanılmayacağı değerlendirilmeli, bunlardan herhangi birisi bulunmuyorsa kullanıcının *açık rızasının* alınmasını sağlamalıdır.

Tavsiye ayrıca yazılımların uygulamaya ve uygulamaya entegre üçüncü taraflara ayrı ayrı izin verme imkânı sağlamamasını bir sorun olarak dile getirmiş, kullanıcı izinlerinin alınırken uygulamada faydalanılan üçüncü taraf işlemlerine ilişkin şeffaf olunması ve uygulamaya entegre edilen üçüncü taraf hizmet aracılığıyla kişisel veri işlenmesinde hukuki bir sebep bulunmadığı takdirde bu hizmetin uygulamada kullanılmaması gerektiğini belirtmiştir.

Öte yandan, uygulamalarda güncelliğin sağlanması ve güncelliğini yitiren kişisel veriler yönünden kimlik hırsızlığının önüne geçilebilmesi adına kullanıcılara kişisel verilerin doğru ve güncel olması adına düzeltilmesi imkânı tanınması gerektiği vurgulanmıştır. Ayrıca, işlenen veriler, uygulamanın kullanılmasıyla belirlenen amaçların gerçekleştirilebilmesine elverişli olmalıdır. Burada önemli olan, veri minimizasyon ve ölçülülük ilkeleri çerçevesinde amacı gerçekleştirmeye yönelik mümkün olan en az çeşit ve sayıda kişisel veri toplanması ve amaç için gerekli olmayan veri işlemeden kaçınılmasıdır.

Son olarak veri güvenliğinin sağlanması konusunda Tavsiye, mobil uygulamaların veri koruma kurallarına uygunluğu öngören tasarımdan itibaren mahremiyet (*privacy by design*) ve başlangıçtan itibaren mahremiyet (*privacy by default*) ilkeleri ile uyumlu şekilde tasarlanmasını, uygulamaların kullandığı cihazlara yetkisiz erişimler gerçekleştirilmesini önlemek adına cihazlarda çok faktörlü kimlik doğrulama yöntemlerinin kullanılmasını, düzenli olarak yama yönetimi ve yazılım güncellemesi süreçlerinin gerçekleştirilmesini ve bot saldırılarına önlem olarak kullanıcı girişlerinde CAPTCHA gibi yöntemlere yer verilmesini, ve kişisel verilerin etkili bir şekilde depolanması ve aktarılmasında yeterli bir şifreleme katmanı ve ilgili şifreleme anahtarlarının güvenli yönetimi aracılığıyla şifrelenmesini tavsiye etmiştir.



4. Türkiye Cumhuriyeti Kimlik Numaralarının İşlenmesine İlişkin Rehber Yayımlandı

Kurum tarafından 16.01.2024 tarihinde Türkiye Cumhuriyeti Kimlik Numaralarının İşlenmesine İlişkin Rehber ("**TCKN Rehberi**") yayımlanmıştır. TCKN Rehberi'nin amacı, Türkiye Cumhuriyeti kimlik numarasının ("**TCKN**") işlenmesini öngören mevzuat hükümlerine dikkat çekmek ve TCKN işleme faaliyetlerinin Kanuna uygun olarak nasıl yürütüleceği konusunda veri sorumlularına yol göstermektir.

TCKN Rehberi'ne göre, TCKN'nin işlenmesinde özet olarak; (i) veri sahiplerinin kişisel verilerini koruma hakkına daha az müdahale eden yöntemlerin mümkün olup olmadığının değerlendirilmesi, (ii) veri işleme faaliyetinin hukuka uygun olarak gerçekleştirilmesi, (iii) veri sorumluları tarafından gerekli teknik ve idari tedbirlerin alınması ve (iv) TCKN'nin Kanun ve ikincil mevzuatına uygun olarak işlenmesinin sağlanması hususlarına dikkat edilmelidir. TCKN Rehberi'nde yer alan önemli hususlar aşağıda kısaca özetlenmiştir.

Öte yandan, TCKN Rehberi, TCKN'nin işlenmesinin öngörüldüğü durumlara ve ilgili mevzuat hükümlerine örnekler vermektedir. TCKN Rehberi'nde bu durumlara ve mevzuat hükümlerine ilişkin verilen örnekler aşağıdaki şekilde özetlenebilir:

- mal ve hizmet alışverişi için fatura düzenlenmesi,
- sipariş ve kargo teslimatı,
- esnaf tarafından ticari elektronik ileti gönderilmesi,
- ticaret siciline tescil ve sicil tasdiknamesi alınması,
- noterliklerde yürütülen yasal işlemler,
- davaların açılması,
- suç gelirlerinin aklanmasının önlenmesi,
- TCKN veya kimlik bilgilerini içeren belgelerin kimlik tespiti ve diğer amaçlarla yetkili makamlara sunulduğu, gösterildiği veya bildirildiği durumlar.

5. Seçim Faaliyetlerinde Kişisel Verilerin Korunması Rehberi Yayımlandı

Kurum tarafından 24.01.2024 tarihinde Seçim Faaliyetlerinde Kişisel Verilerin Korunması Rehberi ("**Seçim Rehberi**") yayımlanmıştır. Seçim Rehberi'nin amacı, seçim faaliyetlerinde yer alan kamu idarelerinin, siyasi partilerin, adayların ve seçmenlerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**") kapsamında yerine getirmesi gereken yükümlülükleri ve Kanun kapsamında sahip oldukları hakları hatırlatmaktır. Aşağıda Seçim Rehberi'nde öne çıkan hususların bir özeti görebilirsiniz:

- Seçim Rehberi'nde Yüksek Seçim Kurulu ("**YSK**"), siyasi partiler ve bağımsız adayların her birinin seçim faaliyetleri kapsamında yürüttükleri veri işleme faaliyetleri bakımından veri sorumlusu olarak kabul edildikleri belirtilmektedir.
- Kanun'un 28. maddesi uyarınca, seçimlerin yönetimi ve denetiminden sorumlu olan YSK'ya, veri sahiplerini aydınlatma yükümlülüğü, veri sahiplerinin hakları (zararların tazminini talep etme hakkı hariç) ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen hükümler uygulanmayacaktır. Öte yandan, siyasi partiler ve bağımsız adayların,

kişisel veri işleme faaliyetleri sırasında veri sahiplerini bilgilendirmek ve haklarını kullanmalarını sağlamakla yükümlü oldukları vurgulanmaktadır.

- Kanun'un 8. maddesinin 3. fıkrasında düzenlenen "Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükmü nedeniyle engellilik verileri gibi sağlık verilerini de içeren özel nitelikli kişisel verilerin, 7062 sayılı Kanun'un 6. maddesi ile 298 sayılı Kanun'un 36. ve 74. maddeleri örnek gösterilerek YSK tarafından ilgili kişilerin açık rızası alınmaksızın aktarılabileceği belirtilmiştir.
- Siyasi partilerin üyelerine sesli, görüntülü veya yazılı mesaj göndermek amacıyla iletişim verilerini işleyebilecekleri; ancak vatandaşların e-posta adreslerine mesaj göndererek veya telefonlarına sesli, görüntülü veya yazılı mesaj göndererek propaganda yapmalarının mümkün olmayacağı belirtilmektedir.
- Seçim Rehberi'nde bağımsız adayların vatandaşlara sesli, görüntülü veya yazılı mesaj göndermemeleri ve bu amaçla vatandaşların kişisel verilerini işlememeleri gerektiği vurgulanıyor.

6. Kurul Tarafından Yayınlanan Kararlar

⇒ Karar No: 2023/567

Konu: Bir e-ticaret sitesinden alışveriş yapılabilmesi için kredi/banka kartı bilgilerinin kaydedilmesinin zorunlu tutulması hakkında

Değerlendirme: Bir online alışveriş platformunda kredi kartının veya banka kartının herhangi bir sisteme kaydedilmesi ve saklanması zorunlu tutulamayacak olup, bu kayıt işlemi ancak ilgili kişinin özgür iradesi zedelenmeden açık rızasıyla yapılabilecektir.

⇒ Karar No: 2023/695

Konu: Özel bir tıp merkezi tarafından ilgili kişinin e-nabız sistemindeki verilerine hukuka aykırı erişilmesi

Değerlendirme: Çalışanların kendi takdirleriyle gerçekleştirdikleri kanuna aykırı veri işleme faaliyetlerinin veri sorumlusunun bünyesinde gerçekleşmesi halinde, veri sorumlusu bu aykırılıktan sorumlu olacaktır.

⇒ Karar No: 2023/845

Konu: Bir kargo şirketi çalışanı tarafından kargo teslimi akabinde ilgili kişinin telefonuna kısa mesaj gönderilmesi suretiyle kişisel verilerin hukuka aykırı işlenmesi

Değerlendirme: Alt-işverenlik veya benzeri bir ilişkiyle veri sorumlusu adına çalışan tüm kişilere, veri sorumlusu tarafından kişisel verilerin korunması eğitimi sağlanması gerekmektedir. İdari tedbirler kapsamında değerlendirilen bu yükümlülük veri sorumlusunun kendi çalışanları ile sınırlandırılmamıştır.



⇒ Karar No: 2023/924

Konu: Otopark işletmecisi veri sorumlusu tarafından ilgili kişinin kişisel verilerinin hukuka aykırı işlenmesi ve aydınlatma yükümlülüğünün yerine getirilmemesi

Değerlendirme: Kararda, delil olarak sunulmak üzere kişisel verilerin işlenmesinin mümkün olduğuna yer verilmektedir.

Ancak ilgili kişilere bu hususta aydınlatma yapılması gerektiği veri sorumlularınca unutulmamalıdır. Aksi takdirde kararda olduğu üzere veri işleme faaliyeti hukuka uygun olsa dahi aydınlatma yükümlülüğü yerine getirilmediğinden veri sorumlularına ceza uygulanabilecektir.

⇒ Karar No: 2023/1041

Konu: Veri sorumlusunun internet sitesinde aydınlatma yükümlülüğünü usulüne uygun olarak yerine getirmemesi ve sunduğu hizmeti açık rıza şartına bağlaması hakkında

Değerlendirme: Kararda, kullanıcılara alternatif satış kanalları sunulması halinde internet üzerinden yapılan satışlarda yurt dışına veri aktarımının açık rıza verilmesi şartına bağlanmasının mümkün olduğuna yer verilmiştir.

⇒ **Karar No: 2023/1130**

Konu: İlgili kişinin rapor ve ilaç kayıtlarının eczane tarafından eski eşi ile paylaşılması

Değerlendirme: Kurul karar kapsamındaki değerlendirmesinde, Medula sisteminin kurulmasından ve yönetilmesinden Sağlık Bakanlığının sorumlu olması nedeniyle eczacıların bu sisteme girilen veriler açısından veri işleyen olduğunu tespit etmiştir. Buna karşılık karara konu olayda, eczacının Medula'ya bilgi girişi yapmanın ötesine geçmesi (ilgili kişinin rapor ve ilaç listesinin çıktısını alıp üçüncü kişi ile paylaşması) nedeniyle eczacı veri sorumlusu olarak değerlendirilmiştir. Bu doğrultuda, veri işleyenlerin, veri sorumlusu tarafından verilen talimatları aşması halinde ayrı bir veri sorumlusu haline geldiklerine yer verilmektedir.

⇒ **Karar No: 2023/1234**

Konu: Bir Araç kiralama şirketi tarafından ilgili kişiden Findeks raporu talep edilmesi suretiyle kişisel verilerinin işlenmesi

Değerlendirme: Aracı hizmet sağlayıcı olarak hareket eden e-pazaryerlerinin, münhasıran satıcılar tarafından gerçekleştirilen işleme faaliyetleri yönünden veri sorumlusu sıfatı bulunmamaktadır. Açık rızaya tabi olarak talep edilen Findeks raporlarının verilmesi hizmetin sunulması şartı yapılması, açık rızanın özgür iradeye dayanması koşulu ile çeliştiğinden bu açık rıza geçersiz olarak kabul edilecektir.

⇒ **Karar No: 2023/1309**

Konu: Bir havayolu şirketi tarafından ilgili kişiye ait kişisel verilerin hukuka aykırı olarak üçüncü kişilerle paylaşılması

Değerlendirme: Kararda veri sorumlusu tarafından ilgili kişi başvurusu kapsamında dahi veri ihlali meydana geldiği öğrenilir ise derhal veri ihlal bildiriminde bulunulması gerektiğine yer verilmiştir.

```
40 .myphoto{
41   width: 500px;
42   margin-top: 15%;
43   clip-path: polygon(25% 0%, 100% 0%, 75% 100%, 0% 100%);
44 }
45 .myphoto2{
46   display: none;
47 }
48 .intro{
49   font-weight: 600;
50   font-family: Montserrat, Sans;
51   line-height: 2.2;
52   font-size: 70%;
53   /* margin-right: 50px; */
54 }
55 .intro1{
56   padding-top: 10px;
57   padding-bottom: 10px;
58   font-size: 157%;
59   color: #65159e;
60 }
61 .intro2{
62   margin-top: 20px;
63   margin-bottom: 20px;
64   font-size: 90%;
65 }
```

⇒ **Karar No: 2023/1310**

Konu: Banka mobil uygulamasında dijital parola belirlerken yüz verisinin işlenmesi suretiyle kişisel verilerin işlenmesi

Değerlendirme: Karar kapsamında kimlik doğrulama gibi meşru bir nedenin varlığı halinde mobil bankacılıkta biyometrik verilerin açık rıza alınarak işlenebileceği belirtilmiştir.

⇒ **Karar No: 2023/1321**

Konu: İlgili kişinin e-posta verilerinin, önceden ortağı olduğu veri sorumlusu şirket tarafından işlenmeye devam edilmesi

Değerlendirme: Çalışanlar ya da eski ortaklara ait e-posta hesaplarının kullanıcılarının yani ilgili kişilerin işten ayrılmalardan diğer bir deyişle veri sorumlusu ile ilişkilerinin sona ermesini müteakip yeni e-posta almayacak şekilde ayarlanması yani kapatılması gereklidir.

⇒ **Karar No: 2023/ 1356**

Konu: Bir işveren tarafından işe iade davasında, ilgili kişinin mescitte ibadet etme görüntülerinin ibraz edilmesi

Değerlendirme: Kararda belli amaçlarla işyerinde kamera kaydı yapılması mümkün olduğuna yer verilmektedir. Ancak kararda belirtildiği üzere kayıt yapılan alanların belirlenmesinde kişilerin mahremiyet beklentileri de göz önünde bulundurulmalı, mescit, dinlenme odaları gibi alanlarda kamera kaydı yapılmamalıdır. Nitekim bu ölçüleri aşarak elde edilen ve mahkemelere sunulan deliller hukuka aykırı kabul edilmeli ve delil niteliğini haiz olmamalıdır.

⇒ **Karar No: 2023/1414**

Konu: İlgili kişiye ait özel nitelikli kişisel verilerin avukat tarafından mahkemeye aktarılması

Değerlendirme: Kararda DNA testi sonuçlarının birden fazla kişinin ortak verisi olması sebebiyle bu ortak veriyi haiz her bir kişi tarafından kullanılabilmesine yer vermiştir. Nitekim Hukuk Muhakemeleri Kanunu, özel nitelikli kişisel verilerin mahkemelere delil olarak sunulmasına hususunda kanuni bir temel teşkil edebilecek olup, kişisel veriler mahkemelere delil olarak sunulurken bir hakkın tesisi/korunması ve kullanılması hukuki sebebine dayanılabilecektir.

⇒ **Karar No: 2023/1461**

Konu: Ses kayıt özelliği bulunan güvenlik kamerası kullanılması

Değerlendirme: Kararda güvenlik kameralarıyla görüntü kaydı alınması ve işlenmesi hukuka uygun kabul edilirken ses kaydı alınması ve işlenmesi istisnai durumlar hariç olmak üzere hukuka aykırı olarak kabul edilmektedir.

⇒ **Karar No: 2023/1465**

Konu: Veri sorumlusuna ait internet sitesinde yapılan kullanıcı girişinde üçüncü kişiye ait kişisel verilerin görüntülenmesi

Değerlendirme: Karara konu olayda, araç kiralama şirketine ait internet sitesine kendi kullanıcı adı ve e-posta adresi ile giriş yapan kullanıcının, sistemsel bir hata nedeniyle bir başka kullanıcının hesabına yönlendirildiği anlaşılmaktadır. Nitekim Kurul karar kapsamındaki değerlendirmesinde yalnızca bu verilerin görüntülenebilir olmasının dahi bir veri işleme faaliyeti olarak değerlendirilmesi sebebiyle, söz konusu teknik hatadan dört kişinin verilerinin etkilenmiş olmasına rağmen bir veri ihlal bildiriminde bulunulmamış olduğunu, yetkisiz erişim sağlayan kişinin ihbarı neticesinde re'sen inceleme başlatıldığını, ihbarda bulunabilmek için ihbar edenin kendi kişisel verilerinin olaydan etkilenmesine gerek olmadığını, yapılan inceleme neticesinde veri sorumlusunun gerekli güvenlik önlemlerini almadığının anlaşıldığını ve bu yetkisiz erişim nedeniyle veri ihlal bildiriminde bulunulmuş olması gerektiğini belirtmiştir.

Sonuç olarak, veri ihlalinden tek bir ilgili kişinin etkilenmesi bile veri ihlal bildirimi yapma zarureti doğurmaktadır.

⇒ **Karar No: 2023/1548**

Konu: İlgili kişinin açık rızası alınmadan ses kaydının alınması, paylaşılması ve mahkeme dosyasına sunulması

Değerlendirme: Kararda belirli durumlarda ses kaydının, işçi-işveren arasında görülen davalarda delil olarak kullanılabilmesine yer verilmektedir. Yargıtay'ın yerleşmiş içtihatları doğrultusunda söz konusu durumlar, işverenin iş sözleşmesini haklı nedenle feshini başka türlü delil ile ispat etme imkânı olmaması ya da kaybolma ihtimali bulunan kanıtların kaybolmasının engellenmesidir. Bu gibi durumlarda veri sorumlusu işveren, bir hakkın tesisi/korunması ve kullanılması hukuki sebebine dayanabilecektir.

⇒ **Karar No: 2023/1578**

Konu: İlgili kişinin hasta dosyasında yer alan özel nitelikli kişisel verilerinin mahkemeye aktarılması

Değerlendirme: Kararda mahkemelerden gelen müzakerelerde belirtilen kapsamda cevaplayan ve belge sunan veri sorumlularının hukuka uygun hareket ettiklerine yer verilmektedir.

7. Kanun Kapsamında 2024 Yılında Uygulanacak İdari Para Cezaları

Yükümlülükler	2024 Alt Sınır (TL)	2024 Üst Sınır (TL)
Aydınlatma Yükümlülüğü İhlali	47.303₺	946.308₺
Veri Yükümlülüğü İhlali	141.934₺	9.463.213₺
Kurul Kararını Yerine Getirmeme	263.557₺	9.463.213₺
VERBİS Kayıt ve Bildirim Yükümlülüğü İhlali	189.245₺	9.463.213₺

Herhangi bir sorunuz olması halinde bizlerle her zaman iletişime geçebilirsiniz.

İletişim

Burçak Kurt Biçer
Yönetici Ortak

burcak.bicer@bicerguner.com

Uğurkan Şeber
Kıdemli Avukat

ugurkan.seber@bicerguner.com

İrem Efe
Avukat

irem.efe@bicerguner.com