GIDE
GIDE LOYRETTE NOUEL

ÖZDİREKCAN DÜNDAR ŞENOCAK AK
AVUKATLIK ORTAKLIĞI

NEWSLETTER

DATA PROTECTION | TURKEY | MARCH 2022

UPDATE ON MAJOR DEVELOPMENTS IN Q1 2022

This Data Protection Newsletter provides information on the latest developments as regards personal data protection and implementation of the Law No.6698 on the Protection of Personal Data (the "**Law**") in the light of recent publications and announcements by the Personal Data Protection Authority (the "**Authority**"), decisions of the Board, as well as main headings from "Wednesday seminars" organised by the Authority.

RECENT ANNOUNCEMENTS

Below is the list of all publications and announcements made by the Authority in the last quarter:

December 2021	
6 December	Communiqué on Procedures and Principles Regarding the Personnel Certification Mechanism[1]
7 December	Announcement on Personal Data Breaches within the scope of the Turkish Criminal Code on Employment Promises[2]
7 December	Announcement of Data Protection Officer Certification Program[3]
10 December	Announcement on Data Protection Officers[4]
17 December	Announcement on Processing of Personal Data by Sending a Verification Code via SMS During In-store Shopping[5]
17-27 December	33 decisions of the Board taken during the period from January to September 2021[6][7]

[1] https://kvkk.gov.tr/Icerik/7091/PERSONEL-SERTIFIKASYON-MEKANIZMASINA-ILISKIN-USUL-VE-ESASLAR-HAKKINDA-TEBLIG

[2] https://kvkk.gov.tr/Icerik/7095/IS-VAADI-KONULU-TCK-KAPSAMINDAKI-KISISEL-VERI-IHLALLERINE-ILISKIN-KAMUOYU-DUYURUSU

[3] https://kvkk.gov.tr/Icerik/7093/Kamuoyu-Duyurusu-Sertifikasyon-

[4] https://kvkk.gov.tr/Icerik/7100/Veri-Koruma-Gorevlisi-Hakkinda-Kamuoyu-Duyurusu

[5] https://kvkk.gov.tr/Icerik/7104/MAGAZALARDA-ALISVERIS-SIRASINDA-ILGILI-KISILERE-SMS-ILE-DOGRULAMA-KODU-GONDERILMESI-SURETIYLE-KISISEL-VERILERIN-ISLENMESINE-ILISKIN-KAMUOYU-DUYURUSU

[6] https://kvkk.gov.tr/Icerik/7124/Kisisel-Verileri-Koruma-Kurulu-nun-Yeni-Yayinlanan-Karar-Ozetleri

[7] https://kvkk.gov.tr/Icerik/7145/Kisisel-Verileri-Koruma-Kurulu-nun-Yeni-Yayimlanan-Karar-Ozetleri

January 2022	
3 January	New issue of the Personal Data Protection Magazine[89]
3 January	2nd guidelines regarding common misconceptions held about the Law[10]
4 January	Announcement regarding registrations to the Data Controllers' Registry Information System[11]
11 January	Draft guidelines on the use of cookies[12]
18 January	Approval by the Board of application for "Undertaking" of the Turkish Football Federation regarding its cross-border data transfers[13]
20 January	New principle decision of the Board regarding "blacklisting operations" in the car rental industry[14]
February 2022	
11 February	Announcements of Principles and Procedures Regarding Issuance of Personnel Certificates[15]
15 February	Announcement on Technical and Organizational Measures Suggested to be Taken by the Data Controllers regarding Users' Data Security[16]
17 February	Announcement on Amounts of Monetary Fines Applicable For 2022[17]
18 February	Publication of 7 principle decisions of the Board[18]

MAIN HIGHLIGHTS

Data Protection Officer

The Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism (the "**Communiqué**") regarding the Data Protection Officer Programme (the "**Programme**") was published in the Official Gazette numbered 31681 and dated 6 December 2021. The Communiqué introduces for the first time the concept of data protection officer, and regulates procedures and principles regarding the training, examination and certification of individuals within the Programme in accordance with the (TS) EN ISO/IEC 17024 standard.

[8] Topics: The Position of the Right to Be Forgotten Against Freedom of Press; Change of Purpose in Data Processing: The Question of Compatibility Criteria; Judicial Remedies Against Sanctions Stipulated Under Data Protection Law: A Comparative Review; Comparative Review of Brazilian Data Protection Law with Personal Data Protection Law No. 6698.

[9] https://kvkk.gov.tr/Icerik/7154/Kisisel-Verileri-Koruma-Dergisi-nin-Yeni-Sayisi-Yayimlandi

[10] https://kvkk.gov.tr/SharedFolderServer/CMSFiles/d077b665-66b6-4615-975a-249f93e084ba.pdf

[11] https://kvkk.gov.tr/Icerik/7156/Veri-Sorumlulari-Siciline-Kayit-Hakkinda-Kamuoyu-Duyurusu

[12] https://kvkk.gov.tr/SharedFolderServer/CMSFiles/1336263f-22bb-4da3-a1b9-aabc0e0e8bff.pdf

[13] https://kvkk.gov.tr/Icerik/7161/Taahhutname-Basvurusu-Hakkinda-Duyuru

[14] https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf

[15] https://kvkk.gov.tr/Icerik/7176/Katilim-Belgesinin-Verilmesine-Dair-Usul-ve-Esaslar

[16] https://kvkk.gov.tr/Icerik/7177/Kullanici-Guvenligine-Iliskin-Veri-Sorumlulari-Tarafindan-Alinmasi-Tavsiye-Edilen-Teknik-ve-Idari-Tedbirlere-Iliskin-Kamuoyu-Duyurusu

[17] https://kvkk.gov.tr/Icerik/7181/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Idari-Para-Cezasi-Tutarlari

[18] https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7a2f2dc1-b656-4325-9249-73e350c3ea57.pdf

The Communiqué defines the data protection officer as a "natural person who has successfully passed the exam and is thus entitled to use the title of data protection officer", and who has sufficient knowledge of personal data protection legislation as part of their certification programme. Individuals who meet the training/certification requirements will be entitled to take the exam. The individuals who successfully pass the exam become data protection officers. The data protection officer certification is valid for four years.

The Communiqué states that the appointment of a data protection officer by the data controller and/or data processor shall not prejudice or remove their legal obligations.

Unlike GDPR, the Communiqué does not stipulate the duties or the authority of the data protection officer, neither does it impose an obligation for data controllers to appoint a data protection officer. Accordingly, the Authority has clarified in its announcement dated 10 December 2021 that the data protection officer in Turkish legislation differs from data protection officer under the GDPR.

Personal Data Breaches via Employment Promises

In its announcement dated 7 December 2021, the Authority stated that there had been an increase in the number of complaints by job applicants, due to requests for sending in pictures of their ID cards and for making payments for job applications available on social media and other online platforms.

The Authority declared that such fraudulent activities on employment promises fell within the scope of the Turkish Criminal Code and shall therefore constitute an offense thereunder. Concerned parties shall resort to the judiciary in order to establish the necessary legal proceedings regarding the issue.

Data Processing During In-Store Shopping

In its announcement dated 17 December 2021, based on the complaints and notices received, the Authority accounted for use of verification codes via SMS during in-store shopping as an explicit consent for receiving commercial electronic messages. In this respect, the Authority underlined that:

- the purpose of the SMS and the consequences of the code exchange via SMS must be explained by the shop staff to the customer before sending the SMS, and the SMS must provide the necessary access to a privacy notice;
- instead of obtaining consent through a single action, such as sending an SMS verification code, for more than one processing activity, such as personal data processing permission and approval for sending commercial electronic messages during shopping in stores, explicit consent must be obtained separately and with an option for each data processing activity;
- explicit consent shall not be obtained within the privacy notice;
- explicit consent for the sending of commercial electronic messages must be obtained for a specific subject, based on informed and free will.

Announcement Regarding VERBIS Registrations

In its announcement dated 4 January 2022, the Authority recalled the following regarding registration of the data controllers to the Data Controllers Registry Information System ("**VERBIS**"):

- The sole submission of the VERBIS registration application form via the online system or sending it to the Authority by mail, cargo, courier, registered email or hand delivery shall not suffice to meet the obligation of registration and notification to VERBIS. The required registration steps indeed consist of (i) submission of the VERBIS registration application form to the Authority; (ii) appointment of a “contact person” through VERBIS; (iii)

logging in of the contact person to VERBIS; (iv) issuance of the notification for the data controller; and (v) approval of the notification through the system.

- Incomplete applications and notifications must be completed as explained above in the shortest possible time. In case registered information in VERBIS changes, it should be notified to the Authority via VERBIS within seven days as of the date such change occurs.

Draft Guidelines on the Use of Cookies

The Draft Guidelines on the use of cookies published on 11 January 2022 (the "**Draft Guidelines**") make recommendations to website operators processing personal data through cookies in order to provide a better understanding of the use of cookies and to ensure their compliance with the Law.

The scope of the Draft Guidelines covers the cookies used only for processing personal data on online platforms such as websites and online applications, and 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*". It categorises cookies mainly under three groups based on (i) timeframe (*i.e.* session cookies, permanent cookies), (ii) purpose (*i.e.* mandatory cookies, functional cookies, performance-analytical cookies, advertising/marketing cookies), and (iii) parties (*i.e.* first party cookies, third party cookies).

The Draft Guidelines point out the relationship between Law No. 5809 on Electronic Communications (the "**ECL**") and the Law. As there is no provision in the Law that expressly regulates cookies, it is considered that in terms of data controller operators, the provisions of the ECL would be applied. Furthermore, it is stated that by taking into consideration the decision dated 27 February 2020 and numbered 2020/173 regarding information company services, the Law would be applicable due to the fact that unlike the EU Directive 2002/58/EC, the ECL does not regulate the processing of personal data through cookies.

Lastly, the Draft Guidelines explain when explicit consent must be obtained for the use of cookies by referring to EU practice. Accordingly, the following questions should be answered: either “are cookies used only for providing communication over an electronic communication network?” or “are cookies strictly necessary for the information company services that are explicitly requested by the subscriber or user?”. If the answer is negative, either the explicit consent of the data subject must be obtained, or another legal basis stipulated under the Law must be used.

Common Misconceptions About the Law

On 3 January 2022, the Authority published its second document aiming to clarify common misconceptions about the law by answering 64 questions. Topics include (i) conditions of data processing, (ii) explicit consent for data processing, (iii) use of opt-in and opt-out options, (iv) biometric data, (v) conditions of cross-border data transfers, (vi) fulfilment of the obligation to inform, and (vii) necessary steps to be taken in the event of a data breach.

Measures Regarding Security of Users' Data

In its announcement dated 15 February 2022, the Authority suggested to data controllers, especially those carrying out activities in finance, e-commerce, social media and game sectors, that they take some technical and organisational measures to the extent possible to ensure the security of their users' personal data. Some of these measures may include:

- establishing two-factor authentication systems;
- sending login information to the data subjects’ contact addresses via email or text message, in cases where users log in to their accounts from different devices;

- using HTTPS (Hypertext Transfer Protocol Secure) or another tool with the same security level, using secure and up-to-date hashing algorithms to protect user passwords against cyber-attacks;
- limiting the number of unsuccessful login attempts from an IP address;
- ensuring that data subjects can view information about at least 5 successful and unsuccessful login attempts;
- reminding data subjects that the same password should not be used on more than one platform;
- creating a password policy and ensuring that passwords are changed periodically, or reminding data subjects to do so, and preventing new passwords from being the same as old passwords (at least the last 3 passwords);
- using technologies such as security codes (CAPTCHA, four operations, etc.) that distinguish between computer and human behaviour during login and limiting IP addresses that may be used for access;
- ensuring that passwords entered into the systems contain at least 10 characters, uppercase and lowercase letters, numbers and special characters;
- updating and controlling systems regularly if third party software or services are being used to log in to the systems.

Monetary Fines Applicable in 2022

Explanation	MONETARY FINES FOR 2022 (TRY)	
Failure to comply with obligation to inform	13,391	267,883
Failure to comply with obligations related to data security	40,179	2,678,863
Failure to comply with any decision issued by the Board	66,965	2,678,863
Failure to comply with obligation to register and obligation to report to the VERBIS	53,572	2,678,863

Highlights from Key Decisions of the Board

- **Blacklisting in the car rental industry:** In its principal decision dated 23 December 2021 and numbered 2021/1304, the Board assessed the privacy violations from blacklisting operations of car rental companies. It concluded that car rental companies having control over data concerned and software companies shall qualify as "joint controllers" for the blacklisting operations conducted in violation of the provisions of the Law. The Board also states in its decision that, although processing of data for the purpose of blacklisting operations could be assessed within "legitimate interest" of the data controller, such interest must only belong to the data controller itself and blacklisting records must remain within the company. Therefore, transfer of such list to third parties would breach fundamental rights and freedoms.

- **Yemeksepeti data breach notification**: In decision numbered 2021/1324 and dated 23 December 2021, the Board decided to impose TRY 1,900,000 administrative fine on Yemeksepeti because of the breach of Article 12 (1) of the Law. The Board ruled that the data controller had not taken the necessary technical and administrative measures to ensure data security, and caused the leak of 21,504,083 user data abroad.

- **Sending commercial electronic messages by dealers and sub-contractors:** In decision numbered 2021/1210 and dated 2 December 2021, the Board decided to instruct the satellite TV provider (Digiturk) to pay due attention and care to comply with the Law in the process of acquiring new customers, even though it is not considered as data controller in the matter at hand. It should also include explicit provisions regarding the identities of the data controller and data processor in its commercial contracts with dealers.

Highlights From Seminars and Events

- The seminar on "**Misdemeanours in the Law on the Protection of Personal Data within the Framework of the General Provisions of the Misdemeanour Law**" held on 1 December 2021, explained that when determining the amount of an administrative fine in the event of data breach, the Board considers three criteria: the unfairness of the misdemeanour, the fault and the economic situation of the perpetrator. With respect to the relationship in between the Law and the Misdemeanour Law, it should be noted that the Law is considered lex specialis *vis-à-vis* the Misdemeanour Law and therefore, exceptional provisions regarding misdemeanours in the Law find application. However, since there is no specific regulation regarding remedies in the Law, the remedies regulated in the Misdemeanour Law will also find application in terms of the Law.

- The seminar on "**Process of Compliance with the Law on the Protection of Personal Data and VERBIS**" held on 15 December 2021 advised data controllers to establish a personal data protection compliance team or commission within the entity/enterprise that must be attentive when preparing the personal data processing inventory and to properly analyse personal data processing procedures.

- The seminar on "**Assessments Regarding the Crimes in the Field of Protection of Personal Data in accordance with the Law on the Protection of Personal Data and the Court of Cassation Decisions**" held on 29 December 2021, stated that before the enforcement of the Law, the Court of Cassation defined personal data as data that "cannot be accessed by everyone". It later came to the conclusion that all data about a natural person should be considered as personal data in accordance with Article 135 of the Turkish Criminal Code. In the post-Law period however, while classifying personal data, the Court of Cassation is of the opinion that an assessment should be made within the scope of Article 134 of the Turkish Criminal Code when the data is related to private life, and an evaluation should be made within the scope of Articles 135 and 136 when the data is outside of private life.

- The seminar on "**Protection of Personal Data on Social Media**" held on 12 January 2022 discussed effective tools and methods to protect personal data such as end-to-end encryption, two-factor authentication, and highlighted issues that should be considered when sharing data on social media.

- The seminar on "**Protection of Personal Data in the Field of Artificial Intelligence**" organized as part of the 28 January Data Protection Day Events, gave advised for the protection of personal data for developers, manufacturers, service providers and decision-makers operating in the field of artificial intelligence (AI).

◆ ❖ ◆

In compliance with Turkish bar regulations, opinions relating to Turkish law matters that are included in this client alert have been issued by Özdirekcan Dündar Şenocak Ak Avukatlık Ortaklığı, a Turkish law firm acting as correspondent firm of Gide Loyrette Nouel in Turkey.

CONTACTS

ARPAT ŞENOCAK
senocak@odsavukatlik.com

PINAR VEZIROĞLU DILEK
veziroglu@odsavukatlik.com