

KVKK
M. 12/5
21 EKİM 2026
BİLGİ NOTU

KVKK Ekim 2026 (II): 21 Ekim Veri İhlali Bildirimleri

PDP Board October 2026 (II): Data Breach Notifications of 21 October

UĞURCAN TEKİN · ORTAK / PARTNER · İNCİ ÖZÇİLSAL · AVUKAT / ATTORNEY AT LAW · BEYZA ERDEMİR · AVUKAT / ATTORNEY AT LAW

Bu bilgi notunda, Kişisel Verileri Koruma Kurulunun 21 Ekim 2026 tarihli kararlarıyla Kişisel Verileri Koruma Kurumunun internet sitesinde ilan edilmesine karar verilen on veri ihlali bildirimi aktarılmaktadır. İlanların tamamı 21 Ekim 2026 tarihinde Kurumun internet sitesinde yayımlanmıştır. Not, 19 Ekim 2026 – 25 Ekim 2026 tarihleri arasında Kurumun internet sitesinde yayımlanan duyuruları kapsamaktadır; bu dönemde yeni bir Kurul karar özeti, ilke kararı veya rehber yayımlanmamıştır.

Kurul, 21 Ekim 2026 tarihli kararlarıyla on veri ihlali bildirimini ilan etmiştir; üç bildirimde ihlal veri işleyen sistemlerindeki üçüncü taraf yazılım kütüphanesi zafiyetine, ikisinde fidye yazılımı saldırısına dayandırılmıştır.

GİRİŞ · INTRODUCTION

Kurul, 21 Ekim 2026 tarihinde on veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar vermiştir. Bildirimlerin üçünde ihlalin, veri sorumlusuna ait verilerin bulunduğu veri işleyen sistemlerindeki bir sunucuya, kullanılan üçüncü taraf yazılım kütüphanesindeki güvenlik zafiyetinin istismar edilmesi suretiyle yetkisiz erişim sağlanması sonucunda gerçekleştiği belirtilmiştir. İki bildirimde fidye yazılımı saldırısı, iki bildirimde sosyal mühendislik yöntemiyle çalışan hesaplarına yetkisiz erişim, bir bildirimde ele geçirilmiş parola ile kurumsal e-posta hesabına erişim, bir bildirimde yazılımdaki güvenlik açıklarından yararlanılarak yetkisiz erişim bildirilmiştir. Bir bildirimde ise otel işletmesinin bilgi işlem altyapısına ve kurumsal e-posta hesaplarına yönelik siber güvenlik olaylarının incelenmekte olduğu ifade edilmiştir.

İlan edilen bildirimler arasında Ankara’da faaliyet gösteren özel bir sağlık kuruluşunun muayene, tahlil, tanı ve tedavi kayıtlarını içeren sunucusunun şifrelenmesine ilişkin bildirim, İzmir Büyükşehir Belediyesi ve Ondokuz Mayıs Üniversitesi gibi kamu kurumlarının bildirimleri ile Choice Hotels International, Inc. ve Baxter Turkey Renal Hizmetler AŞ gibi uluslararası grup şirketlerinin bildirimleri yer almaktadır. Etkilenen ilgili kişi sayısı beş bildirimde rakam olarak belirtilmiş, diğer bildirimlerde sayının henüz tespit edilemediği ifade edilmiştir. İlanların tamamında konuya ilişkin incelemenin devam ettiği belirtilmiş; ilan kararlarında ihlale ilişkin bir yaptırıma yer verilmemiştir.

This legal update reports ten data breach notifications which the Personal Data Protection Board (“the Board”) decided, by its decisions dated 21 October 2026, to publish on the website of the Personal Data Protection Authority (“the Authority”). All of the notices were published on the Authority’s website on 21 October 2026. The update covers announcements published on the Authority’s website between 19 October 2026 and 25 October 2026; no new Board decision summary, resolution of principle or guide was published during this period.

By decisions dated 21 October 2026, the Board published ten data breach notifications; three attribute the breach to a third-party software library vulnerability in data processor systems and two to a ransomware attack.

On 21 October 2026, the Board decided to publish ten data breach notifications on the Authority’s website. Three of the notifications state that the breach occurred as a result of unauthorised access being gained to a server in the data processor’s systems holding the data controller’s data, by exploiting a security vulnerability in a third-party software library in use. Two notifications report a ransomware attack, two report unauthorised access to employee accounts by means of social engineering, one reports access to a corporate e-mail account by means of a compromised password, and one reports unauthorised access through the exploitation of a security vulnerability in software. One notification states that cyber security incidents directed at a hotel undertaking’s information technology infrastructure and corporate e-mail accounts are under examination.

The published notifications include a notification concerning the encryption of a server holding the examination, test, diagnosis and treatment records of a private healthcare institution operating in Ankara, notifications by public bodies such as İzmir Büyükşehir Belediyesi and Ondokuz Mayıs Üniversitesi, and notifications by international group companies such as Choice Hotels International, Inc. and Baxter Turkey Renal Hizmetler AŞ. The number of affected data subjects is stated as a figure in five notifications, while the other notifications state that the number has not yet been determined. All of the notices state that the examination of the matter is ongoing; the publication decisions do not include any sanction in respect of the breaches.

01

Veri İşleyen Sistemlerindeki Üçüncü Taraf Yazılım Kütüphanesi Zafiyetine Dayanan Üç Bildirim

Three Notifications Based on a Third-Party Software Library Vulnerability in Data Processor Systems

Kurulun 21.10.2026 tarihli ve 2026/2281 sayılı kararıyla Dermojet Sağlık Ürünleri Sanayi ve Ticaret Anonim Şirketi, Güllüoğlu Gıda San. ve Tic. AŞ ve Kurukahveci

By the Board’s decision No. 2026/2281 dated 21 October 2026, the notifications of Dermojet Sağlık Ürünleri Sanayi ve Ticaret Anonim Şirketi, Güllüoğlu Gıda San. ve

Mehmet Efendi Mahdumları Gıda Sanayi ve Ticaret Anonim Şirketi bildirimleri ilan edilmiştir. Üç bildirimde de ihlalin, veri sorumlusuna ait verilerin bulunduğu veri işleyen sistemlerindeki bir sunucuya, kullanılan üçüncü taraf yazılım kütüphanesindeki güvenlik zafiyetinin istismar edilmesi suretiyle yetkisiz erişim sağlanması sonucunda gerçekleştiği ve ihlalin veri işleyenin veri sorumlusuna yaptığı bildirim üzerine tespit edildiği belirtilmiştir. Tespit tarihi Dermojet bildiriminde 10.09.2026, Mehmet Efendi bildiriminde 07.10.2026, Güllüoğlu bildiriminde 08.10.2026 olarak yer almaktadır.

Dermojet bildirimine göre ihlalden ilgili kişilere ait ad-soyad, telefon numarası, e-posta adresi, adres bilgisi ve hash'lenmiş parola/kullanıcı giriş bilgileri etkilenmiş; etkilenen ilgili kişi sayısı 50.636, etkilenen ilgili kişi grubu müşteriler/potansiyel müşteriler olarak bildirilmiştir. Güllüoğlu bildiriminde ihlalden mağaza müşterilerine ait ad-soyad, telefon numarası, e-posta adresi, adres bilgisi ve saklanan şifre değerleri ile satıcı paneli kullanıcı hesapları ve saklanan şifre değerlerinin etkilendiği, etkilenen ilgili kişi sayısının 67.193 olduğu belirtilmiştir. Mehmet Efendi bildiriminde etkilenen veriler mağaza müşterilerine ait ad-soyad, telefon numarası, e-posta adresi, adres bilgisi ve hash'lenmiş şifre değeri ile satıcı (yönetim) paneli kullanıcı hesapları ve hash'li saklanan şifre değeri olarak sayılmış; ihlalden etkilenmiş olabilecek ilgili kişi sayısının en fazla 15.303 nihai müşteri ile 18 yönetim paneli hesabı sahibinden oluşabileceği ifade edilmiştir. Üç bildirimde de ilgili kişilerin veri sorumlusunun e-posta adresi, telefon numarası veya internet sitesi üzerinden ihlal hakkında bilgi alabilecekleri belirtilmiştir.

Tic. AŞ and Kurukahveci Mehmet Efendi Mahdumları Gıda Sanayi ve Ticaret Anonim Şirketi were published. All three notifications state that the breach occurred as a result of unauthorised access being gained to a server in the data processor's systems holding the data controller's data, by exploiting a security vulnerability in a third-party software library in use, and that the breach was detected upon the notification made by the data processor to the data controller. The date of detection is given as 10 September 2026 in the Dermojet notification, 7 October 2026 in the Mehmet Efendi notification and 8 October 2026 in the Güllüoğlu notification.

According to the Dermojet notification, the data subjects' name and surname, telephone number, e-mail address, address information and hashed password/user login information were affected by the breach; the number of affected data subjects was reported as 50,636 and the affected group of data subjects as customers/potential customers. The Güllüoğlu notification states that the name and surname, telephone number, e-mail address, address information and stored password values of store customers, together with seller panel user accounts and stored password values, were affected by the breach, and that the number of affected data subjects is 67,193. The Mehmet Efendi notification lists the affected data as the name and surname, telephone number, e-mail address, address information and hashed password value of store customers, together with seller (administration) panel user accounts and the hashed stored password value; it states that the number of data subjects who may have been affected by the breach could consist of at most 15,303 end customers and 18 administration panel account holders. All three notifications state that data subjects may obtain information about the breach through the data controller's e-mail address, telephone number or website.

KURULUN DEĞERLENDİRMESİ

THE BOARD'S ASSESSMENT

Üç ilanda da "Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.10.2026 tarih ve 2026/2281 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir." ifadesine yer verilmiştir. İlan metinlerinde veri işleyenin kimliğine ve istismar edilen yazılım kütüphanesine ilişkin bilgi bulunmamaktadır.

All three notices contain the statement: "Although the examination of the matter is ongoing, by the Decision of the Personal Data Protection Board No. 2026/2281 dated 21 October 2026 it has been decided that the data breach notification in question be published on the Authority's website." The notices contain no information on the identity of the data processor or on the software library exploited.

Kurumun internet sitesinde 7 Ekim 2026 tarihinde ilan edilen Hüşyar Tekstil Paz. İth. İhr. San. Tic. Ltd. Şti. bildiriminde de ihlal, aynı ifadelerle, veri işleyen sistemlerindeki bir sunucuya üçüncü taraf yazılım kütüphanesindeki güvenlik zafiyetinin istismar edilmesi suretiyle yetkisiz erişim sağlanması olarak tanımlanmış ve etkilenen veriler mağaza müşterilerinin kimlik ve iletişim bilgileri ile saklanan şifre değerleri olarak bildirilmişti. Dört bildirim arasında bir bağlantı bulunup bulunmadığına ilişkin bir açıklama ilan metinlerinde yer almamaktadır.

In the notification of Hüşyar Tekstil Paz. İth. İhr. San. Tic. Ltd. Şti., published on the Authority's website on 7 October 2026, the breach was likewise described, in the same terms, as unauthorised access gained to a server in the data processor's systems by exploiting a security vulnerability in a third-party software library, and the affected data were reported as the identity and contact information and stored password values of store customers. The notices contain no statement as to whether there is a connection between the four notifications.

02

Sağlık Sektöründen İki Bildirim

Two Notifications from the Health Sector

DNC Sağlık Hizmetleri AŞ: Sağlık Kayıtlarını İçeren Sunucunun Şifrelenmesi

Kurulun 21.10.2026 tarihli ve 2026/2282 sayılı kararıyla ilan edilen DNC Sağlık Hizmetleri AŞ bildiriminde, veri sorumlusunun Ankara Çankaya'da sağlık hizmeti sunan özel bir sağlık kuruluşu olduğu ve ihlalin, veri sorumlusu bilişim personeli tarafından sunucu ekranında beliren Türkçe fidye notunun görülmesi ve veri tabanı dosyalarına erişilemediğinin anlaşılmaması üzerine tespit edildiği belirtilmiştir. Bildirime göre ihlalden veri sorumlusundan hizmet alan hastalar, hasta yakınları, şirket personeli ve iş ortakları etkilenmiştir.

Bildirimde, şifrelenen sunucuda sağlık kuruluşu faaliyetleri kapsamında etkilenen kişisel veriler dört kategori altında sayılmıştır: kimlik verileri (ad,

DNC Sağlık Hizmetleri AŞ: Encryption of a Server Holding Health Records

The notification of DNC Sağlık Hizmetleri AŞ, published by the Board's decision No. 2026/2282 dated 21 October 2026, states that the data controller is a private healthcare institution providing healthcare services in Çankaya, Ankara, and that the breach was detected when the data controller's information technology personnel saw a ransom note in Turkish appearing on the server screen and it became apparent that the database files could not be accessed. According to the notification, patients receiving services from the data controller, patients' relatives, company personnel and business partners were affected by the breach.

The notification lists the personal data affected on the encrypted server, within the scope of the healthcare institution's activities, under four categories: identity data (name, surname, Turkish identity number), contact data (telephone number,

soyadı, T.C. kimlik numarası), iletişim verileri (telefon numarası, adres, e-posta adresi), özel nitelikli kişisel veriler olarak sağlık verileri (muayene, tahlil, tetkik, tanı, teşhis, reçete ve tıbbi tedavi geçmişine dair sağlık kayıtları) ve finansal veriler (randevu kayıtları, faturalandırma ve SGK/özel sigorta provizyon kayıtları). Sunucu veri tabanının şifrelenmiş olması sebebiyle kesin kişi ve kayıt sayısının ilk aşamada tespit edilemediği ifade edilmiştir.

Baxter Turkey Renal Hizmetler AŞ: Sesli Oltalama Temelli Sosyal Mühendislik Saldırısı

Kurulun 21.10.2026 tarihli ve 2026/2292 sayılı kararıyla ilan edilen Baxter Turkey Renal Hizmetler AŞ bildiriminde ihlalin 04.08.2026 tarihinde başladığı ve 06.10.2026 tarihinde tespit edildiği belirtilmiştir. Bildirime göre yetkisiz üçüncü taraflarca veri sorumlusu çalışanlarını hedef alan sesli oltalama temelli bir sosyal mühendislik saldırısı gerçekleştirilmiş; bu saldırı "tehdit aktörünün çalışanların kimlik bilgilerini elde etmesine ve tek bir çalışan hesabı üzerinden Baxter'ın Salesforce veri tabanına ve Baxter'ın Active Directory'si olarak işlev gören bir dahili veri dosyasına erişmesine" olanak sağlamıştır. Etkilenen kişisel verilerin ad, e-posta adresi ve posta adresi gibi temel iş iletişim bilgileri olduğu, etkilenen ilgili kişi grubunun ve sayısının henüz tespit edilemediği ve incelemelerin devam ettiği ifade edilmiştir.

address, e-mail address), health data as special categories of personal data (health records relating to examinations, tests, investigations, diagnoses, diagnostic findings, prescriptions and medical treatment history) and financial data (appointment records, invoicing and SGK/private insurance pre-authorisation records). It is stated that, because the server database was encrypted, the exact number of persons and records could not be determined at the initial stage.

Baxter Turkey Renal Hizmetler AŞ: Vishing-Based Social Engineering Attack

The notification of Baxter Turkey Renal Hizmetler AŞ, published by the Board's decision No. 2026/2292 dated 21 October 2026, states that the breach began on 4 August 2026 and was detected on 6 October 2026. According to the notification, a vishing-based social engineering attack targeting the data controller's employees was carried out by unauthorised third parties; this attack enabled "the threat actor to obtain employees' credentials and, through a single employee account, to access Baxter's Salesforce database and an internal data file functioning as Baxter's Active Directory". It is stated that the affected personal data are basic business contact information such as name, e-mail address and postal address, that the affected group and number of data subjects have not yet been determined and that the examinations are ongoing.

03

Kamu Kurumlarının Bildirimleri

Notifications by Public Bodies

İzmir Büyükşehir Belediyesi: Ele Geçirilmiş Parola ile Kurumsal E-Posta Hesabına Erişim

Kurulun 21.10.2026 tarihli ve 2026/2271 sayılı kararıyla ilan edilen İzmir Büyükşehir Belediyesi bildiriminde, bir kurumsal e-posta hesabından olağan dışı hacimde e-posta gönderimi yapıldığının 30.09.2026 tarihinde tespit edildiği belirtilmiştir. Bildirime göre ilgili hesaba e-posta sunucusundaki bir güvenlik zafiyetinden ötürü değil, önceden ele geçirilmiş parola vasıtasıyla erişim sağlandığı anlaşılmıştır.

Bildirimde, yetkisiz erişim sağlanan hesaplardan ikisine ait posta kutusu içeriklerinin Kurum dışına aktarıldığının, gelen iletileri silmeye yönelik kural tanımlandığının, toplu spam gönderimi yapıldığının, ileti ayarlarının değiştirildiğinin, mevcut yazışmaların açıldığının ve e-posta imza alanına dolandırıcılık içerikli metin eklendiğinin görüldüğü ifade edilmiştir. Etkilenen kişisel veriler ad, soyad, e-posta adresi ve dahili telefon numarası olarak bildirilmiş; etkilenen ilgili kişi sayısının tam olarak belirlenemediği belirtilmiştir.

Ondokuz Mayıs Üniversitesi: USOM Bildirimiyle Tespit Edilen Yetkisiz Erişim

Kurulun 21.10.2026 tarihli ve 2026/2290 sayılı kararıyla ilan edilen Ondokuz Mayıs Üniversitesi bildiriminde, veri sorumlusunun kullandığı bir yazılımdaki güvenlik açığından yararlanılarak yetkisiz erişim gerçekleştirildiği ve 109 kişinin kişisel verilerinin ele geçirildiği belirtilmiştir. İhlal, Ulusal Siber Olaylara Müdahale Merkezinden (USOM) gelen bildirim ile 14.10.2026 tarihinde tespit edilmiştir. Etkilenen kişisel veri kategorileri kimlik, iletişim ve lokasyon olarak bildirilmiş; etkilenen ilgili kişi gruplarının henüz bilinmediği ifade edilmiştir.

İzmir Büyükşehir Belediyesi: Access to a Corporate E-Mail Account by Means of a Compromised Password

The notification of İzmir Büyükşehir Belediyesi, published by the Board's decision No. 2026/2271 dated 21 October 2026, states that it was detected on 30 September 2026 that e-mails were being sent in an unusual volume from a corporate e-mail account. According to the notification, it was established that access to the account in question was gained not through a security vulnerability in the e-mail server but by means of a previously compromised password.

The notification states that it was observed that the mailbox contents of two of the accounts to which unauthorised access had been gained were transferred outside the institution, that a rule was created to delete incoming messages, that bulk spam was sent, that message settings were changed, that existing correspondence was opened and that text of a fraudulent nature was added to the e-mail signature field. The affected personal data were reported as name, surname, e-mail address and internal telephone number; it is stated that the number of affected data subjects could not be determined precisely.

Ondokuz Mayıs Üniversitesi: Unauthorised Access Detected upon Notification by USOM

The notification of Ondokuz Mayıs Üniversitesi, published by the Board's decision No. 2026/2290 dated 21 October 2026, states that unauthorised access was carried out by exploiting a security vulnerability in software used by the data controller and that the personal data of 109 persons were obtained. The breach was detected on 14 October 2026 upon a notification received from the National Cyber Incident Response Centre (USOM). The affected categories of personal data were reported as identity, contact and location; it is stated that the affected groups of data subjects are not yet known.

04

Konaklama Sektöründen İki Bildirim

Two Notifications from the Accommodation Sector

Choice Hotels International, Inc.

Kurulun 21.10.2026 tarihli ve 2026/2288 sayılı kararıyla ilan edilen Choice Hotels International, Inc. bildiriminde ihlalin, tehdit aktörünün sosyal mühendislik yöntemini kullanarak veri sorumlusu çalışanın ağ hesabına yetkisiz erişim sağlaması neticesinde gerçekleştiği ve veri sorumlusunun güvenlik izleme kontrolleri aracılığıyla üretilen bir uyarı vasıtasıyla tespit edildiği belirtilmiştir. Bildirime göre ihlal 05.06.2026 tarihinde başlamış, 06.06.2026 tarihinde sona ermiş ve 05.06.2026 tarihinde tespit edilmiştir. Etkilenen ilgili kişi grubu müşteriler; etkilenen kişisel veriler ad-soyad ve iletişim bilgileri ile etkilenen kişilerin bir kısmı için geçmiş otel konaklamalarına ilişkin detaylardır. Etkilenen kişi sayısı 9.550 olarak bildirilmiştir.

Akropol Turizm Yatırımları İnşaat ve Dış Ticaret Anonim Şirketi (MW Phokaia Beach & Resort)

Kurulun 21.10.2026 tarihli ve 2026/2285 sayılı kararıyla ilan edilen Akropol Turizm Yatırımları İnşaat ve Dış Ticaret Anonim Şirketi bildiriminde, veri sorumlusu tarafından işletilen MW Phokaia Beach & Resort'un bilgi işlem altyapısı ve kurumsal elektronik posta hesaplarına yönelik siber güvenlik olaylarının meydana geldiği belirtilmiştir. Bildirime göre yetkisiz erişim şüphesi bulunan kurumsal hesaplarda veri sorumlusu çalışanları, misafirleri, tedarikçi ve iş ortaklarının gerçek kişi temsilcilerine ait kişisel verilerin bulunması mümkündür; bu çerçevede kimlik ve iletişim bilgileri, kurumsal elektronik posta yazışmalarındaki gerçek kişilere ait bilgiler, rezervasyon ve konaklama süreçlerine ilişkin kişisel veriler, çalışanlara ilişkin özlük ve iletişim bilgileri ile gerçek kişilere ait finansal veya işlem bilgilerinin ihlalden etkilenip etkilenmediği araştırılmaktadır. Olayın başlangıç ve bitiş tarihi, etkilenen hesaplar, kişisel veri kategorileri, ilgili kişi sayısı ve olası veri aktarımının tespiti için veri sorumlusu tarafından inceleme sürecinin yürütülmekte olduğu ifade edilmiştir.

Choice Hotels International, Inc.

The notification of Choice Hotels International, Inc., published by the Board's decision No. 2026/2288 dated 21 October 2026, states that the breach occurred as a result of the threat actor gaining unauthorised access to the network account of a data controller employee by using a social engineering method, and that it was detected by means of an alert generated through the data controller's security monitoring controls. According to the notification, the breach began on 5 June 2026, ended on 6 June 2026 and was detected on 5 June 2026. The affected group of data subjects is customers; the affected personal data are name and surname and contact information and, for some of the affected persons, details relating to past hotel stays. The number of affected persons was reported as 9,550.

Akropol Turizm Yatırımları İnşaat ve Dış Ticaret Anonim Şirketi (MW Phokaia Beach & Resort)

The notification of Akropol Turizm Yatırımları İnşaat ve Dış Ticaret Anonim Şirketi, published by the Board's decision No. 2026/2285 dated 21 October 2026, states that cyber security incidents occurred directed at the information technology infrastructure and corporate e-mail accounts of MW Phokaia Beach & Resort, which is operated by the data controller. According to the notification, the corporate accounts suspected of having been subject to unauthorised access may contain personal data belonging to the data controller's employees and guests and to the natural person representatives of its suppliers and business partners; in this context, it is being investigated whether identity and contact information, information relating to natural persons contained in corporate e-mail correspondence, personal data relating to reservation and accommodation processes, employees' personnel and contact information, and financial or transaction information belonging to natural persons were affected by the breach. It is stated that an examination process is being conducted by the data controller in order to determine the start and end dates of the incident, the accounts affected, the categories of personal data, the number of data subjects and any transfer of data.

05

Vakıf Sunucu Altyapısına Fidyeye Yazılımı Saldırısı: Enka Spor Eğitim ve Sosyal Yardım Vakfı

Ransomware Attack on a Foundation's Server Infrastructure: Enka Spor Eğitim ve Sosyal Yardım Vakfı

Kurulun 21.10.2026 tarihli ve 2026/2284 sayılı kararıyla ilan edilen Enka Spor Eğitim ve Sosyal Yardım Vakfı bildiriminde, veri sorumlusunun sunucu altyapısına yönelik fidye yazılımı saldırısı gerçekleştirildiği ve saldırganın sisteme giriş yöntemi ile etkilenen sistemlerin tam kapsamına ilişkin teknik incelemenin devam ettiği belirtilmiştir. Etkilenen ilgili kişi grupları çalışanlar, öğrenciler, mezun öğrenciler ve çocuklar olarak bildirilmiştir.

Bildirime göre etkilenen kişisel veri kategorileri, öğretmen, öğrenci ve mezunlara ait pasaport kopyalarında yer alan ad-soyad, doğum tarihi ve yeri, uyruk, pasaport numarası ve fotoğraf bilgilerinden oluşan kimlik verileri ile sunucuda arşivlenmiş etkinlik fotoğrafları ve pasaport fotoğraflarından oluşan görsel ve işitsel kayıtlardır. İhlalden etkilenen kişi ve kayıt sayısının bu aşamada bilinmediği ifade edilmiştir.

The notification of Enka Spor Eğitim ve Sosyal Yardım Vakfı, published by the Board's decision No. 2026/2284 dated 21 October 2026, states that a ransomware attack was carried out on the data controller's server infrastructure and that the technical examination of the attacker's method of entry into the system and of the full extent of the systems affected is ongoing. The affected groups of data subjects were reported as employees, students, former students and children.

According to the notification, the affected categories of personal data are identity data, consisting of the name and surname, date and place of birth, nationality, passport number and photograph information contained in copies of the passports of teachers, students and graduates, and visual and audio recordings, consisting of event photographs and passport photographs archived on the server. It is stated that the number of persons and records affected by the breach is not known at this stage.

06

İhlal Bildirimine İlişkin Yükümlülükler

Obligations Relating to Breach Notification

MEVZUATTAKİ
DÜZENLEMETHE LEGISLATION
PROVIDES

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin beşinci fıkrasına göre "işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." On ilanın tamamında bu hükme atıf yapılmış ve ilan kararının bu hükme dayandığı belirtilmiştir.

Under Article 12(5) of Law No. 6698 on the Protection of Personal Data ("PDPL"): "Where the processed personal data are obtained by others through unlawful means, the data controller shall notify the data subject and the Board of this situation as soon as possible. Where necessary, the Board may publish this situation on its own website or by any other method it deems appropriate." All ten notices refer to this provision and state that the publication decision is based on it.

Kurulun 24.01.2019 tarihli ve 2019/10 sayılı kararı uyarınca veri sorumlusunun ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesi, veri işleyenin ise nezdinde gerçekleşen ihlali gecikmeye yer vermeksizin veri sorumlusuna bildirmesi gerekmektedir. Bu notta aktarılan bildirimlerin üçünde ihlal veri işleyen sistemlerinde gerçekleşmiş ve veri işleyen tarafından veri sorumlusuna bildirilmiştir. İlan metinlerinde bildirimlerin Kurula yapıldığı tarihlere yer verilmemiştir.

Pursuant to the Board's decision No. 2019/10 dated 24 January 2019, the data controller must notify the Board without delay and within 72 hours at the latest from the date on which it becomes aware of the breach, and the data processor must notify the data controller without delay of any breach occurring within its organisation. In three of the notifications reported in this update, the breach occurred in data processor systems and was notified by the data processor to the data controller. The notices do not state the dates on which the notifications were made to the Board.

KURUL KARAR NO
BOARD DECISION NO.VERİ SORUMLUSU
DATA CONTROLLERETKİLENEN İLGİLİ KİŞİ SAYISI / GRUBU
NUMBER / GROUP OF AFFECTED DATA SUBJECTS

2026/2271 2026/2271	İzmir Büyükşehir Belediyesi İzmir Büyükşehir Belediyesi	Tam olarak belirlenemedi Could not be determined precisely
2026/2281 2026/2281	Dermojet Sağlık Ürünleri Sanayi ve Ticaret Anonim Şirketi Dermojet Sağlık Ürünleri Sanayi ve Ticaret Anonim Şirketi	50.636; müşteriler/potansiyel müşteriler 50,636; customers/potential customers
2026/2281 2026/2281	Güllüoğlu Gıda San. ve Tic. AŞ Güllüoğlu Gıda San. ve Tic. AŞ	67.193; mağaza müşterileri ve satıcı paneli kullanıcıları 67,193; store customers and seller panel users
2026/2281 2026/2281	Kurukahveci Mehmet Efendi Mahdumları Gıda Sanayi ve Ticaret Anonim Şirketi Kurukahveci Mehmet Efendi Mahdumları Gıda Sanayi ve Ticaret Anonim Şirketi	En fazla 15.303 nihai müşteri ve 18 yönetim paneli hesabı sahibi At most 15,303 end customers and 18 administration panel account holders
2026/2282 2026/2282	DNC Sağlık Hizmetleri AŞ DNC Sağlık Hizmetleri AŞ	İlk aşamada tespit edilemedi; hastalar, hasta yakınları, personel, iş ortakları Not determined at initial stage; patients, relatives, personnel, business partners
2026/2284 2026/2284	Enka Spor Eğitim ve Sosyal Yardım Vakfı Enka Spor Eğitim ve Sosyal Yardım Vakfı	Bu aşamada bilinmiyor; çalışanlar, öğrenciler, mezun öğrenciler, çocuklar Not known at this stage; employees, students, former students, children
2026/2285 2026/2285	Akropol Turizm Yatırımları İnşaat ve Dış Ticaret Anonim Şirketi Akropol Turizm Yatırımları İnşaat ve Dış Ticaret Anonim Şirketi	İnceleme süreci yürütülüyor Examination process ongoing
2026/2288 2026/2288	Choice Hotels International, Inc. Choice Hotels International, Inc.	9.550; müşteriler 9,550; customers
2026/2290 2026/2290	Ondokuz Mayıs Üniversitesi Ondokuz Mayıs Üniversitesi	109; gruplar henüz bilinmiyor 109; groups not yet known
2026/2292 2026/2292	Baxter Turkey Renal Hizmetler AŞ Baxter Turkey Renal Hizmetler AŞ	Henüz tespit edilemedi Not yet determined

21 EKİM 2026 TARİHLİ İLANLAR: KARAR NO, VERİ SORUMLUSU VE ETKİLENEN İLGİLİ KİŞİ SAYISI / PUBLICATIONS OF 21 OCTOBER 2026: DECISION NO., DATA CONTROLLER AND NUMBER OF AFFECTED DATA SUBJECTS

SONUÇ / CONCLUSION

Kurul, 21 Ekim 2026 tarihli 2026/2271, 2026/2281, 2026/2282, 2026/2284, 2026/2285, 2026/2288, 2026/2290 ve 2026/2292 sayılı kararlarıyla on veri ihlali bildirimini Kurumun internet sitesinde ilan etmiştir. Dermojet, Güllüoğlu ve Kurukahveci Mehmet Efendi bildirimlerinde ihlal, veri işleyen sistemlerindeki bir sunucuya üçüncü taraf yazılım kütüphanesindeki güvenlik zafiyetinin istismar edilmesi suretiyle yetkisiz erişim sağlanmasına dayandırılmış; bu üç bildirimde etkilenen ilgili kişi sayısı sırasıyla 50.636, 67.193 ve en fazla 15.303 nihai müşteri ile 18 yönetim paneli hesabı sahibi olarak bildirilmiştir. DNC Sağlık Hizmetleri AŞ

By its decisions Nos. 2026/2271, 2026/2281, 2026/2282, 2026/2284, 2026/2285, 2026/2288, 2026/2290 and 2026/2292 dated 21 October 2026, the Board published ten data breach notifications on the Authority's website. In the Dermojet, Güllüoğlu and Kurukahveci Mehmet Efendi notifications, the breach was attributed to unauthorised access gained to a server in the data processor's systems by exploiting a security vulnerability in a third-party software library; in these three notifications the number of affected data subjects was reported as 50,636, 67,193 and at most 15,303 end customers and 18 administration panel account holders,

bildiriminde fidye yazılımı saldırısıyla şifrelenen sunucuda hastalara ait sağlık kayıtlarının bulunduğu, Enka Spor Eğitim ve Sosyal Yardım Vakfı bildiriminde fidye yazılımı saldırısından pasaport kopyalarındaki verilerin etkilendiği belirtilmiştir.

Baxter Turkey Renal Hizmetler AŞ ve Choice Hotels International, Inc. bildirimlerinde ihlal sosyal mühendislik yöntemiyle çalışan hesaplarına yetkisiz erişime, İzmir Büyükşehir Belediyesi bildiriminde önceden ele geçirilmiş parola ile kurumsal e-posta hesabına erişime, Ondokuz Mayıs Üniversitesi bildiriminde yazılımdaki güvenlik açığından yararlanılarak gerçekleştirilen yetkisiz erişime dayandırılmıştır. Choice Hotels bildiriminde etkilenen kişi sayısı 9.550, Ondokuz Mayıs Üniversitesi bildiriminde 109 olarak belirtilmiş; Akropol Turizm bildiriminde olayın kapsamına ilişkin incelemenin sürdüğü ifade edilmiştir. İlanların tamamında konuya ilişkin incelemenin devam ettiği belirtilmiş, ilan kararlarında ihlale ilişkin bir yaptırıma yer verilmemiştir.

respectively. The DNC Sağlık Hizmetleri AŞ notification states that the server encrypted by a ransomware attack held patients' health records, and the Enka Spor Eğitim ve Sosyal Yardım Vakfı notification states that data contained in passport copies were affected by a ransomware attack.

In the Baxter Turkey Renal Hizmetler AŞ and Choice Hotels International, Inc. notifications, the breach was attributed to unauthorised access to employee accounts by means of social engineering; in the İzmir Büyükşehir Belediyesi notification, to access to a corporate e-mail account by means of a previously compromised password; and in the Ondokuz Mayıs Üniversitesi notification, to unauthorised access carried out by exploiting a security vulnerability in software. The number of affected persons was stated as 9,550 in the Choice Hotels notification and 109 in the Ondokuz Mayıs Üniversitesi notification; the Akropol Turizm notification states that the examination of the scope of the incident is continuing. All of the notices state that the examination of the matter is ongoing, and the publication decisions do not include any sanction in respect of the breaches.

ATIF YAPILAN MEVZUAT VE KARARLAR / LEGISLATION AND DECISIONS CİTED

6698 sayılı Kişisel Verilerin Korunması Kanunu m. 12/5 · Kurulun 24.01.2019 tarihli ve 2019/10 sayılı kararı · Kurulun 21.10.2026 tarihli ve 2026/2271, 2026/2281, 2026/2282, 2026/2284, 2026/2285, 2026/2288, 2026/2290, 2026/2292 sayılı kararları · Kurumun 07.10.2026 tarihli Hüşyar Tekstil Paz. İth. İhr. San. Tic. Ltd. Şti. veri ihlali ilanı

Law No. 6698 on the Protection of Personal Data, Article 12(5) · The Board's decision No. 2019/10 dated 24 January 2019 · The Board's decisions Nos. 2026/2271, 2026/2281, 2026/2282, 2026/2284, 2026/2285, 2026/2288, 2026/2290, 2026/2292 dated 21 October 2026 · The Authority's data breach notice of 7 October 2026 concerning Hüşyar Tekstil Paz. İth. İhr. San. Tic. Ltd. Şti.

İşbu bilgi notu genel bilgilendirme amacıyla hazırlanmış olup hukuki tavsiye niteliği taşımamaktadır. Notta anılan karar, düzenleme ve duyurular yayın tarihi itibarıyla ilgili kurumların internet sitelerinde ve Resmî Gazete'de kamuya açık kaynaklara dayanmaktadır; aktarılan tespitler ilgili kurul ve mahkemelerin değerlendirmesi olup Devin Law & IP'nin görüşünü yansıtmaz. İşbu yazı avukat ile müvekkil arasında bir ilişki kurmamakta ve güncellenmesi hususunda herhangi bir taahhüt içermemektedir. 26 Ekim 2026.

This legal update has been prepared for general information purposes only and does not constitute legal advice. The decisions, legislation and announcements referred to are based on sources published on the relevant authorities' websites and in the Official Gazette as at the date of publication; the findings reported are those of the relevant boards and courts and do not reflect the views of Devin Law & IP. This update does not create an attorney-client relationship and contains no undertaking as to its updating. 26 October 2026.