KVKK
4 VE 11 KASIM 2026
KURUL İLAN KARARLARI
BİLGİ NOTU

KVKK Kasım 2026: Veri İşleyen Kaynaklı İhlaller

PDP Board November 2026: Breaches Originating from Data Processors

Bu bilgi notu, Kişisel Verileri Koruma Kurulunun 04.11.2026 ve 11.11.2026 tarihli kararlarıyla Kurumun internet sitesinde ilan edilmesine karar verilen on iki veri ihlali bildirimini konu almaktadır. İncelenen dönemde Kurum tarafından yeni bir ilke kararı, karar özeti veya rehber yayımlanmamış; 11.11.2026 tarihinde "Seçilmiş Güncel Gelişmeler" derlemesi duyurulmuştur. Notta yalnızca kamuoyu duyurularında yer alan bilgilere yer verilmiş; duyurularda "inceleme devam etmekle birlikte" ifadesiyle belirtildiği üzere, bildirimlerin ilanı veri sorumluları hakkında bir ihlal tespiti veya yaptırım kararı anlamına gelmemektedir.

Kurul, 4 ve 11 Kasım 2026 tarihli kararlarıyla on iki veri ihlali bildirimini ilan etmiştir; bildirimlerin önemli bir bölümü veri işleyen veya alt veri işleyen sistemlerinden kaynaklanmaktadır. Tüm duyurularda incelemenin devam ettiği belirtilmektedir.

This legal update covers the twelve data breach notifications that the Personal Data Protection Board decided, by its decisions dated 4 November 2026 and 11 November 2026, to announce on the Authority's website. During the period under review, the Authority published no new principle decision, decision summary or guideline; a compilation entitled "Selected Current Developments" was announced on 11 November 2026. The update is confined to information contained in the public announcements; as indicated in the announcements by the words "while the examination is ongoing", the announcement of the notifications does not amount to a finding of infringement or a sanction decision in respect of the data controllers.

By its decisions of 4 and 11 November 2026, the Board announced twelve data breach notifications; a significant number of them originate from the systems of data processors or sub-processors. All the announcements state that the examination is ongoing.

GIRIŞ · INTRODUCTION

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin (5) numaralı fıkrası, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildirmesini; Kurulun ise gerekmesi hâlinde bu durumu kendi internet sitesinde veya uygun göreceği başka bir yöntemle ilan edebileceğini düzenlemektedir. Kurul, 4 Kasım 2026 tarihli toplantısında beş, 11 Kasım 2026 tarihli toplantısında yedi veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar vermiştir.

İlan edilen bildirimlerin önemli bir bölümünde ihlalin veri sorumlusunun kendi sistemlerinde değil, hizmet aldığı veri işleyenin veya alt veri işleyenin sistemlerinde gerçekleştiği belirtilmektedir. Bu kapsamda çalışan anketi hizmeti sağlayıcısı (DHL), rezervasyon sistemleri (Air India), hasar danışmanlık firmasının alt tedarikçi yazılımı (Ethica Sigorta), otel işletmelerinin veri işleyen sistemleri (Yazıcı Turizm, Çamyuva Otelcilik, Vinero) ve alt veri işleyenin bulut uygulamaları (Stemline Therapeutics) üzerinden gerçekleşen ihlaller duyurulmuştur. Diğer bildirimler, yönetici parolasının ele geçirilmesi (Pegasus), SQL enjeksiyonu saldırısı (Bursa Ticaret ve Sanayi Odası), web uygulaması güvenlik açığı (NCL) ve sunucu sistemlerine siber saldırı (Mard-Inn Hotel) kaynaklıdır. Aşağıda bildirimler bu gruplandırma çerçevesinde aktarılmaktadır.

Paragraph (5) of Article 12 of the Personal Data Protection Law No. 6698 provides that, where the personal data processed are obtained by others through unlawful means, the data controller is to notify the data subject and the Board of this situation as soon as possible, and that the Board may, where necessary, announce this situation on its own website or by any other method it deems appropriate. At its meeting of 4 November 2026 the Board decided to announce five data breach notifications, and at its meeting of 11 November 2026 seven data breach notifications, on the Authority's website.

A significant number of the notifications announced state that the breach occurred not in the data controller's own systems but in the systems of the data processor or sub-processor whose services it used. In this context, breaches were announced that occurred through an employee survey service provider (DHL), reservation systems (Air India), the sub-supplier software of a claims consultancy firm (Ethica Sigorta), the data processor systems of hotel businesses (Yazıcı Turizm, Çamyuva Otelcilik, Vinero) and the cloud applications of a sub-processor (Stemline Therapeutics). The other notifications arise from the compromise of an administrator password (Pegasus), an SQL injection attack (Bursa Chamber of Commerce and Industry), a web application security vulnerability (NCL) and a cyber attack on server systems (Mard-Inn Hotel). The notifications are set out below in accordance with this grouping.

01 Veri İşleyen ve Alt Veri İşleyen Kaynaklı İhlaller

Breaches Originating from Data Processors and Sub-processors

DHL AG — Çalışan Anketi Hizmet Sağlayıcısı (Kurul Kararı 11.11.2026, 2026/2483)

Duyuruya göre ihlal, "veri sorumlusu tarafından merkezi olarak yürütülen çalışan anketleri kapsamında hizmet alınan veri işleyenin işlettiği veri analizi ve raporlama ortamına yetkisiz erişim sağlanması sonucunda" gerçekleşmiş ve 02.11.2026 tarihinde tespit edilmiştir. İhlalden etkilenen kişisel veri kategorileri kimlik, iletişim ve özlük verileri olup, Türkiye'de istihdam edilen 10.622 çalışanın verilerinin ihlalden etkilendiği tespit edilmiştir. İlgili kişi grubu çalışanlardır.

Air India Limited — Veri İşleyen Rezervasyon Sistemleri (Kurul Kararı 11.11.2026, 2026/2487)

Duyuruya göre ihlal, "veri sorumlusunun veri işleyen sistemlerinde bulunan seyahat rezervasyonu verilerine yetkisiz olarak erişilmesi neticesinde" gerçekleşmiştir. İhlalin 10.08.2023 tarihinde başladığı, 23.09.2026 tarihinde sona erdiği ve "veri işleyen tarafından haber verilmesiyle 03.11.2026 tarihinde tespit edildiği" belirtilmektedir. Etkilenen veriler sınırlı sayıda ad-soyad ve rezervasyon bilgilerini (rezervasyon referans numarası / kısmi PNR kayıtları, uçuş tarihi ve numarası, maskelenmiş kart bilgileri) içermekte; etkilenen kişi sayısı bilinmemektedir.

Ethica Sigorta A.Ş. — Hasar Danışmanının Alt Tedarikçi Yazılımı (Kurul Kararı 11.11.2026, 2026/2493)

Duyuruya göre, "hasar süreçlerinde danışmanlık hizmeti alınan firmanın kullandığı alt tedarikçi yazılımında bulunan yazılımdan kaynaklı güvenlik açığı nedeniyle, hasar dosyalarına ve evraklarına yetkisiz erişim sağlandığının anlaşıldığı" belirtilmektedir. İhlalin 15.01.2022 tarihinde başladığı ve 14.02.2022 tarihinde sona erdiği; etkilenen ilgili kişi grubunun müşteriler ve potansiyel müşteriler olduğu bildirilmiştir. Etkilenen veriler arasında ad, soyad, T.C. kimlik numarası, dosya numarası, poliçe numarası ve hasar bilgisinin yanı sıra 3091 adet araç plaka bilgisi, 2256 adet araç şasi numarası, 885 adet sigorta bedeli bilgisi, 657 adet cep telefonu bilgisi ve 153 adet IBAN bilgisi sayılmaktadır. İlgili kişilerin veri sorumlusunun telefon, e-posta ve KEP adresinden bilgi alabileceği duyurulmuştur.

Yazıcı Turizm, Çamyuva Otelcilik ve Vinero — Veri İşleyen Sistemlerine Yetkisiz Erişim (Kurul Kararları 04.11.2026, 2026/2442, 2026/2441, 2026/2431 ve 2026/2432)

Yazıcı Turizm Yatırımları ve İşletmeleri AŞ, Yazıcı Turizm Marmaris İşletmeleri AŞ, Çamyuva Otelcilik İşletmeleri AŞ (Sveo Resort Kemer) ve Vinero Bağcılık Sanayi ve Ticaret AŞ'ye ilişkin dört duyuruda, ihlalin "veri sorumlusuna ait verilerin bulunduğu veri işleyen sistemlerine yetkisiz erişim sağlanması sonucunda" gerçekleştiği belirtilmektedir. İhlaller sırasıyla 26.10.2026, 25.10.2026, 23.10.2026 ve 23.10.2026 tarihlerinde tespit edilmiştir. Dört bildirimde de etkilenen veri kategorileri kimlik, iletişim ve müşteri işlem bilgileri; ilgili kişi grubu müşteriler olup, etkilenen kişi sayısının tespiti çalışmalarının devam ettiği bildirilmiştir.

Stemline Therapeutics, Inc. — Alt Veri İşleyene Yönelik Sesli Oltalama (Kurul Kararı 11.11.2026, 2026/2490)

Duyuruya göre, veri sorumlusunun alt veri işleyeninden edindiği beyana göre "yetkisiz bir üçüncü kişi tarafından sesli oltalama yöntemi kullanılarak alt veri işleyenin bilgi teknolojileri personelinin kimliğine bürünüldüğü ve bu suretle

DHL AG — Employee Survey Service Provider (Board Decision of 11 November 2026, 2026/2483)

According to the announcement, the breach occurred "as a result of unauthorised access to the data analysis and reporting environment operated by the data processor whose services were used for the employee surveys conducted centrally by the data controller" and was detected on 2 November 2026. The categories of personal data affected by the breach are identity, contact and employment data, and it was established that the data of 10,622 employees employed in Türkiye were affected by the breach. The group of data subjects concerned is employees.

Air India Limited — Data Processor Reservation Systems (Board Decision of 11 November 2026, 2026/2487)

According to the announcement, the breach occurred "as a result of unauthorised access to travel reservation data held in the data controller's data processor systems". It is stated that the breach began on 10 August 2023, ended on 23 September 2026 and "was detected on 03.11.2026 upon notification by the data processor". The data affected include a limited number of names and surnames and reservation information (reservation reference numbers / partial PNR records, flight dates and numbers, masked card information); the number of persons affected is not known.

Ethica Sigorta A.Ş. — Sub-supplier Software of the Claims Consultant (Board Decision of 11 November 2026, 2026/2493)

According to the announcement, "it was understood that unauthorised access to claim files and documents was obtained owing to a software-related security vulnerability in the sub-supplier software used by the firm from which consultancy services were obtained in claims processes". It was reported that the breach began on 15 January 2022 and ended on 14 February 2022, and that the group of data subjects affected is customers and potential customers. The data affected include name, surname, Turkish identity number, file number, policy number and claim information, as well as 3,091 vehicle registration plates, 2,256 vehicle chassis numbers, 885 sums insured, 657 mobile telephone numbers and 153 IBANs. It was announced that data subjects may obtain information through the data controller's telephone, e-mail and registered electronic mail (KEP) address.

Yazıcı Turizm, Çamyuva Otelcilik and Vinero — Unauthorised Access to Data Processor Systems (Board Decisions of 4 November 2026, 2026/2442, 2026/2441, 2026/2431 and 2026/2432)

The four announcements concerning Yazıcı Turizm Yatırımları ve İşletmeleri AŞ, Yazıcı Turizm Marmaris İşletmeleri AŞ, Çamyuva Otelcilik İşletmeleri AŞ (Sveo Resort Kemer) and Vinero Bağcılık Sanayi ve Ticaret AŞ state that the breach occurred "as a result of unauthorised access to the data processor systems holding data belonging to the data controller". The breaches were detected on 26 October 2026, 25 October 2026, 23 October 2026 and 23 October 2026 respectively. In all four notifications, the categories of data affected are identity, contact and customer transaction information, and the group of data subjects concerned is customers; it was reported that work to determine the number of persons affected is ongoing.

Stemline Therapeutics, Inc. — Voice Phishing Targeting a Sub-processor (Board Decision of 11 November 2026, 2026/2490)

According to the announcement, on the basis of the statement obtained by the data controller from its sub-processor, "an unauthorised third party impersonated the sub-processor's information technology staff using the voice phishing method and thereby

çalışanlarına ait hesaplara erişim sağlanarak, saldırganın alt veri işleyenin bazı bulut uygulamalarına erişerek veri sızıntısına neden olduğu" belirtilmektedir. Alt veri işleyen tarafından verileri işlenen azami kişi sayısı 18 olarak bildirilmiş; sağlık verilerinin ve genetik verilerin (belirli mutasyonların tespiti amacıyla analiz edilen tümör hücrelerinin genomunun sınırlı bir kısmına ilişkin) takma adlandırılmış şekilde işlendiği ve etkilenmesi muhtemel ilgili kişi grubunun hastalar olduğu duyurulmuştur. İhlalin kapsamı ve detaylarının henüz belirlenmediği belirtilmektedir.

gained access to accounts belonging to its employees, and the attacker caused a data leak by accessing certain cloud applications of the sub-processor". The maximum number of persons whose data were processed by the sub-processor was reported as 18; it was announced that health data and genetic data (relating to a limited part of the genome of tumour cells analysed to detect specific mutations) were processed in pseudonymised form and that the group of data subjects likely to be affected is patients. It is stated that the scope and details of the breach have not yet been determined.

02 Veri Sorumlusunun Kendi Sistemlerinden Kaynaklanan İhlaller

Breaches Originating from the Data Controller's Own Systems

Pegasus Hava Taşımacılığı A.Ş. — Yönetici Parolasıyla Yetkisiz Erişim (Kurul Kararı 11.11.2026, 2026/2486)

Duyuruya göre, "veri sorumlusu bilgi teknolojileri talep ve geliştirme sistemine ait yönetici (admin) parolasının ne şekilde elde edildiği kesin olarak tespit edilememekle birlikte, bahse konu parola kullanılarak yetkisiz erişim sağlandığı" belirtilmektedir. İhlal 12.10.2026 tarihinde başlamış ve 26.10.2026 tarihinde tespit edilmiştir. Etkilenen veri kategorileri kimlik ve iletişim verileri, etkilenen ilgili kişi sayısı 11.762, ilgili kişi grubu çalışanlar ve kullanıcılardır.

Bursa Ticaret ve Sanayi Odası — SQL Enjeksiyonu (Kurul Kararı 11.11.2026, 2026/2494)

Duyuruya göre veri sorumlusu SQL injection saldırısına maruz kalmış; ihlal 02.11.2026 tarihinde veri tabanı hizmetinin durması üzerine gerçekleştirilen kontroller sonucunda tespit edilmiştir. Üye firma ve şahıslara ait kimlik, iletişim, üyelik ve tahsilat kayıtlarının dışarı aktarıldığı, genel muhasebe kayıtlarının etkilenmediği; etkilenen gerçek kişi sayısı ve kayıt sayısının henüz kesin olarak belirlenemediği bildirilmiştir.

NCL (Bahamas) Ltd. — Web Uygulaması Açığı ve Oltalama E-postaları (Kurul Kararı 04.11.2026, 2026/2437)

Duyuruya göre, rezervasyonların yönetimi amacıyla kullanılan bir web uygulamasındaki güvenlik açığından yararlanan yetkisiz kişilerin bazı müşterilerin adı, e-posta adresi, doğum tarihi ve rezervasyon numarası bilgilerine eriştiğine dair bulgular tespit edilmiş; bu bilgilerin söz konusu müşterilere sahte e-postalar göndermek için kullanıldığı anlaşılmıştır. Veri sorumlusu oltalama e-postalarından 10.10.2026 tarihinde haberdar olmuş, 12.10.2026 tarihinde yapılan incelemede zararlı faaliyetlere ilişkin bulgular tespit edilmiştir. En fazla 2.392 ilgili kişiye ait bilgilere erişilmiş olabileceği değerlendirilmektedir.

Sadunoğlu İnşaat (Mard-Inn Hotel) — Sunucu ve Misafir Kablosuz Ağına Siber Saldırı (Kurul Kararı 11.11.2026, 2026/2485)

Duyuruya göre, sunucu sistemlerine ve misafir kablosuz ağ altyapısına yönelik siber saldırı neticesinde sistem ve dosyalara erişim engellenmiş; sunucuda kayıtlı otel misafirlerine ait kişisel veriler yetkisiz kişilerce ele geçirilmiştir. İhlal 27.10.2026 tarihinde başlamış ve aynı gün tespit edilmiştir. Etkilenen veri kategorileri kimlik, iletişim, özlük, müşteri işlem, fiziksel mekân güvenliği, işlem güvenliği, finans ile görsel ve işitsel kayıtlar; ilgili kişi grubu çalışanlar, müşteriler ve kullanıcılardır. Etkilenen kişi sayısı hakkında net bir tespit yapılamadığı bildirilmiştir.

Pegasus Hava Taşımacılığı A.Ş. — Unauthorised Access Using an Administrator Password (Board Decision of 11 November 2026, 2026/2486)

According to the announcement, "although it could not be established with certainty how the administrator (admin) password of the data controller's information technology request and development system was obtained, unauthorised access was gained using that password". The breach began on 12 October 2026 and was detected on 26 October 2026. The categories of data affected are identity and contact data, the number of data subjects affected is 11,762, and the groups of data subjects concerned are employees and users.

Bursa Chamber of Commerce and Industry — SQL Injection (Board Decision of 11 November 2026, 2026/2494)

According to the announcement, the data controller was subjected to an SQL injection attack; the breach was detected on 2 November 2026 as a result of checks carried out after the database service stopped. It was reported that identity, contact, membership and collection records of member companies and individuals were exported, that the general accounting records were not affected, and that the number of natural persons and records affected has not yet been determined with certainty.

NCL (Bahamas) Ltd. — Web Application Vulnerability and Phishing E-mails (Board Decision of 4 November 2026, 2026/2437)

According to the announcement, findings were made that unauthorised persons, exploiting a security vulnerability in a web application used to manage reservations, had accessed the name, e-mail address, date of birth and reservation number of certain customers, and it was understood that this information was used to send fraudulent e-mails to those customers. The data controller became aware of the phishing e-mails on 10 October 2026, and findings relating to the malicious activity were made in the examination carried out on 12 October 2026. It is assessed that information belonging to at most 2,392 data subjects may have been accessed.

Sadunoğlu İnşaat (Mard-Inn Hotel) — Cyber Attack on Servers and the Guest Wireless Network (Board Decision of 11 November 2026, 2026/2485)

According to the announcement, as a result of a cyber attack on the server systems and guest wireless network infrastructure, access to systems and files was blocked and personal data of hotel guests stored on the server were obtained by unauthorised persons. The breach began on 27 October 2026 and was detected on the same day. The categories of data affected are identity, contact, employment, customer transaction, physical premises security, transaction security, financial, and visual and audio records; the groups of data subjects concerned are employees, customers and users. It was reported that no clear determination could be made as to the number of persons affected.

03 Duyurularda Yer Alan Ortak Unsurlar

Common Elements of the Announcements

Kurulun ilan kararlarının tamamında Kanun'un 12 nci maddesinin (5) numaralı fıkrası dayanak gösterilmekte ve "konuya ilişkin inceleme devam etmekle birlikte" ifadesine yer verilmektedir. Duyurularda ihlalin başlangıç, bitiş ve tespit tarihleri, etkilenen veri kategorileri, ilgili kişi grupları ve biliniyorsa etkilenen kişi sayısı ile ilgili kişilerin bilgi alabileceği iletişim kanalları aktarılmaktadır.

Veri işleyen kaynaklı bildirimlerde iki husus öne çıkmaktadır. Birincisi, ihlalin tespiti ile başlangıcı arasındaki süredir: Air India bildiriminde ihlalin 2023 yılında başladığı ve veri işleyenin haber vermesiyle 2026 yılında tespit edildiği; Ethica Sigorta bildiriminde ihlalin 2022 yılının Ocak–Şubat aylarında gerçekleştiği belirtilmektedir. İkincisi, ihlalin alt tedarikçi veya alt veri işleyen düzeyinde gerçekleşmesidir: Ethica Sigorta bildiriminde danışmanlık firmasının "alt tedarikçi yazılımı", Stemline bildiriminde "alt veri işleyen" ifadeleri kullanılmaktadır. Kanun'un 12 nci maddesinin (2) numaralı fıkrasına göre veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, veri güvenliğine ilişkin tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

Kurulun 24.01.2019 tarihli ve 2019/10 sayılı kararında veri sorumlusunun ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirimde bulunması esası benimsenmiştir; ilan edilen duyurularda bildirim tarihleri ayrıca belirtilmemekte, yalnızca ihlalin tespit tarihi ve Kurulun ilan kararının tarihi yer almaktadır.

All the Board's announcement decisions cite paragraph (5) of Article 12 of the Law as their legal basis and contain the words "while the examination of the matter is ongoing". The announcements set out the start, end and detection dates of the breach, the categories of data affected, the groups of data subjects concerned and, where known, the number of persons affected, together with the contact channels through which data subjects may obtain information.

Two points stand out in the notifications originating from data processors. The first is the time between the start and the detection of the breach: the Air India notification states that the breach began in 2023 and was detected in 2026 upon notification by the data processor, and the Ethica Sigorta notification states that the breach occurred in January–February 2022. The second is that the breach occurred at the level of a sub-supplier or sub-processor: the Ethica Sigorta notification uses the words "sub-supplier software" of the consultancy firm and the Stemline notification the words "sub-processor". Under paragraph (2) of Article 12 of the Law, where personal data are processed on the data controller's behalf by another natural or legal person, the data controller is jointly responsible with those persons for taking the measures relating to data security.

The Board's decision dated 24 January 2019 and numbered 2019/10 adopted the principle that the data controller is to notify the Board without delay and within 72 hours at the latest from the date on which it becomes aware of the breach; the notification dates are not stated separately in the announcements, which contain only the date of detection of the breach and the date of the Board's announcement decision.

04 Kurumun Diğer Yayımları

Other Publications of the Authority

Kurumun Duyurular sayfasında 11.11.2026 tarihinde "Seçilmiş Güncel Gelişmeler" başlıklı derleme, 28.10.2026 tarihinde "Klinik Araştırmalarda Kişisel Verilerin Korunması Çalıştayı" duyurusu yayımlanmıştır. İlke Kararları sayfasında en güncel kayıt, 08.10.2026 tarihli Resmî Gazete'de yayımlanan, işverenler tarafından çalışanlara tahsis edilen kurumsal e-posta hesapları başta olmak üzere işin yürütülmesi amacıyla kullanılan iletişim kanallarının denetlenmesine ilişkin 16.09.2026 tarihli ve 2026/2035 sayılı İlke Kararıdır. Rehberler sayfasında en güncel yayın, Eylül 2026'da duyurulan Avukatların Mesleki Faaliyetlerinde Kişisel Verilerin Korunmasına İlişkin Uygulama Rehberidir. İncelenen dönemde Kurul Karar Özetleri sayfasına yeni bir özet eklenmemiştir.

On the Authority's Announcements page, a compilation entitled "Selected Current Developments" was published on 11 November 2026 and an announcement of the "Workshop on the Protection of Personal Data in Clinical Trials" on 28 October 2026. The most recent entry on the Principle Decisions page is Principle Decision No. 2026/2035 dated 16 September 2026, published in the Official Gazette dated 8 October 2026, on the monitoring of communication channels used for the conduct of business, in particular corporate e-mail accounts allocated to employees by employers. The most recent publication on the Guidelines page is the Implementation Guide on the Protection of Personal Data in the Professional Activities of Attorneys, announced in September 2026. No new summary was added to the Board Decision Summaries page during the period under review.

SONUÇ · CONCLUSION

Kurul, 4 ve 11 Kasım 2026 tarihli kararlarıyla on iki veri ihlali bildiriminin kamuoyuna duyurulmasına karar vermiştir. Bildirimlerin önemli bir bölümü veri işleyen veya alt veri işleyen sistemlerinden kaynaklanan ihlallere ilişkindir; bunlar arasında Türkiye'de istihdam edilen 10.622 çalışanı etkileyen DHL bildirimi ile T.C. kimlik numarası ve IBAN bilgilerini içeren Ethica Sigorta bildirimi yer almaktadır. Veri sorumlusunun kendi sistemlerinden kaynaklanan ihlaller arasında 11.762 kişiyi etkileyen Pegasus bildirimi ile Bursa Ticaret ve Sanayi Odasının üye veri

By its decisions of 4 and 11 November 2026, the Board decided to announce twelve data breach notifications to the public. A significant number of the notifications concern breaches originating from the systems of data processors or sub-processors; these include the DHL notification affecting 10,622 employees employed in Türkiye and the Ethica Sigorta notification involving Turkish identity numbers and IBANs. The breaches originating from the data controller's own systems include the Pegasus notification affecting 11,762 persons and the SQL injection attack on the member database of the Bursa Chamber of Commerce and Industry. All the announcements state that the

tabanına yönelik SQL enjeksiyonu saldırısı bulunmaktadır. Tüm duyurularda incelemenin devam ettiği belirtilmekte; ilan kararı, veri sorumluları hakkında Kanun'un 18 inci maddesi kapsamında bir yaptırım kararı içermemektedir.

examination is ongoing; the announcement decisions do not contain any sanction decision under Article 18 of the Law in respect of the data controllers.

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. 9 Kasım 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. 9 November 2026.

Devin | LAW & IP

DEVİN LAW & IP · FERKO SIGNATURE, KAT B3, ŞİŞLİ / İSTANBUL

devinlaw.com.tr/insights