

KVKK

İLKE KARARI 2026/2035

RG 8 EKİM 2026 · 33394

İHLAL BİLDİRİMLERİ · 7 EKİM

2026

KVKK Ekim 2026: Kurumsal E-Posta Denetimi ve İhlal Bildirimleri

PDP Board October 2026: Corporate E-Mail Monitoring and Breach Notifications

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

Bu bilgi notunda, Kişisel Verileri Koruma Kurulunun 16 Eylül 2026 tarihli ve 2026/2035 sayılı ilke kararı ile Kurulun 7 Ekim 2026 tarihli kararlarıyla Kişisel Verileri Koruma Kurumunun internet sitesinde ilan edilen on yedi veri ihlali bildirimi aktarılmaktadır. İlke kararı 8 Ekim 2026 tarihli ve 33394 sayılı Resmî Gazete’de yayımlanmış, aynı tarihte Kurumun internet sitesinde duyurulmuştur. Not, 5 Ekim 2026 – 11 Ekim 2026 tarihleri arasında Kurumun internet sitesinde yayımlanan duyuruları kapsamaktadır.

Kurulun kurumsal e-posta ve iş iletişim kanallarının denetlenmesine ilişkin 2026/2035 sayılı ilke kararı 8 Ekim 2026 tarihli Resmî Gazete’de yayımlanmış; Kurul, 7 Ekim 2026 tarihli kararlarıyla on yedi veri ihlali bildirimini ilan etmiştir.

GİRİŞ · INTRODUCTION

Kurulun 2026/2035 sayılı ilke kararı, işverenler tarafından çalışanlara tahsis edilen kurumsal e-posta hesapları başta olmak üzere işin yürütülmesi amacıyla kullanılan iletişim kanallarının denetlenmesinde uyulması gereken usul ve esasları konu almaktadır. Kararda, Kuruma intikal eden ihbar ve şikâyetlerin incelenmesi sonucunda bu kanalların izlendiği, yazışma içeriklerine erişildiği, trafik ve log kayıtlarının incelendiği ve elde edilen verilerin disiplin süreçlerinde veya iş sözleşmesinin sona erdirilmesine ilişkin süreçlerde kullanıldığı, çalışanların ise bu faaliyetler hakkında yeterli, açık ve somut şekilde bilgilendirilmediği tespitine yer verilmiştir. Karar, işverenler bakımından dikkate alınması gereken hususları on dört başlık altında saymaktadır.

Kurul, 7 Ekim 2026 tarihinde on yedi veri ihlali bildiriminin ilan edilmesine karar vermiş, ilanlar aynı tarihte Kurumun internet sitesinde yayımlanmıştır. Bildirimlerin altısında ihlal fidye yazılımı saldırısına, üçünde veri sorumlusu sistemlerine dışarıdan erişim sağlanarak verilerin şifrelenmesine dayandırılmıştır. Yedi bildirimde ihlal, veri sorumlusunun hizmet aldığı veri işleyenin sistemlerinde gerçekleşmiştir. İlanların tamamında konuya ilişkin incelemenin devam ettiği belirtilmiştir. İlan kararlarında ihlale ilişkin bir yaptırıma yer verilmemiştir.

This legal update reports the resolution of principle No. 2026/2035 dated 16 September 2026 of the Personal Data Protection Board (“the Board”) and seventeen data breach notifications published on the website of the Personal Data Protection Authority (“the Authority”) pursuant to the Board’s decisions dated 7 October 2026. The resolution of principle was published in the Official Gazette No. 33394 dated 8 October 2026 and was announced on the Authority’s website on the same date. The update covers announcements published on the Authority’s website between 5 October 2026 and 11 October 2026.

Principle decision No. 2026/2035 on monitoring corporate e-mail and business communication channels was published in the Official Gazette of 8 October 2026; the Board published seventeen data breach notifications by decisions dated 7 October 2026.

The Board’s resolution of principle No. 2026/2035 concerns the procedures and principles to be observed in the monitoring of communication channels used for the performance of work, in particular corporate e-mail accounts allocated to employees by employers. The decision records the finding that, following the examination of reports and complaints submitted to the Authority, these channels were being monitored, the content of correspondence was being accessed, traffic and log records were being examined and the data obtained were being used in disciplinary proceedings or in proceedings relating to the termination of the employment contract, while employees were not informed of these activities in a sufficient, clear and specific manner. The decision lists the matters to be taken into account by employers under fourteen headings.

On 7 October 2026, the Board decided to publish seventeen data breach notifications, and the notices were published on the Authority’s website on the same date. In six of the notifications the breach is attributed to a ransomware attack, and in three to the encryption of data following external access to the data controller’s systems. In seven notifications, the breach occurred in the systems of a data processor from which the data controller receives services. 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

Kurumsal E-Posta ve İş İletişim Kanallarının Denetlenmesine İlişkin İlke Kararı

Resolution of Principle on the Monitoring of Corporate E-Mail and Business Communication Channels

Kararın Künyesi ve Dayandığı Tespitler

İlke kararının başlığı "İşverenler Tarafından Çalışanlara Tahsis Edilen Kurumsal E-Posta Hesapları Başta Olmak Üzere, İşin Yürütülmesi Amacıyla Kullanılan İletişim Kanallarının Denetlenmesinde Uyulması Gereken Usul ve Esaslar Hakkında" şeklindedir. Kararda, kurumsal e-posta hesaplarının yalnızca bir iletişim aracı olmadığı, çalışanın mesleki ve kimi durumlarda kişisel ilişki ağına, çalışma düzenine, iletişim faaliyetlerine ve yazışma içeriklerine ilişkin kişisel verileri barındıran bir veri kaynağı niteliği taşıdığı belirtilmiştir.

Kurul, bu hesapların ve diğer iletişim kanallarının denetlenmesini, işverenin iş sözleşmesinden ve yönetim hakkından kaynaklanan yetkileri ile çalışanın Anayasa'nın 20 nci ve 22 nci maddelerinde güvence altına alınan özel hayatın gizliliği, kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti arasında adil bir dengenin gözetilmesini gerektiren bir kişisel veri işleme faaliyeti olarak nitelendirmiştir.

KURULUN DEĞERLENDİRMESİ

THE BOARD'S ASSESSMENT

Kararda, denetleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("Kanun") öngörülen kişisel veri işleme şartlarına ve genel ilkelere tabi olduğu, ilgili durumlarda aydınlatma ve veri güvenliği yükümlülüklerinin de yerine getirilmesini gerektirdiği belirtilmiş ve şu ifadeye yer verilmiştir: "İletişim aracının işverene ait olması veya işyerinde kullanılması, işverene çalışanların iletişim faaliyetleri üzerinde sınırsız bir denetim yetkisi sağlamamaktadır."

The decision states that monitoring activities are subject to the conditions for processing personal data and the general principles laid down in Law No. 6698 on the Protection of Personal Data ("PDPL"), and that, where relevant, they also require compliance with the obligation to inform and the data security obligations; it includes the following statement: "The fact that the means of communication belongs to the employer or is used in the workplace does not confer on the employer an unlimited power of monitoring over employees' communication activities."

İş Amaçlı ve Özel Amaçlı Kullanım Ayrımı

Karara göre denetimin kapsamı belirlenirken iletişim aracının hangi amaçla tahsis edildiği ve kullanımına ilişkin kuralların neler olduğu dikkate alınmalıdır. İşveren, yönetim hakkı kapsamında işyeri iletişim araçlarının özel amaçlı kullanımına ilişkin kuralları belirleyebilir. Bu kuralların açık, anlaşılır ve çalışan tarafından bilinebilir olması gerekmektedir. Kararda, özel amaçlı kullanımın yasaklandığı durumlarda dahi işverenin denetim yetkisinin ölçülülük ilkesiyle sınırlı olduğu, iş amaçlı kullanım ile özel amaçlı kullanımın birbirinden kesin olarak ayrılmadığı hallerde ise denetim yetkisinin kapsamının daha dar değerlendirilmesi gerektiği belirtilmiştir.

Kurul, teknik erişim yetkisi ile hukuki erişim yetkisinin birbirinden ayrılması gerektiğini ifade etmiştir. Karara göre işverenin belirli bir cihaz, oturum, ağ veya kurumsal sistem üzerinde teknik erişim imkânına sahip olması, çalışanın kişisel e-posta hesabı, kişisel anlık mesajlaşma uygulaması, sosyal medya hesabı veya benzeri özel iletişim alanlarında bulunan yazışma içeriklerine serbestçe erişebileceği anlamına gelmemektedir.

Önceden Bilgilendirme ve Aydınlatma Yükümlülüğü

Kararda, çalışanların gerçekleştirilecek denetim faaliyeti hakkında önceden bilgilendirilmiş olmasının, denetimin hukuka uygunluğunun tespitinde önem taşıyan unsurlardan biri olduğu belirtilmiştir. Kurul, Anayasa Mahkemesi içtihadında aranan bilgilendirme ile Kanun'un 10 uncu maddesinde düzenlenen aydınlatma yükümlülüğünün aynı kavramlar olmadığını ifade etmiştir. Karara göre Kanun'un 10 uncu maddesinde öngörülen unsurları içeren ve denetim faaliyetinin amacı, kapsamı ve yöntemi hakkında açık ve somut bilgi veren

Particulars of the Decision and the Findings on Which It Is Based

The resolution of principle is entitled "On the Procedures and Principles to be Observed in the Monitoring of Communication Channels Used for the Performance of Work, in Particular Corporate E-Mail Accounts Allocated to Employees by Employers". The decision states that corporate e-mail accounts are not merely a means of communication, but constitute a source of data containing personal data relating to the employee's professional and, in some cases, personal network of relationships, working patterns, communication activities and the content of correspondence.

The Board characterised the monitoring of these accounts and of other communication channels as a personal data processing activity requiring a fair balance to be struck between the employer's powers arising from the employment contract and the right of management, on the one hand, and the employee's privacy of private life, right to request the protection of personal data and freedom of communication, as guaranteed by Articles 20 and 22 of the Constitution, on the other.

Distinction Between Business Use and Private Use

According to the decision, in determining the scope of monitoring, account must be taken of the purpose for which the means of communication was allocated and of the rules governing its use. The employer may, within the scope of its right of management, lay down rules on the private use of workplace means of communication. Those rules must be clear, comprehensible and capable of being known by the employee. The decision states that, even where private use is prohibited, the employer's power of monitoring is limited by the principle of proportionality, and that, where business use and private use cannot be definitively separated from one another, the scope of the power of monitoring must be assessed more narrowly.

The Board stated that technical access authority and legal access authority must be distinguished from one another. According to the decision, the fact that the employer has the technical means of access to a particular device, session, network or corporate system does not mean that it may freely access the content of correspondence held in the employee's personal e-mail account, personal instant messaging application, social media account or similar private communication spaces.

Prior Notice and the Obligation to Inform

The decision states that the fact that employees have been given prior notice of the monitoring activity to be carried out is one of the elements of importance in determining the lawfulness of the monitoring. The Board stated that the notice required in the case-law of the Constitutional Court and the obligation to inform governed by Article 10 of the PDPL are not the same concepts. According to the decision, a duly provided information notice which contains the elements prescribed in Article 10 of the PDPL and gives clear and specific information on the

usulüne uygun bir aydınlatma, çalışanın denetim konusunda önceden bilgilendirilmesi şartını karşılayabilecektir.

İşveren tarafından yapılacak aydınlatmada kişisel veri işleme faaliyetinin hukuki sebebi, amacı, kapsamı ve yöntemi ile iletişim içeriklerine hangi hâllerde erişilebileceği, verilerin saklama süresi ve ilgili kişilerin Kanun'un 11 inci maddesi kapsamındaki hakları açık, anlaşılır ve somut biçimde ortaya konulmalıdır. Kararda, çalışanlara yalnızca kurumsal e-posta hesabının işveren tarafından denetlenebileceğine ilişkin genel bir bildirimde bulunulmasının, somut olayın özelliklerine göre önceden bilgilendirme bakımından yeterli olmayacağı ve aydınlatma yükümlülüğünün yerine getirildiği sonucunu kendiliğinden doğurmayacağı belirtilmiştir.

MEVZUATTAKİ DÜZENLEME

THE LEGISLATION PROVIDES

Kanun'un 10 uncu maddesinin birinci fıkrasına göre veri sorumlusu veya yetkilendirdiği kişi, kişisel verilerin elde edilmesi sırasında ilgili kişilere veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi ile 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür.

Under Article 10(1) of the PDPL, the data controller or the person authorised by it is obliged, at the time the personal data are obtained, to inform data subjects of the identity of the data controller and of its representative, if any, the purpose for which the personal data will be processed, to whom and for what purpose the processed personal data may be transferred, the method and legal basis of the collection of personal data, and their other rights listed in Article 11.

Açık Rıza

Kararda, iş ilişkisindeki bağımlılık hâli ve taraflar arasındaki güç dengesi dikkate alındığında, çalışanın açık rızasının kural olarak e-posta denetimi bakımından "her durumda öncelikli hukuki dayanak olarak kabul edilmesi"nin mümkün olmadığı belirtilmiştir. Açık rızaya dayanan durumlarda rızanın özgür iradeyle verilip verilmediği somut olayın koşulları çerçevesinde ayrıca değerlendirilmelidir. Karara göre geçerli bir açık rızanın veya Kanun'da öngörülen diğer bir kişisel veri işleme şartının bulunması da işverene sınırsız bir denetim yetkisi tanımamaktadır.

Ölçülülük, Kademeli Denetim ve İçerik Denetimi

Karara göre denetim faaliyetleri, Kanun'un 4 üncü maddesinde düzenlenen genel ilkelere uygun olarak hukuka ve dürüstlük kurallarına uygun, belirli, açık ve meşru amaçlarla ve bu amaçla bağlantılı, sınırlı ve ölçülü bir şekilde yürütülmelidir. Elde edilen kişisel veriler, işleme amacı bakımından gerekli olan süreden daha uzun süreyle muhafaza edilmemelidir. Kararda denetim faaliyetlerinde kademeliğin esas alınması gerektiği, işverenin ulaşmak istediği meşru amaca daha az müdahaleci bir yöntemle ulaşmasının mümkün olduğu hâllerde daha ağır bir denetim yöntemine başvurulmaması gerektiği ifade edilmiştir.

KURULUN DEĞERLENDİRMESİ

THE BOARD'S ASSESSMENT

Kararda içerik denetimine ilişkin olarak, çalışana tahsis edilen e-posta ya da diğer iletişim araçlarında yer alan içeriklerin incelenmesine "kural olarak yalnızca somut şüphe veya belirli bir olayla bağlantılı meşru bir amaç bulunması halinde ve denetimin amacıyla sınırlı olacak şekilde" başvurulması gerektiği belirtilmiştir. Kararda, kapsamı belirsiz, genel ve sürekli nitelikte içerik incelemelerinden kaçınılması gerektiği ifade edilmiştir.

As regards content monitoring, the decision states that the examination of content held in the e-mail or other means of communication allocated to the employee is to be resorted to "as a rule only where there is a specific suspicion or a legitimate purpose connected with a particular event, and in a manner limited to the purpose of the monitoring". The decision states that content examinations which are of indeterminate scope, general and continuous in nature must be avoided.

Özel Nitelikli Veriler, Erişim Yetkisi ve İş İlişisinin Sona Ermesi

Kararda, içerik denetiminde incelenen içerik veya eklerinde Kanun'un 6 ncı maddesi kapsamında özel nitelikli kişisel verilerin bulunabileceğinin dikkate alınması gerektiği belirtilmiştir. Kurul, çalışanların iletişimlerinin iletişimin karşı taraflarına veya başka üçüncü kişilere ait kişisel veri de içerebileceğini, denetimin bu kişiler bakımından doğurabileceği etkilerin de göz önünde bulundurulması gerektiğini ifade etmiştir.

purpose, scope and method of the monitoring activity is capable of satisfying the requirement that the employee be given prior notice of the monitoring.

The information notice to be provided by the employer must set out, in a clear, comprehensible and specific manner, the legal basis, purpose, scope and method of the personal data processing activity, the circumstances in which the content of communications may be accessed, the retention period of the data and the rights of data subjects under Article 11 of the PDPL. The decision states that merely giving employees a general notice to the effect that the corporate e-mail account may be monitored by the employer will not, depending on the particular circumstances of the case, be sufficient in terms of prior notice and will not of itself lead to the conclusion that the obligation to inform has been fulfilled.

Explicit Consent

The decision states that, having regard to the state of dependency in the employment relationship and the balance of power between the parties, it is not possible, as a rule, for the employee's explicit consent to be "accepted in every case as the primary legal basis" for e-mail monitoring. Where explicit consent is relied upon, whether the consent was given of the employee's own free will must be assessed separately in the light of the circumstances of the particular case. According to the decision, the existence of valid explicit consent or of another condition for processing personal data laid down in the PDPL likewise does not confer on the employer an unlimited power of monitoring.

Proportionality, Graduated Monitoring and Content Monitoring

According to the decision, monitoring activities must be carried out, in accordance with the general principles set out in Article 4 of the PDPL, lawfully and in conformity with the rules of good faith, for specified, explicit and legitimate purposes and in a manner that is relevant, limited and proportionate to that purpose. The personal data obtained must not be retained for longer than is necessary for the purpose of the processing. The decision states that monitoring activities must be based on a graduated approach and that, where the employer is able to achieve the legitimate aim pursued by a less intrusive method, a more severe method of monitoring must not be resorted to.

Special Categories of Data, Access Authority and Termination of the Employment Relationship

The decision states that, in content monitoring, account must be taken of the fact that the content examined or its attachments may contain special categories of personal data within the meaning of Article 6 of the PDPL. The Board stated that employees' communications may also contain personal data belonging to the other parties to the communication or to other third parties, and that the effects which the monitoring may have on those persons must also be taken into consideration.

Karara göre bu kanallardan elde edilen verilere erişim, yalnızca bu konuda görev ve yetki verilmiş belli sayıdaki personelle sınırlandırılmalıdır. Erişim yetkileri görev tanımları doğrultusunda belirlenmeli, erişim işlemlerine ilişkin kayıtlar tutulmalı ve verilere erişen kişilerin gizlilik yükümlülükleri güvence altına alınmalıdır. İş ilişkisinin sona ermesinden sonra kurumsal e-posta hesabı ve bu hesap kapsamında elde edilmiş veya tutulmakta olan verilere ilişkin kişisel veri işleme faaliyetlerinin hukuki dayanağı ayrıca değerlendirilmelidir. Kararda, iş ilişkisinin sona ermesinin söz konusu verilerin süresiz olarak erişilebilir veya işlenebilir olduğu anlamına gelmediği belirtilmiştir.

Kararın Sonuç Kısmı

Kurul, sayılan yükümlülükler uylmadığının tespiti hâlinde somut olayın özellikleri dikkate alınarak gerekli inceleme ve değerlendirmelerin yapılacağı ve Kanun'un 18 inci maddesi hükümleri gereğince ilgili veri sorumluları hakkında işlem tesis edileceği hususunda kamuoyunun bilgilendirilmesine karar vermiştir. Kanun'un 18 inci maddesi, Kanun'da öngörülen yükümlülükler aykırılık hâlinde uygulanacak idari para cezalarını düzenlemektedir.

According to the decision, access to the data obtained from these channels must be restricted to a specified number of personnel who have been assigned duties and authority in this regard. Access authorisations must be determined in line with job descriptions, records of access operations must be kept and the confidentiality obligations of persons accessing the data must be secured. After the employment relationship has ended, the legal basis of the personal data processing activities relating to the corporate e-mail account and to the data obtained or held within the scope of that account must be assessed separately. The decision states that the termination of the employment relationship does not mean that the data in question may be accessed or processed indefinitely.

Operative Part of the Decision

The Board decided to inform the public that, where non-compliance with the obligations listed is established, the necessary examinations and assessments will be carried out having regard to the particular circumstances of the case and action will be taken against the data controllers concerned pursuant to the provisions of Article 18 of the PDPL. Article 18 of the PDPL governs the administrative fines applicable in the event of non-compliance with the obligations laid down in the PDPL.

02

Fidye Yazılımı ve Verilerin Şifrelenmesine Dayanan İhlal Bildirimleri

Breach Notifications Based on Ransomware and the Encryption of Data

30 Eylül 2026 Tarihli İhlale İlişkin Dört Bildirim: Çağrı Kayıtları ve Özlük Verileri

Kurulun 07.10.2026 tarihli ve 2026/2204, 2026/2205, 2026/2206 ve 2026/2207 sayılı kararlarıyla sırasıyla PCT Yazılım Danışmanlık Telekomünikasyon Pazarlama Ticaret Anonim Şirketi, PCX Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi, Procat Teknoloji Danışmanlık Hizmetleri Anonim Şirketi ve Procatcx Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi bildirimleri ilan edilmiştir. Dört bildirimde de ihlalin veri sorumlusu sistemlerine gerçekleştirilen fidye yazılımı saldırısı neticesinde meydana geldiği, 30.09.2026 tarihinde gerçekleştiği ve aynı gün tespit edildiği belirtilmiştir.

Bildirimlere göre ihlale uğramış olabileceği değerlendirilen veriler, çalışanlara ait performans değerlendirme verileri ve özlük dosyalarındaki eski tip nüfus cüzdanı suretleri üzerinde bulunan veriler dâhil insan kaynakları özlük bilgileri, iş başvurusunda bulunmuş kişilere ait özgeçmişler ile çağrı merkezi hizmetleri kapsamındaki çağrı detay kayıtları ve çağrı ses kayıtlarıdır. Bildirimlerde kişisel verilerin dışarıya aktarıldığına ilişkin henüz bir tespitin bulunmadığı, etkilenen kişi ve kayıt sayısının henüz kesin olarak tespit edilemediği ifade edilmiştir.

Üniversite ve Perakende Sektöründen İki Bildirim

Kurulun 07.10.2026 tarihli ve 2026/2203 sayılı kararıyla ilan edilen Yıldız Teknik Üniversitesi bildiriminde, veri sorumlusunun sanallaştırma altyapısı ve üzerinde çalışan sunucuların fidye yazılımı saldırısından etkilendiği belirtilmiştir. İhlal 01.10.2026 tarihinde başlamış ve aynı gün tespit edilmiştir. Etkilenen ilgili kişi grupları öğrenci, personel ve ziyaretçilerdir. Bildirimde, mevcut kayıtlara göre ihlalden etkilenmiş olabilecek ilgili kişi sayısının yaklaşık 140.000 öğrenci ve 4.500 personel olduğu, ziyaretçilere ilişkin sayının henüz belirlenemediği ve etkilenen kişisel veri kategorilerinin belirlenemediği ifade edilmiştir.

Kurulun 07.10.2026 tarihli ve 2026/2210 sayılı kararıyla ilan edilen Monnalisa Bebek Giyim San ve Tic AŞ bildiriminde ihlalin fidye yazılımı saldırısı neticesinde gerçekleştiği, 28.09.2026 tarihinde başladığı, 29.09.2026 tarihinde sona erdiği ve 29.09.2026 tarihinde tespit edildiği belirtilmiştir. Bildirime göre saldırının hangi yöntemle ve hangi güvenlik açılarından yararlanılarak gerçekleştirildiği

Four Notifications Concerning the Breach of 30 September 2026: Call Records and Personnel Data

By the Board's decisions Nos. 2026/2204, 2026/2205, 2026/2206 and 2026/2207 dated 7 October 2026, the notifications of PCT Yazılım Danışmanlık Telekomünikasyon Pazarlama Ticaret Anonim Şirketi, PCX Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi, Procat Teknoloji Danışmanlık Hizmetleri Anonim Şirketi and Procatcx Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi, respectively, were published. All four notifications state that the breach arose as a result of a ransomware attack on the data controller's systems, that it occurred on 30 September 2026 and that it was detected on the same day.

According to the notifications, the data considered possibly to have been subject to the breach are human resources personnel information, including employees' performance evaluation data and the data appearing on copies of old-format identity cards held in personnel files, the curricula vitae of persons who had submitted job applications, and call detail records and call voice recordings within the scope of call centre services. The notifications state that there has as yet been no finding that personal data were transferred outside, and that the number of affected persons and records has not yet been definitively determined.

Two Notifications from the University and Retail Sectors

The notification of Yıldız Teknik Üniversitesi, published by the Board's decision No. 2026/2203 dated 7 October 2026, states that the data controller's virtualisation infrastructure and the servers running on it were affected by a ransomware attack. The breach began on 1 October 2026 and was detected on the same day. The affected groups of data subjects are students, staff and visitors. The notification states that, according to the existing records, the number of data subjects who may have been affected by the breach is approximately 140,000 students and 4,500 staff, that the number relating to visitors has not yet been determined and that the affected categories of personal data could not be determined.

The notification of Monnalisa Bebek Giyim San ve Tic AŞ, published by the Board's decision No. 2026/2210 dated 7 October 2026, states that the breach occurred as a result of a ransomware attack, that it began on 28 September 2026, ended on 29 September 2026 and was detected on 29 September 2026. According to the notification, the method by which the attack was carried out and the security vulnerability exploited could not be definitively determined. The notice records that

kesin olarak belirlenememiştir. İlanda, etkilenen ilgili kişi grubunun ve kişisel veri kategorilerinin bildirimde belirtilmediği kaydedilmiştir.

Sistemlere Dışarıdan Erişimle Verilerin Şifrelenmesi

Kurulun 07.10.2026 tarihli ve 2026/2214, 2026/2215 ve 2026/2216 sayılı kararlarıyla sırasıyla Gür Grup İnşaat San.ve Tic. Anonim Şirketi, Medikalyapı Sağlık Yatırımları Anonim Şirketi ve Ortadoğu Holding Anonim Şirketi bildirimleri ilan edilmiştir. Üç bildirimde de ihlalin 03.10.2026 tarihinde başladığı ve aynı gün tespit edildiği, veri sorumlusu sistemlerine dışarıdan erişim sağlanarak verilerin şifrelendiği ve erişime kapatıldığı belirtilmiştir.

Medikalyapı ve Ortadoğu Holding bildirimlerinde etkilenen ilgili kişi grupları çalışanlar, kullanıcılar ve müşteriler; etkilenen veri kategorileri lokasyon, özlük, hukuki işlem, risk yönetimi, finans, mesleki deneyim, pazarlama ile görsel ve işitsel kayıtlar olarak bildirilmiştir. Gür Grup bildiriminde etkilenen gruplar çalışanlar ve kullanıcılar, etkilenen kategoriler lokasyon, özlük ile görsel ve işitsel kayıtlardır. Üç bildirimde de etkilenmiş olabilecek kişi sayısının tahmin edilemediği ifade edilmiştir.

the affected group of data subjects and the categories of personal data were not stated in the notification.

Encryption of Data Following External Access to Systems

By the Board's decisions Nos. 2026/2214, 2026/2215 and 2026/2216 dated 7 October 2026, the notifications of Gür Grup İnşaat San.ve Tic. Anonim Şirketi, Medikalyapı Sağlık Yatırımları Anonim Şirketi and Ortadoğu Holding Anonim Şirketi, respectively, were published. All three notifications state that the breach began on 3 October 2026 and was detected on the same day, and that external access was gained to the data controller's systems and the data were encrypted and rendered inaccessible.

In the Medikalyapı and Ortadoğu Holding notifications, the affected groups of data subjects were reported as employees, users and customers, and the affected data categories as location, personnel, legal transaction, risk management, finance, professional experience, marketing, and visual and audio recordings. In the Gür Grup notification, the affected groups are employees and users, and the affected categories are location, personnel, and visual and audio recordings. All three notifications state that the number of persons who may have been affected could not be estimated.

KURUL KARAR NO BOARD DECISION NO.	VERİ SORUMLUSU DATA CONTROLLER	İHLALIN NİTELİĞİ NATURE OF THE BREACH
2026/2203 2026/2203	Yıldız Teknik Üniversitesi Yıldız Teknik Üniversitesi	Fidye yazılımı saldırısı Ransomware attack
2026/2204 2026/2204	PCT Yazılım Danışmanlık Telekomünikasyon Pazarlama Ticaret Anonim Şirketi PCT Yazılım Danışmanlık Telekomünikasyon Pazarlama Ticaret Anonim Şirketi	Fidye yazılımı saldırısı Ransomware attack
2026/2205 2026/2205	PCX Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi PCX Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi	Fidye yazılımı saldırısı Ransomware attack
2026/2206 2026/2206	Procat Teknoloji Danışmanlık Hizmetleri Anonim Şirketi Procat Teknoloji Danışmanlık Hizmetleri Anonim Şirketi	Fidye yazılımı saldırısı Ransomware attack
2026/2207 2026/2207	Procatcx Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi Procatcx Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi	Fidye yazılımı saldırısı Ransomware attack
2026/2210 2026/2210	Monnalisa Bebek Giyim San ve Tic AŞ Monnalisa Bebek Giyim San ve Tic AŞ	Fidye yazılımı saldırısı Ransomware attack
2026/2214 2026/2214	Gür Grup İnşaat San.ve Tic. Anonim Şirketi Gür Grup İnşaat San.ve Tic. Anonim Şirketi	Dışarıdan erişimle verilerin şifrelenmesi Encryption of data following external access
2026/2215 2026/2215	Medikalyapı Sağlık Yatırımları Anonim Şirketi Medikalyapı Sağlık Yatırımları Anonim Şirketi	Dışarıdan erişimle verilerin şifrelenmesi Encryption of data following external access
2026/2216 2026/2216	Ortadoğu Holding Anonim Şirketi Ortadoğu Holding Anonim Şirketi	Dışarıdan erişimle verilerin şifrelenmesi Encryption of data following external access

7 EKİM 2026 TARİHLİ İLANLAR: FİDYE YAZILIMI VE VERİLERİN ŞİFRELENMESİ / PUBLICATIONS OF 7 OCTOBER 2026: RANSOMWARE AND ENCRYPTION OF DATA

03

Veri İşleyen Sistemlerine İlişkin Bildirimler ve Restoran Zinciri Bildirimleri

Notifications Concerning Data Processor Systems and the Restaurant Chain Notifications

Çağrı Merkezi ve Ses Kaydı Hizmeti Alınan Veri İşleyenler

Kurulun 07.10.2026 tarihli ve 2026/2212 sayılı kararıyla D Elektronik Şans Oyunları ve Yayıncılık A.Ş., 2026/2211 sayılı kararıyla 4 Race Teknoloji ve Yazılım A.Ş. bildirimleri ilan edilmiştir. İki bildirimde de çağrı merkezi hizmeti alınan veri işleyenin sistemlerine siber saldırı gerçekleştirildiği ve verilerin şifrelenerek erişilemez hâle getirildiği, veri işleyenin 30.09.2026 tarihinde sisteminde hizmet kesintisi yaşaması üzerine durumu tespit ederek veri sorumlusuna bilgi verdiği belirtilmiştir.

Data Processors Providing Call Centre and Voice Recording Services

By the Board's decision No. 2026/2212 dated 7 October 2026, the notification of D Elektronik Şans Oyunları ve Yayıncılık A.Ş. was published, and by decision No. 2026/2211 that of 4 Race Teknoloji ve Yazılım A.Ş. Both notifications state that a cyber attack was carried out on the systems of the data processor from which call centre services are received and that the data were encrypted and rendered inaccessible, and that the data processor, upon experiencing a service interruption in its system on 30 September 2026, identified the situation and informed the data controller.

Bildirimlerde, ilk incelemelerde verilerin dışarı aktarıldığına dair bulguya rastlanmadığı, saldırganın sistemlerde bulunduğu süre ve altyapının paylaşımlı yapısı dikkate alındığında yetkisiz erişim ihtimalinin de tam olarak dışlanamadığı ve kesin sonucun adli bilişim incelemesiyle netleşeceği ifade edilmiştir. Etkilenen veriler çağrı ses kayıtları ile çağrı detay kayıtlarıdır. Bildirimlere göre ses kayıtları, görüşme içeriğine bağlı olarak doğum tarihi ve T.C. kimlik numarası gibi kimlik doğrulama bilgilerini ve işlem bilgilerini de içerebilmektedir. Bildirimlerde, görme engelli üyelere destek süreci de çağrı merkezi üzerinden yürütüldüğünden sınırlı sayıda görüşmede engellilik durumuna ilişkin beyan bulunabileceği belirtilmiştir.

Kurulun 07.10.2026 tarihli ve 2026/2195 sayılı kararıyla ilan edilen GIG Sigorta AŞ bildiriminde, veri sorumlusunun teknolojik altyapı hizmeti, IVR kurulumu ve ses kayıtlarının arşivlenmesi konusunda hizmet aldığı veri işleyenin siber saldırıya maruz kaldığının 30.09.2026 tarihinde tespit edildiği belirtilmiştir. Bildirime göre bir günlük ses kayıt verileri şifrelenmiş, 161 adet çağrıya ilişkin ses kaydına erişim sağlanamamıştır. Etkilenen veriler müşterilere ait kimlik, iletişim ve müşteri işlem verileridir.

E-Ticaret ve Restoran Zinciri Bildirimleri

Kurulun 07.10.2026 tarihli ve 2026/2213 sayılı kararıyla ilan edilen Hüşyar Tekstil Paz. İth. İhr. San. Tic. Şti. bildiriminde 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. İhlal, veri işleyenin 29.09.2026 tarihinde gerçekleştirdiği bildirim üzerine tespit edilmiştir. Etkilenen veriler mağaza müşterilerinin adı, soyadı, posta adresi, e-posta adresi, telefon numarası ve saklanan şifre değerleri ile admin paneli kullanıcı hesapları ve saklanan şifre değerleridir.

Kurulun 07.10.2026 tarihli ve 2026/2200, 2026/2197 ve 2026/2198 sayılı kararlarıyla sırasıyla Smart Delivery Pizza Yemekçilik Gıda E-Ticaret Reklamcılık ve Ticaret Limited Şirketi, DDP Temizlik Pizza Gıda Sanayi ve Ticaret Limited Şirketi ve Deniz Pizza Restoranları ve Ticaret Limited Şirketi bildirimleri ilan edilmiştir. Üç bildirimde de ihlalin, veri sorumlusuna ait verilerin bulunduğu veri işleyen sistemlerine yetkisiz erişim sağlanması sonucunda gerçekleştiği ve veri işleyenin bildirimiyle tespit edildiği belirtilmiştir. Veri işleyenin bildirim tarihi Smart Delivery ve Deniz Pizza bakımından 30.09.2026, DDP bakımından 01.10.2026'dır.

Kurulun 07.10.2026 tarihli ve 2026/2199 sayılı kararıyla ilan edilen Dodo Brands International FZCO bildiriminde, veri sorumlusuna ait verilerin bulunduğu sistemlere yetkisiz erişim sağlanması sonucunda ihlalin gerçekleştiği ve 28.09.2026 tarihinde tespit edildiği belirtilmiştir. Bu dört bildirimde etkilenen ilgili kişi grupları müşteriler ve çalışanlar, etkilenen veri kategorileri kimlik, iletişim, lokasyon, müşteri işlem ve finans bilgileridir. Dört bildirimde de etkilenen ilgili kişi sayısının tespiti çalışmalarının devam ettiği ifade edilmiştir. Dodo Brands bildiriminde ilgili kişilerin Dodo Pizza mobil uygulaması üzerinden aydınlatılacağı belirtilmiştir.

The notifications state that the initial examinations revealed no finding that data were transferred outside, that, having regard to the length of time the attacker was present in the systems and the shared structure of the infrastructure, the possibility of unauthorised access could also not be entirely excluded, and that the definitive outcome will be clarified by a digital forensic examination. The affected data are call voice recordings and call detail records. According to the notifications, the voice recordings may, depending on the content of the conversation, also contain identity verification information, such as date of birth and Turkish identity number, and transaction information. The notifications state that, since the support process for visually impaired members is also conducted through the call centre, a limited number of conversations may contain statements relating to disability status.

The notification of GIG Sigorta AŞ, published by the Board's decision No. 2026/2195 dated 7 October 2026, states that it was detected on 30 September 2026 that the data processor from which the data controller receives services in respect of technological infrastructure, IVR installation and the archiving of voice recordings had been subjected to a cyber attack. According to the notification, one day's voice recording data were encrypted and the voice recordings relating to 161 calls could not be accessed. The affected data are identity, contact and customer transaction data belonging to customers.

E-Commerce and Restaurant Chain Notifications

The notification of Hüşyar Tekstil Paz. İth. İhr. San. Tic. Ltd. Şti., published by the Board's decision No. 2026/2213 dated 7 October 2026, states 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. The breach was detected upon the notification made by the data processor on 29 September 2026. The affected data are the name, surname, postal address, e-mail address, telephone number and stored password values of store customers, and admin panel user accounts and stored password values.

By the Board's decisions Nos. 2026/2200, 2026/2197 and 2026/2198 dated 7 October 2026, the notifications of Smart Delivery Pizza Yemekçilik Gıda E-Ticaret Reklamcılık ve Ticaret Limited Şirketi, DDP Temizlik Pizza Gıda Sanayi ve Ticaret Limited Şirketi and Deniz Pizza Restoranları ve Ticaret Limited Şirketi, respectively, were published. All three notifications state that the breach occurred as a result of unauthorised access being gained to the data processor's systems holding the data controller's data and that it was detected upon the data processor's notification. The date of the data processor's notification is 30 September 2026 for Smart Delivery and Deniz Pizza, and 1 October 2026 for DDP.

The notification of Dodo Brands International FZCO, published by the Board's decision No. 2026/2199 dated 7 October 2026, states that the breach occurred as a result of unauthorised access being gained to the systems holding the data controller's data and that it was detected on 28 September 2026. In these four notifications, the affected groups of data subjects are customers and employees, and the affected data categories are identity, contact, location, customer transaction and finance information. All four notifications state that work to determine the number of affected data subjects is continuing. The Dodo Brands notification states that data subjects will be informed through the Dodo Pizza mobile application.

KURUL KARAR NO BOARD DECISION NO.	VERİ SORUMLUSU DATA CONTROLLER	İHLALIN NİTELİĞİ NATURE OF THE BREACH
2026/2195 2026/2195	GİG Sigorta AŞ GİG Sigorta AŞ	Veri işleyene siber saldırı; ses kayıt verileri şifrelenmiş Cyber attack on data processor; voice recording data encrypted
2026/2197 2026/2197	DDP Temizlik Pizza Gıda Sanayi ve Ticaret Limited Şirketi DDP Temizlik Pizza Gıda Sanayi ve Ticaret Limited Şirketi	Veri işleyen sistemlerine yetkisiz erişim Unauthorised access to data processor's systems
2026/2198 2026/2198	Deniz Pizza Restoranları ve Ticaret Limited Şirketi Deniz Pizza Restoranları ve Ticaret Limited Şirketi	Veri işleyen sistemlerine yetkisiz erişim Unauthorised access to data processor's systems
2026/2199 2026/2199	Dodo Brands International FZCO Dodo Brands International FZCO	Veri sorumlusuna ait verilerin bulunduğu sistemlere yetkisiz erişim Unauthorised access to systems holding the data controller's data
2026/2200 2026/2200	Smart Delivery Pizza Yemekçilik Gıda E-Ticaret Reklamcılık ve Ticaret Limited Şirketi Smart Delivery Pizza Yemekçilik Gıda E-Ticaret Reklamcılık ve Ticaret Limited Şirketi	Veri işleyen sistemlerine yetkisiz erişim Unauthorised access to data processor's systems
2026/2211 2026/2211	4 Race Teknoloji ve Yazılım A.Ş. 4 Race Teknoloji ve Yazılım A.Ş.	Çağrı merkezi veri işleyene siber saldırı; veriler şifrelenmiş Cyber attack on call centre data processor; data encrypted
2026/2212 2026/2212	D Elektronik Şans Oyunları ve Yayıncılık A.Ş. D Elektronik Şans Oyunları ve Yayıncılık A.Ş.	Çağrı merkezi veri işleyene siber saldırı; veriler şifrelenmiş Cyber attack on call centre data processor; data encrypted
2026/2213 2026/2213	Hüşyar Tekstil Paz. İth. İhr. San. Tic. Ltd. Şti. Hüşyar Tekstil Paz. İth. İhr. San. Tic. Ltd. Şti.	Üçüncü taraf yazılım kütüphanesi zafiyetiyle veri işleyen sunucusuna yetkisiz erişim Unauthorised access to data processor's server via third-party software library vulnerability

7 EKİM 2026 TARİHLİ İLANLAR: ÇAĞRI MERKEZİ, E-TİCARET VE RESTORAN ZİNCİRİ BİLDİRİMLERİ / PUBLICATIONS OF 7 OCTOBER 2026: CALL CENTRE, E-COMMERCE AND RESTAURANT CHAIN NOTIFICATIONS

04

İhlal Bildirimine İlişkin Yükümlülükler

Obligations Relating to Breach Notification

MEVZUATTAKİ
DÜZENLEMETHE LEGISLATION
PROVIDES

Kanun'un 12 nci maddesinin beşinci fıkrasına göre "İşlenen 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."

Article 12(5) of the PDPL provides: "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."

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.

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.

SONUÇ / CONCLUSION

Kurulun 16 Eylül 2026 tarihli ve 2026/2035 sayılı ilke kararı 8 Ekim 2026 tarihli ve 33394 sayılı Resmî Gazete'de yayımlanmıştır. Kararda, kurumsal e-posta hesapları ve işin yürütülmesi amacıyla kullanılan diğer iletişim kanallarının denetlenmesinin Kanun'daki işleme şartlarına, genel ilkelere, aydınlatma ve veri güvenliği yükümlülüklerine tabi olduğu belirtilmiştir. Karar; iş amaçlı ve özel amaçlı kullanım ayrımı, teknik ve hukuki erişim yetkisinin ayrılması, önceden bilgilendirme, aydınlatmanın kapsamı, açık rıza, kademeli denetim, içerik denetimi, erişim yetkilendirmesi ve iş ilişkisinin sona ermesi konularında hususlar içermektedir. Kurul, bu yükümlülükler uylmadığının tespiti hâlinde Kanun'un 18 inci maddesi gereğince işlem tesis edileceğini duyurmuştur.

The Board's resolution of principle No. 2026/2035 dated 16 September 2026 was published in the Official Gazette No. 33394 dated 8 October 2026. The decision states that the monitoring of corporate e-mail accounts and of other communication channels used for the performance of work is subject to the processing conditions and general principles in the PDPL and to the obligation to inform and the data security obligations. The decision contains points on the distinction between business use and private use, the separation of technical and legal access authority, prior notice, the scope of the information notice, explicit consent, graduated monitoring, content monitoring, access authorisation and the termination of the employment relationship. The Board announced that, where non-compliance with these obligations is established, action will be taken pursuant to Article 18 of the PDPL.

Kurul, 7 Ekim 2026 tarihli 2026/2195, 2026/2197, 2026/2198, 2026/2199, 2026/2200, 2026/2203, 2026/2204, 2026/2205, 2026/2206, 2026/2207, 2026/2210, 2026/2211, 2026/2212, 2026/2213, 2026/2214, 2026/2215 ve

By its decisions Nos. 2026/2195, 2026/2197, 2026/2198, 2026/2199, 2026/2200, 2026/2203, 2026/2204, 2026/2205, 2026/2206, 2026/2207, 2026/2210, 2026/2211, 2026/2212, 2026/2213, 2026/2214, 2026/2215 and 2026/2216 dated 7 October 2026,

2026/2216 sayılı kararlarıyla on yedi veri ihlali bildirimini ilan etmiştir. Bildirimlerin altında fidye yazılımı saldırısı, üçünde veri sorumlusu sistemlerine dışarıdan erişim sağlanarak verilerin şifrelenmesi bildirilmiş, yedisinde ihlal veri işleyen sistemlerinde gerçekleşmiştir. Etkilenen ilgili kişi sayısına ilişkin bir rakam yalnızca Yıldız Teknik Üniversitesi bildiriminde yer almış, bu bildirimde sayı yaklaşık 140.000 öğrenci ve 4.500 personel olarak belirtilmiştir. İlanların tamamında konuya ilişkin incelemenin devam ettiği belirtilmiştir.

the Board published seventeen data breach notifications. In six of the notifications a ransomware attack was reported and in three the encryption of data following external access to the data controller's systems, while in seven the breach occurred in data processor systems. A figure for the number of affected data subjects appears only in the Yıldız Teknik Üniversitesi notification, in which the number is stated as approximately 140,000 students and 4,500 staff. All of the notices state that the examination of the matter is ongoing.

ATIF YAPILAN MEVZUAT VE KARARLAR / LEGISLATION AND DECISIONS CITED

Türkiye Cumhuriyeti Anayasası m. 20, 22 - 6698 sayılı Kişisel Verilerin Korunması Kanunu m. 4, 6, 10, 11, 12, 18 - Kurulun 16.09.2026 tarihli ve 2026/2035 sayılı ilke kararı (RG 08.10.2026, 33394) - Kurulun 24.01.2019 tarihli ve 2019/10 sayılı kararı - Kurulun 07.10.2026 tarihli ve 2026/2195, 2026/2197, 2026/2198, 2026/2199, 2026/2200, 2026/2203, 2026/2204, 2026/2205, 2026/2206, 2026/2207, 2026/2210, 2026/2211, 2026/2212, 2026/2213, 2026/2214, 2026/2215, 2026/2216 sayılı kararları

Constitution of the Republic of Türkiye, Articles 20, 22 - Law No. 6698 on the Protection of Personal Data, Articles 4, 6, 10, 11, 12, 18 - The Board's resolution of principle No. 2026/2035 dated 16 September 2026 (Official Gazette No. 33394 dated 8 October 2026) - The Board's decision No. 2019/10 dated 24 January 2019 - The Board's decisions Nos. 2026/2195, 2026/2197, 2026/2198, 2026/2199, 2026/2200, 2026/2203, 2026/2204, 2026/2205, 2026/2206, 2026/2207, 2026/2210, 2026/2211, 2026/2212, 2026/2213, 2026/2214, 2026/2215, 2026/2216 dated 7 October 2026

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 kurmakta ve güncellenmesi hususunda herhangi bir taahhüt içermemektedir. 12 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. 12 October 2026.