

KVKK

M. 8, 9, 12, 18

REHBER NO. 115

EYLÜL 2026

Avukatların KVKK Yükümlülükleri ve Veri İşleyen Kaynaklı İhlaller

Lawyers' Data Protection Obligations and Breaches at Data Processors

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

Bu bilgi notunda, Kişisel Verileri Koruma Kurumunun 22 Eylül 2026 tarihinde yayımladığı Avukatların Mesleki Faaliyetlerinde Kişisel Verilerin Korunmasına İlişkin Uygulama Rehberi, Kurulun 16 ve 23 Eylül 2026 tarihli kararlarıyla ilan edilen veri işleyen kaynaklı ihlal bildirimleri ve karar özetleri arasında yer alan 2024 tarihli üç fidye yazılımı kararı incelenmektedir. İncelenen rehber ve kararlarda veri sorumlusu ile veri işleyen sıfatının her bir faaliyet için ayrı belirlenmesi, verinin kaynağının belgelenmesi, üretken yapay zekâ araçlarına yüklenen belgelerin işlenmesi ve aktarılması ile veri işleyen nezdindeki ihlallerde sorumluluğun paylaşımı ele alınmaktadır.

Rehber avukatı kural olarak veri sorumlusu saymakta; incelenen ihlal ilanları ve fidye yazılımı kararları ise veri işleyen nezdindeki bir güvenlik açığının bildirim yükümlülüğünü ve yaptırım riskini veri sorumlusundan uzaklaştırmadığını göstermektedir.

This note examines the Implementation Guide on the Protection of Personal Data in the Professional Activities of Lawyers, published by the Personal Data Protection Authority on 22 September 2026, the processor-originated breach notifications announced by the Board's decisions of 16 and 23 September 2026, and three ransomware decisions of 2024 appearing among the published decision summaries. The guide and decisions examined concern the determination of controller and processor status for each activity, the documentation of the source of data, the processing and transfer of documents uploaded to generative AI tools, and the allocation of liability for breaches at a data processor.

The Guide treats the lawyer as a data controller as a rule, while the breach announcements and ransomware decisions examined show that a security vulnerability at a data processor does not relieve the controller of its notification obligation or of the risk of sanction.



GİRİŞ · INTRODUCTION

Dönemin ana gelişmesi, Kurumun Türkiye Barolar Birliğinin görüş ve katkılarıyla hazırladığı ve KVKK Yayınları No. 115 olarak yayımlanan 158 sayfalık Uygulama Rehberidir. Rehber, avukatın kendisinden avukatlık ortaklığına, tevkil olunan meslektaştan stajyer ve büro çalışanına kadar mesleki faaliyette yer alan kişilerin Kanun karşısındaki sıfatını ele almaktadır. Verinin elde edilmesi ve açıklanmasının hukuki dayanakları, yurt dışına aktarım, yapay zekâ araçlarının kullanımı, veri sorumlusunun yükümlülükleri ve veri güvenliği ayrı bölümlerde incelenmektedir. Rehberde Kurulun avukatlar hakkında bugüne kadar verdiği kararlara atıf yapılmakta ve açıklamalar bu kararlarla desteklenmektedir.

Aynı dönemde Kurul, bir veri işleyenin sunucusunda üçüncü taraf bir yazılım kütüphanesindeki açığın istismar edilmesiyle başlayan ve perakende, hazır giyim, kozmetik ve elektronik sektörlerinde çok sayıda veri sorumlusunu etkileyen ihlal bildirimlerini ilan etmiştir. Kurumun yayımladığı karar özetleri arasında ise fidye yazılımı saldırısı sonrasında veri sorumlusunun çelişkili beyanlarını ve alınmamış teknik tedbirleri idari para cezasına bağlayan 2024 tarihli üç karar yer almaktadır.

The principal development of the period is the 158-page Implementation Guide, prepared by the Authority with the opinions and contributions of the Union of Turkish Bar Associations and published as PDPA Publication No. 115. The Guide addresses the status under the PDPL of those involved in legal practice, from the individual lawyer to the law partnership and from the substituted colleague to trainee lawyers and office staff. Separate chapters examine the legal bases for obtaining and disclosing data, transfers abroad, the use of artificial intelligence tools, the obligations of the data controller and data security. The Guide refers to the decisions the Board has rendered to date concerning lawyers and supports its explanations with those decisions.

In the same period, the Board announced breach notifications that began with the exploitation of a vulnerability in a third-party software library on a data processor's server and affected numerous data controllers in the retail, apparel, cosmetics and electronics sectors. The decision summaries published by the Authority also include three decisions of 2024 in which, following a ransomware attack, the controller's contradictory statements and the technical measures it had failed to take formed the basis of an administrative fine.

01

Avukatların ve Avukatlık Ortaklıklarının KVKK Kapsamındaki Sıfatı

The Status of Lawyers and Law Partnerships under the PDPL

Rehberin en uzun bölümü, avukatın veri sorumlusu mu yoksa veri işleyen mi olduğu sorusuna ayrılmıştır. Kurum bu soruya tek bir cevap vermek yerine, veri sorumlusu kavramının işlevsel olduğunu ve sıfatın "her bir kişisel veri işleme faaliyeti açısından ayrı ayrı" irdelenmesi gerektiğini hatırlatmaktadır. Rehberde, avukatlık sözleşmesinin asli ediminin "belirli bir hukuki yardımda bulunmak" olduğu belirtilmektedir; kişisel veri işlenmesi ise bu edimin ifası için gerekli bir yan yükümlülüktür. Dolayısıyla avukatlık sözleşmesi bir "kişisel veri işleme sözleşmesi"ne dönüşmemekte ve avukat, sırf müvekkilin talimatıyla bağlı olduğu için veri işleyen sayılmamaktadır.

The longest chapter of the Guide is devoted to whether a lawyer is a data controller or a data processor. Rather than giving a single answer, the Authority recalls that the concept of data controller is functional and that status must be examined "separately for each personal data processing activity". The Guide states that the principal obligation under a legal services agreement is "to provide specific legal assistance"; the processing of personal data is an ancillary obligation necessary for performing it. A legal services agreement therefore does not become a "personal data processing agreement", and a lawyer is not a data processor merely because the lawyer is bound by the client's instructions.

REHBERDEKİ AÇIKLAMA

THE GUIDE'S EXPLANATION

Mesleğini bağımsız olarak icra eden avukat, müvekkilinin ve üçüncü kişilerin verileri bakımından kural olarak veri sorumlusudur; hangi verinin hangi amaçla işleneceğine son tahlilde avukat karar vermektedir. Aynı büroda birlikte çalışan avukatlar, ortak büroya rağmen kendi müvekkilleri bakımından ayrı ayrı gerçek kişi veri sorumlusudur. Avukatlık ortaklığında sıfat, tüzel kişiliği haiz ortaklığa aittir; ortaklık bünyesindeki avukatlar ayrıca veri sorumlusu sayılmamaktadır. Tevkil eden ile tevkil olunan avukat arasındaki ilişki kural olarak veri sorumlusu-veri işleyen ilişkisidir. Bağlı çalışan avukat, stajyer avukat ve büro personeli ise veri sorumlusunun organizasyonu içinde kaldığından ne veri sorumlusu ne de veri işleyen sıfatını taşımaktadır.

A lawyer practising independently is, as a rule, the data controller for the data of clients and third parties; it is ultimately the lawyer who decides which data will be processed and for what purpose. Lawyers working together in the same office are, notwithstanding the shared office, separate natural-person data controllers for their own clients. In a law partnership, the status belongs to the partnership, which has legal personality; the lawyers within the partnership are not separately regarded as data controllers. The relationship between the substituting lawyer and the substituted lawyer is, as a rule, one of data controller and data processor. Employed lawyers, trainee lawyers and office staff remain within the data controller's organisation and hold neither data controller nor data processor status.

Bağımsız Avukat ve Avukatlık Ortaklığı

Kurulun 22 Mart 2023 tarihli ve 2023/437 sayılı kararında, sözleşmede kullanılan nitelendirmenin tek başına belirleyici olmadığı görülmektedir. Ortaklık ile şirket arasındaki sözleşmede ortaklığın "veri işleyen" olarak nitelendirilmesine rağmen Kurul, ortaklığın "şirket tarafından kendisine aktarılan kişisel veriler üzerinde gerçekleştirilecek işleme faaliyetlerini yönettiğinin görüldüğü, bu itibarla, avukatlık faaliyetleri çerçevesinde avukatlık ortaklığının kişisel veri işleme faaliyetleri bakımından serbestçe karar verme yetkisine sahip olduğu" gerekçesiyle ortaklığı veri sorumlusu saymıştır. Buna karşılık, aşağıdaki iki kararda avukat veya avukatlık ortaklığı veri işleyen olarak nitelendirilmiştir. 9 Şubat 2021 tarihli ve 2021/115 sayılı kararda, bankanın talimatları çerçevesinde icra işlemlerini yürüten avukat veri işleyen kabul edilmiştir. 19 Ocak 2023 tarihli ve 2023/78 sayılı kararda ise borç tahsil için tek bir kısa mesaj gönderen ve numaraları doğrulama imkânı bulunmayan avukatlık ortaklığı hakkında aynı sonuca varılmıştır. Rehber bu kararları, avukata "müvekkili adına kişisel verileri işlemesi için açık, ayrıntılı ve özel talimatlar verildiği" ve avukatın amaç ile araçlar üzerinde kontrolünün bulunmadığı hâllere özgü istisnalar olarak konumlandırmaktadır.

Tevkil, Bağlı Çalışan ve Stajyer Avukatlar

Tevkil olunan avukat, kendisine yetki veren meslektaşının talimatları çerçevesinde ve yalnızca belirtilen amaçla veri işleyebilmektedir. Rehberdeki örnekte, duruşma için tevkil edilen avukatın dosyadan öğrendiği taşınmaz bilgilerini kullanarak müvekkile başka işler için vekâlet teklif etmesi, talimat sınırının aşılması ve bu faaliyet bakımından veri sorumlusu sıfatının doğması olarak değerlendirilmektedir. Bağlı çalışan avukat için de benzer bir ayrım yapılmaktadır. Tevkil ile yetkilendirilmiş olsa bile bağlı çalışan avukatın işveren avukatın organizasyonu içinde hareket ettiği kabul edilmekte; zorunlu müdafilik kapsamında kendi dosyalarını alması hâlinde ise o dosyalar bakımından bağımsız veri sorumlusu olduğu belirtilmektedir. Bu ayrım dikkate alınarak, bağlı çalışan avukatların baro görevlendirmesiyle aldıkları dosyaların büronun veri envanterinden ayrı tutulması önerilmektedir.

Independent Lawyers and Law Partnerships

The Board's decision No. 2023/437 dated 22 March 2023 shows that the characterisation used in the contract is not decisive on its own. Although the agreement between the partnership and the company described the partnership as a "data processor", the Board treated it as the data controller on the ground that "it is seen that the partnership manages the processing activities to be carried out on the personal data transferred to it by the company, and that, accordingly, within the framework of its legal practice, the law partnership has the authority to decide freely in respect of its personal data processing activities". In two other decisions, however, the Board treated the lawyer or law partnership as a data processor. In decision No. 2021/115 dated 9 February 2021, a lawyer conducting enforcement proceedings on a bank's instructions was regarded as a data processor. In decision No. 2023/78 dated 19 January 2023, the same conclusion was reached for a law partnership that sent a single text message for debt collection and had no means of verifying the numbers. The Guide positions these decisions as exceptions confined to cases in which the lawyer "has been given clear, detailed and specific instructions to process personal data on behalf of the client" and has no control over the purposes and means.

Substitution, Employed Lawyers and Trainee Lawyers

A substituted lawyer may process data only on the instructions of the colleague who granted the authority and solely for the stated purpose. In the Guide's example, a lawyer substituted for a hearing who uses immovable property information learned from the case file to offer the client representation in other matters exceeds the limits of the instruction and becomes a data controller for that activity. A similar distinction is drawn for the employed lawyer. Even where authorised by substitution, the employed lawyer is deemed to act within the organisation of the employing lawyer; where the employed lawyer takes on files under the mandatory defence counsel scheme, however, the Guide treats them as an independent data controller for those files. In view of this distinction, it is recommended that files taken on by employed lawyers through bar association assignment be kept separate from the office's data inventory.

AKTÖR ACTOR	SIFAT STATUS	DAYANAK / SINIR BASIS / LIMIT
Bağımsız avukat Independent lawyer	Veri sorumlusu (kural olarak) Data controller (as a rule)	Amaç ve araçlara son tahlilde avukat karar vermektedir The lawyer ultimately decides purposes and means
Aynı büroda çalışan avukatlar Lawyers sharing an office	Her biri ayrı gerçek kişi veri sorumlusu Each a separate natural-person data controller	Kendi müvekkilleri bakımından For their own clients
Avukatlık ortaklığı Law partnership	Tüzel kişi ortaklık veri sorumlusu The partnership (legal person) is the data controller	Ortaklık bünyesindeki avukatlar ayrıca veri sorumlusu değildir Lawyers within the partnership are not separate controllers
Tevkil olunan avukat Substituted lawyer	Veri işleyen (kural olarak) Data processor (as a rule)	Talimat sınırı aşırsa veri sorumlusu Becomes data controller if instructions are exceeded
Bağlı çalışan avukat, stajyer, büro personeli Employed lawyer, trainee, office staff	Ne veri sorumlusu ne veri işleyen Neither data controller nor data processor	Veri sorumlusunun organizasyonu içinde Within the data controller's organisation
Zorunlu müdafî olarak bağlı avukat Employed lawyer as mandatory defence counsel	0 dosyalar bakımından bağımsız veri sorumlusu Independent data controller for those files	Baro görevlendirmesi; büro envanterinden ayrı tutulması önerilmektedir Bar assignment; separate inventory recommended

KVKK KAPSAMINDAKİ SIFAT: AKTÖR BAZINDA ÖZET / STATUS UNDER THE PDPL: SUMMARY BY ACTOR

02

Kişisel Verilerin Elde Edilmesi ve Açıklanması

Obtaining and Disclosing Personal Data

Rehberin bu bölümü, avukatların müvekkil dışındaki kişilere ait verileri hangi kaynaklardan ve hangi sınırlar içinde elde edebileceğini ele almaktadır. Kurum, Avukatlık Kanunu'nun 2 nci maddesinin üçüncü fıkrasında sayılan kurumların avukata bilgi ve belge sunma yükümlülüğünü, Kanun'un 8 inci maddesi anlamında "aktanma cevaz veren bir düzenleme" olarak kabul etmektedir. Bu yetkinin sınırlı olduğu ise hem Danıştay hem Kurul kararlarıyla ortaya konulmaktadır.

The Guide also addresses how lawyers obtain third-party personal data, namely the sources from which, and the limits within which, data relating to persons other than the client may be collected. The Authority accepts the obligation of the institutions listed in the third paragraph of Article 2 of the Attorneyship Law to provide information and documents to lawyers as "a provision permitting transfer" within the meaning of Article 8 of the PDPL. Decisions of both the Council of State and the Board show, however, that this authority is not unlimited.

REHBERDEKİ AÇIKLAMA

THE GUIDE'S
EXPLANATION

Avukatın "gerek duyduğu" bilgi ve belge kavramı, Danıştay 1. Dairesi'nin 2002/26 E., 2002/52 K. sayılı kararında ifade edildiği gibi "keyfi, hiçbir nedene bağlı olmaksızın bir şeyi istemek iradesi" anlamına gelmemekte; Kanun'un 4 üncü maddesindeki amaçla bağlantılı, sınırlı ve ölçülü olma ilkesiyle örtüşmektedir. Avukatlık Kanunu'nun 2 nci maddesi genel bir hükümdür ve adli sicil kaydı gibi özel kanunla korunan verilere resen erişim yetkisi vermemektedir. Hukuka aykırı yollarla toplanmış verilerle kimlik ve iletişim bilgisi sorgulamaya yarayan yazılımların kullanılması, 2019/308 sayılı İlke Kararı gereğince avukatlar için de Kanun'un 12 nci maddesine aykırıdır.

The information and documents a lawyer "needs" do not, as stated in the decision of the First Chamber of the Council of State No. 2002/26 E., 2002/52 K., extend to "the will to demand something arbitrarily and without any reason whatsoever"; the concept coincides with the principle in Article 4 of the PDPL that processing be relevant, limited and proportionate to the purpose. Article 2 of the Attorneyship Law is a general provision and does not confer authority to access ex officio data protected by special legislation, such as criminal records. Using software that queries identity and contact information from data collected by unlawful means is, under Principle Decision No. 2019/308, contrary to Article 12 of the PDPL for lawyers as well.

UYAP ve TAKPAS Üzerinden Veri Elde Edilmesi

Kurulun 20 Mayıs 2021 tarihli ve 2021/511-512-513 sayılı kararlarına göre, takip kesinleştikten sonra alacaklı vekilinin borçlunun alacaklı olduğu dosyaları UYAP'tan sorgulaması "kanunlarda açıkça öngörülme" şartına dayanmaktadır; tevzi bürosunun bu bilgileri avukata vermesi ise Avukatlık Kanunu'nun 2 nci maddesi uyarınca hukuka uygundur. Rehber, iştirak nafakasının kaldırılması davasında davalı eski eşin taşınmaz bilgilerinin TAKPAS'tan alınmasını da "bir hakkın korunması için veri işlemenin zorunlu olması" şartı altında meşru bir örnek olarak vermektedir. Sağlık verileri bakımından Rehberde bir hatırlatma yer almaktadır: Kişisel Sağlık Verileri Hakkında Yönetmeliğin vekâletnamede özel yetki arayan 10 uncu maddesi, 3 Aralık 2025 tarihli değişiklikle yürürlükten kaldırılmıştır. Rehberdeki malpraktis örneğinde, hastanenin epikriz ve ameliyat notlarını özel yetki aramaksızın avukata teslim etmesi gerektiği belirtilmektedir.

Obtaining Data through UYAP and TAKPAS

According to the Board's decisions No. 2021/511-512-513 dated 20 May 2021, a creditor's counsel who queries on UYAP, once the enforcement proceedings have become final, the files in which the debtor is in turn a creditor relies on the condition of processing being "expressly provided for by law"; the distribution office's provision of this information to the lawyer is lawful under Article 2 of the Attorneyship Law. The Guide also cites, as a legitimate example under the condition that "processing is necessary for the protection of a right", obtaining from TAKPAS the immovable property information of the defendant former spouse in an action to remove child maintenance. On health data, the Guide contains a reminder: Article 10 of the Regulation on Personal Health Data, which required special authority in the power of attorney, was repealed by the amendment of 3 December 2025. In the Guide's malpractice example, the hospital is expected to hand over the discharge summary and surgical notes to the lawyer without requiring special authority.

Adli Sicil Kaydı ve Hukuka Aykırı Sorgulama Yazılımları

2 Kasım 2021 tarihli ve 2021/1111 sayılı kararda Kurul, Avukatlık Kanunu'nun 2 nci maddesinin Adli Sicil Kanunu'nun 7 nci maddesindeki "özel hüküm" karşısında "genel hüküm" olduğunu ve "avukatlara ilgili kişilerin adli sicil kaydı bilgilerine resen erişim yetkisi vermediği"ni belirterek avukat hakkında idari para cezası uygulamıştır. Rehberde buna iki örnek daha eklenmektedir. 28 Mayıs 2020 tarihli ve 2020/429 sayılı kararda, ilgili kişinin akraba ve iş arkadaşlarının telefon numaralarının "ihtimallere dayalı ve kesin olarak kanıtlanamayan bir şekilde" elde edilmesi idari para cezasıyla sonuçlanmıştır. 11 Mart 2021 tarihli ve 2021/228 sayılı kararda ise ilgisi olmayan bir şirkete icra takibine dair mesajlar gönderilmesi aynı yaptırma bağlanmıştır. Buna karşılık 7 Temmuz 2022 tarihli ve 2022/655 sayılı kararda, münfesiş şirketin yönetim kurulu üyeliğinin Ticaret Sicili Gazetesi'nde aleni olması ve avukatın verileri "T.C. mevzuatına uygun faaliyet yürüten yasal platformlar üzerinden" edinmiş olması nedeniyle aykırılık görülmemiştir.

Kamuya Açık Kaynaklar ve Alenileştirme

Sosyal ağlarda herkese açık paylaşılan fotoğrafların boşanma davasında delil olarak sunulması, Rehberde göre Kanun'un 5 inci maddesinin ikinci fıkrasının (d) bendi kapsamında hukuka uygundur. Bununla birlikte iki sınır belirtilmektedir: alenileştirme, kişinin "alenileştirme iradesinin varlığı"nı gerektirmekte ve veri, alenileştirme amacı dışında kullanılamamaktadır. Ticaret Sicili Gazetesi'nden ya da şirketin internet sitesinden alınan yetkili bilgileri için de aynı esas geçerlidir; bu veriler yalnızca hukuki sürecin yürütülmesi için, gerektiği kadar ve ölçülü biçimde kullanılabilir.

Borç Bilgisinin Üçüncü Kişilere Açıklanması

Kurul, 31 Mayıs 2019 tarihli ve 2019/166 sayılı kararında borçlunun ad, soyad ve hizmet numarasının yeğeni olduğu anlaşılan şikâyetçiye ait hatta gönderilmesini Kanun'un 12 nci maddesinin birinci fıkrasının (a) bendine aykırı bulmuştur. 9 Şubat 2021 tarihli ve 2021/111 sayılı kararda ise yakınına ait olduğu bilinen numaraya kısa mesaj gönderilmesi aynı hükme aykırı görülmüştür; iki dosyada da 50.000 TL idari para cezası uygulanmıştır. Rehberde, üçüncü kişilere yapılan açıklamaların tamamının hukuka aykırı olmadığı da belirtilmektedir. İcra ve İflas Kanunu'nun 89 uncu maddesi uyarınca haciz ihbarnamesi gönderilmesi ya da adi kefil müvekkilin haklarını korumak için asıl borçlunun verilerinin alacaklıya açıklanması, "bir hakkın tesisi, kullanılması veya korunması" şartına dayanabilmektedir.

Criminal Records and Unlawful Query Software

In decision No. 2021/1111 dated 2 November 2021, the Board imposed an administrative fine on a lawyer, stating that Article 2 of the Attorneyship Law is a "general provision" as against the "special provision" in Article 7 of the Criminal Records Law and that it "does not confer on lawyers the authority to access ex officio the criminal record information of data subjects". The Guide adds two further examples. In decision No. 2020/429 dated 28 May 2020, obtaining the telephone numbers of the data subject's relatives and colleagues "on the basis of probabilities and in a manner that cannot be conclusively proven" resulted in an administrative fine. In decision No. 2021/228 dated 11 March 2021, sending messages about enforcement proceedings to an unrelated company attracted the same sanction. By contrast, in decision No. 2022/655 dated 7 July 2022, no infringement was found, because membership of the dissolved company's board of directors was public in the Trade Registry Gazette and the lawyer had obtained the data "through lawful platforms operating in accordance with Turkish legislation".

Publicly Available Sources and Data Made Public

According to the Guide, submitting as evidence in divorce proceedings photographs shared publicly on social networks is lawful under Article 5(2)(d) of the PDPL. Two limits are noted, however: making data public requires "the existence of the person's intention to make it public", and the data may not be used for a purpose other than that for which it was made public. The same principle applies to information on authorised signatories taken from the Trade Registry Gazette or the company's website; such data may be used only for the conduct of the legal process, to the extent necessary and in a proportionate manner.

Disclosure of Debt Information to Third Parties

In decision No. 2019/166 dated 31 May 2019, the Board found the sending of the debtor's name, surname and service number to a line belonging to the complainant, understood to be the debtor's nephew or niece, contrary to Article 12(1)(a) of the PDPL. In decision No. 2021/111 dated 9 February 2021, sending a text message to a number known to belong to a relative was found contrary to the same provision; an administrative fine of TRY 50,000 was imposed in each file. The Guide also notes that not all disclosures to third parties are unlawful. Sending a garnishment notice under Article 89 of the Enforcement and Bankruptcy Law, or disclosing the principal debtor's data to the creditor in order to protect the rights of a client who is an ordinary surety, may rest on the condition of "the establishment, exercise or protection of a right".

03

Yurt Dışına Aktarım ve Üretken Yapay Zekâ Araçları

Transfers Abroad and Generative AI Tools

Rehber, 7499 sayılı Kanun'la değişen 9 uncu maddedeki üç kademeli sistemi (yeterlilik kararı, uygun güvenceler, anzi aktarım hâlleri) aktarmaktadır. Ardından müvekkil dosyalarının ChatGPT, Claude ya da Gemini gibi üretken yapay zekâ araçlarına yüklenmesi, kişisel veri aktarımı bakımından değerlendirilmektedir.

The Guide sets out the three-tier system in Article 9, as amended by Law No. 7499 (adequacy decision, appropriate safeguards, and cases of incidental transfer). It then considers the data transfer implications of uploading client documents to generative AI tools such as ChatGPT, Claude or Gemini.

REHBERDEKİ AÇIKLAMA

THE GUIDE'S EXPLANATION

Yapay zekâ aracına kişisel veri içeren belge yüklenmesi "yalnızca teknik destek alınması veya hukuki araştırma yapılması olarak değerlendirilmemelidir". Hizmet sağlayıcının mukim olduğu ülke, sunucuların bulunduğu yer ve alt hizmet sağlayıcıların konumu dikkate alındığında bu işlem, Kanun'un 9 uncu maddesi anlamında yurt dışına aktarım teşkil edebilmektedir. Sağlayıcı yurt içinde olsa bile belgelerin ona aktarılması, Kanun'un 8 inci maddesi kapsamında bir aktarımdır.

Uploading a document containing personal data to an AI tool "should not be regarded merely as obtaining technical support or conducting legal research". Having regard to the country in which the service provider is resident, the location of the servers and the location of sub-service providers, this operation may constitute a transfer abroad within the meaning of Article 9 of the PDPL. Even where the provider is located within Türkiye, the transfer of documents to it is a transfer within the scope of Article 8 of the PDPL.

Üretken Yapay Zekâ Kullanımında Veri Güvenliği Tedbirleri

Veri güvenliği bölümünde Rehber, yapay zekâ araçları için somut bir tedbir listesi sunmaktadır. Bu tedbirler arasında kişisel verilerin mümkün olduğunca

Data Security Measures for Generative AI Use

In its data security chapter, the Guide offers a concrete list of measures for AI tools. These include masking or anonymising personal data wherever possible, not

maskelenmesi veya anonimleştirilmesi, özel nitelikli kişisel verilerin sisteme yüklenmemesi ve yalnızca amaç için gereken asgari verinin paylaşılması yer almaktadır. Ayrıca kullanılan aracın veri saklama, model eğitimi, insan incelemesi ve alt işleyen politikalarının okunması ile büro içinde yazılı kullanım kurallarının belirlenmesi önerilmektedir. Kurum bu bölümde, Şubat 2026 tarihli İşyerlerinde Üretken Yapay Zekâ Araçlarının Kullanımı ve Kasım 2025 tarihli Üretken Yapay Zekâ ve Kişisel Verilerin Korunması Rehberi gibi önceki yayınlarına da atıf yapmaktadır.

uploading special categories of personal data to the system, and sharing only the minimum data required for the purpose. The Guide further recommends reading the data retention, model training, human review and sub-processor policies of the tool used, and laying down written rules of use within the office. In this chapter the Authority also refers to its earlier publications, such as the February 2026 publication on the Use of Generative AI Tools in the Workplace and the November 2025 Guide on Generative AI and the Protection of Personal Data.

04

Veri Sorumlusu Avukatın Yükümlülükleri

Obligations of the Lawyer as Data Controller

Rehberde, sicile kayıt istisnasının kapsamı açıklanmaktadır. Avukatların Kurulun 2 Nisan 2018 tarihli ve 2018/32 sayılı kararıyla Veri Sorumlular Siciline kayıttan istisna tutulması, uygulamada "avukatların 6698 sayılı Kanun kapsamında yükümlülüklerinin bulunmadığı" şeklinde anlaşılmıştır. Kurum bu anlayışın doğru olmadığını ve istisnanın yalnızca Sicile kayıt ve bildirim yükümlülüğüyle sınırlı kaldığını vurgulamaktadır.

The Guide explains the scope of the exemption from registration. The exemption of lawyers from registration with the Data Controllers' Registry by the Board's decision No. 2018/32 dated 2 April 2018 has been understood in practice as meaning that "lawyers have no obligations under Law No. 6698". The Authority emphasises that this understanding is incorrect and that the exemption is confined to registration with, and notification to, the Registry.

REHBERDEKİ AÇIKLAMA

THE GUIDE'S
EXPLANATION

Veri doğrudan ilgili kişiden alınmamışsa aydınlatma en geç ilk iletişim veya ilk aktarım anında yapılmalı ve hukuki yardım talebinin alınmasından danışmanlık sürecine kadar kademeli olarak uygulanmalıdır. Silme ve imha talepleri, Avukatlık Kanunu'nun 39 uncu maddesindeki üç yıllık evrak saklama yükümlülüğü ve olası sorumluluk süreçleriyle birlikte değerlendirilmelidir; talep reddedilirse saklama yükümlülüğünün dayanağı ve süresi ilgili kişiye açıkça yazılı olarak bildirilmelidir. Kurula gelen şikâyetlerin büyük bölümü "kişisel verilerinin avukatlar tarafından ne suretle elde edildiğini bilmek isteme" noktasında toplandığından, verinin kaynağının hem ilgili kişiye hem Kurula belgelenebilmesi önem taşımaktadır.

Where data has not been obtained directly from the data subject, the privacy notice must be provided at the latest at the moment of first contact or first transfer, and applied in stages from receipt of the request for legal assistance through to the advisory process. Requests for erasure and destruction must be assessed together with the three-year document retention obligation under Article 39 of the Attorneyship Law and possible liability proceedings; where a request is refused, the basis and duration of the retention obligation must be set out clearly in writing to the data subject. Since most complaints reaching the Board centre on "wishing to know by what means their personal data was obtained by lawyers", being able to document the source of the data both to the data subject and to the Board is important.

İlgili Kişi Başvuruları ve Erişilebilirlik

Rehberdeki örnekte, hakkında icra takibi başlatılan kişi alacaklı vekiline başvurduğunda avukatın verilerin "müvekkil tarafından mı, icra dosyasından mı, kamu kurumlarından mı yoksa kamuya açık kaynaklardan mı elde edildiğini" açıklaması beklenmektedir. Rehberde ayrıca iletişim bilgilerinin güncelliğine ilişkin bir açıklama yer almaktadır: internet sitesi olan büroların sitedeki iletişim bilgilerini, olmayan avukatların ise baro levhasındaki bilgilerini güncel tutması gerekmektedir. Aksi hâlde başvuru avukata ulaşmadığından otuz günlük cevap süresi kaçınılmamaktadır.

Data Subject Applications and Accessibility

In the Guide's example, when a person against whom enforcement proceedings have been initiated applies to the creditor's counsel, the lawyer is expected to explain whether the data was obtained "from the client, from the enforcement file, from public institutions or from publicly available sources". The Guide also addresses keeping contact details current: offices with a website must keep the contact details on the site up to date, and lawyers without one must keep the details on the bar association roll up to date. Otherwise, the thirty-day period for responding may be missed because the application never reaches the lawyer.

Veri İhlali Bildirimi ve İlan Süresi

Rehber, adliye dönüşünde kaybedilen dava dosyası örneği üzerinden, avukatın etkilenen kişi ve veri kategorilerini değerlendirip 2019/10 sayılı Kurul karar uyanca yetmiş iki saat içinde Kurula bildirimde bulunması gerektiğini açıklamaktadır. Kurulun 25 Aralık 2025 tarihli ve 2025/2451 sayılı kararıyla ihlal ilanlarının altmış güne sınırlandırıldığı ve ilgili kişilere daha erken bildirim yapıldığının belgelenmesi hâlinde ilanın kaldırılacağı da hatırlatılmaktadır. Veri güvenliği yükümlülüğünün ihlali için 2026 yılında uygulanacak idari para cezası aralığı Rehberde 256.357 TL ile 17.092.242 TL olarak belirtilmiştir.

Data Breach Notification and the Announcement Period

Using the example of a case file lost on the way back from the courthouse, the Guide explains that the lawyer must assess the affected persons and data categories and notify the Board within seventy-two hours under Board decision No. 2019/10. It also recalls that, by the Board's decision No. 2025/2451 dated 25 December 2025, breach announcements are limited to sixty days and are removed where it is documented that the data subjects were notified earlier. The Guide states the range of administrative fines applicable in 2026 for breach of the data security obligation as TRY 256,357 to TRY 17,092,242.

05

Veri İşleyen Kaynaklı İhlaller ve Fidyeye Yazılımı Kararları

Breaches at Data Processors and Ransomware Decisions

Kurul, 16 Eylül 2026 tarihli ve 2026/2039 sayılı karar ile 23 Eylül 2026 tarihli ve 2026/2081 sayılı kararla, ortak bir veri işleyenin sistemlerinde yaşanan yetkisiz erişimden etkilenen çok sayıda veri sorumlusunun ihlal bildirimlerini Kurum internet sitesinde ilan etmiştir. Bildirimlerin büyük bölümünde aynı ifade yer almaktadır: ihlal, "veri işleyen sistemlerindeki bir sunucuya, kullanılan üçüncü taraf yazılım kütüphanesindeki güvenlik zafiyetinin istismar edilmesi suretiyle yetkisiz erişim sağlanması" sonucunda gerçekleşmiş ve veri sorumluları bunu 10 Eylül 2026 tarihinde veri işleyenin bildirimiyle öğrenmiştir.

Kişisel verilerin bir veri işleyen aracılığıyla işlenmesi hâlinde, gerekli güvenlik tedbirlerinin alınmasından veri sorumlusu ile veri işleyen müştereken sorumludur (KVKK m. 12/2). İhlalin Kurula ve ilgili kişilere bildirilmesi yükümlülüğü ise Kanun'un 12 nci maddesinin beşinci fıkrası uyarınca veri sorumlusuna aittir; bu nedenle ortak bir veri işleyenden kaynaklanan ihlalde, etkilenen veri sorumluları kendi ilgili kişileri için ayrı ayrı bildirimde bulunmaktadır. Veri güvenliği yükümlülüğünün ihlali nedeniyle öngörülen idari para cezası da Kanun'un 18 inci maddesi uyarınca veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanmaktadır.

By its decision No. 2026/2039 dated 16 September 2026 and its decision No. 2026/2081 dated 23 September 2026, the Board announced on the Authority's website the breach notifications of a large number of data controllers affected by unauthorised access to the systems of a shared data processor. Most of the notifications contain the same wording: the breach occurred as a result of "unauthorised access to a server in the data processor's systems through the exploitation of a security vulnerability in a third-party software library in use", and the data controllers learned of it on 10 September 2026 through the data processor's notification.

Where personal data is processed on behalf of the controller by a data processor, the controller and the processor are jointly responsible for taking the necessary security measures (Article 12(2) of the PDPL). The obligation to notify the breach to the Board and to the data subjects rests, under Article 12(5), with the data controller; in a breach originating from a shared processor, the affected controllers therefore each notify separately for their own data subjects. The administrative fine for breach of the data security obligation is, under Article 18, imposed on data controllers that are natural persons or private-law legal persons.

KURULUN DEĞERLENDİRMESİ

THE BOARD'S ASSESSMENT

Fidyeye yazılımı saldırılarına ilişkin incelenen kararlarda, veri sorumlusunun etkilenen kişi ve veri kategorileri hakkında çelişkili beyanlarda bulunması, ihlale konu belge örneklerini ve kişisel veri işleme envanterini Kuruma sunmaması, log kayıtlarına ulaşılabilmesi ve ağ segmentasyonunun yapılmamış olması, Kanun'un 12 nci maddesi kapsamında teknik ve idari tedbirlerin alınmadığını gösteren olgular olarak değerlendirilmiştir.

In the ransomware decisions examined, the Board treated the controller's contradictory statements about the affected persons and data categories, its failure to submit to the Authority sample documents affected by the breach and its personal data processing inventory, the unavailability of log records and the absence of network segmentation as facts showing that the technical and organisational measures required by Article 12 of the PDPL had not been taken.

Perakende ve E-Ticaret Sektöründe Toplu İhlal Bildirimleri

En geniş kapsamlı bildirim Yeni Mağazacılık A.Ş.'ye aittir ve Eve Kozmetik müşterilerine ilişkin 6.263.305 kişiyi kapsamaktadır. Bildirimde, Eve Mağazacılık'ın Yeni Mağazacılık ile birleşmiş olmasına rağmen sistemlerin ayrı tutulduğu ve ihlalin yalnızca Eve Kozmetik müşterilerinin ad, soyad, e-posta ve telefon bilgilerini kapsadığı belirtilmiştir. Shaya Mağazacılık A.Ş., 2.298.726 çalışan ve müşterinin ad, soyad, e-posta ve adres bilgilerinin etkilendiğini bildirmiştir. Samsonite Seyahat Ürünleri ise kimlik ve iletişim bilgilerinin yanı sıra "hesap kimlik doğrulama bilgilerinin (saklanan şifre değerleri)" sızdığını açıklamıştır. Desa Deri, Bilen Mağazaları, Locco Elektronik ve çok sayıda hazır giyim, kozmetik ve elektronik perakendecisi aynı kaynaklı bildirimlerde bulunmuştur. Yazarların değerlendirmesine göre bu bildirimler, e-ticaret altyapısını dışarıdan alan veri sorumluları bakımından veri işleyen sözleşmelerindeki güvenlik, denetim ve ihlal bildirim hükümlerinin uygulamada nasıl yerine getirildiğinin incelenmesini gerektirmektedir.

Yurt Dışında Yerleşik Veri Sorumlusu ve Meslek Kuruluşu Bildirimleri

Canva Pty Ltd, üçüncü taraf bir araçtaki yetkisiz erişim sonucu Türkiye'deki 424 organizasyonla ilişkili verilerin etkilendiğini bildirmiştir; etkilenen veriler, müşteri çalışanlarına ait iş e-posta adresleri ve telefon numaraları ile sözleşme, fatura ve veri koruma anlaşmalarıdır. Kurul, bu bildirimin ilanına 16 Eylül 2026 tarihli ve 2026/2037 sayılı kararla karar vermiştir. Vergi Mükellefleri Demeği'nin 23 Eylül 2026 tarihli ve 2026/2082 sayılı kararla ilan edilen bildiriminde ise veri işleyen sistemlerine yetkisiz erişim sonucu azami 9.462 üyenin T.C. kimlik numarası, doğum tarihi, parola ve iletişim bilgilerinin etkilendiği belirtilmiştir. Kimlik numarası ile parolanın aynı sistemde tutulduğu üyelik yapılarında, veri işleyen nezdindeki güvenlik zafiyeti Kanun'un 12 nci maddesinin ikinci fıkrası uyarınca veri sorumlusunun da müştereken sorumlu olduğu bir alana ilişkindir. Yazarların

Mass Breach Notifications in Retail and E-Commerce

The most extensive notification is that of Yeni Mağazacılık A.Ş., covering 6,263,305 persons among Eve Kozmetik customers. The notification states that, although Eve Mağazacılık had merged with Yeni Mağazacılık, the systems were kept separate and the breach covered only the name, surname, e-mail and telephone details of Eve Kozmetik customers. Shaya Mağazacılık A.Ş. reported that the name, surname, e-mail and address details of 2,298,726 employees and customers were affected. Samsonite Seyahat Ürünleri disclosed that, in addition to identity and contact details, "account authentication information (stored password values)" had been leaked. Desa Deri, Bilen Mağazaları, Locco Elektronik and numerous apparel, cosmetics and electronics retailers made notifications arising from the same source. In the authors' assessment, these notifications call for controllers that outsource their e-commerce infrastructure to examine how the security, audit and breach notification clauses of their data processor agreements are performed in practice.

Notifications by a Controller Established Abroad and a Professional Association

Canva Pty Ltd reported that, following unauthorised access to a third-party tool, data associated with 424 organisations in Türkiye had been affected; the affected data comprised the business e-mail addresses and telephone numbers of customer employees together with contracts, invoices and data protection agreements. The Board resolved to announce the notification by its decision No. 2026/2037 dated 16 September 2026. The notification of the Association of Tax Inspectors, announced by decision No. 2026/2082 dated 23 September 2026, states that the Turkish identity numbers, dates of birth, passwords and contact details of up to 9,462 members were affected following unauthorised access to data processor systems. In membership structures where the identity number and the password are held in the same system, a security vulnerability at the processor concerns an area for which the controller is jointly responsible under Article 12(2) of

değerlendirmesine göre bu tür yapılarda veri işleyenin güvenlik tedbirlerinin veri sorumlusunca denetlenmesi ayrı bir önem taşımaktadır.

Fidye Yazılımı Saldırılarında Çelişkili Beyanlar ve Alınmayan Tedbirler

Bu notta incelenen fidye yazılımı kararları 2024 tarihli olup Kurumun yayımladığı karar özetleri arasında yer almaktadır. Kurulun 26 Aralık 2024 tarihli ve 2024/2196 sayılı kararına konu olayda, plastik ev gereçleri üreten bir şirketin sistemleri fidye yazılımıyla şifrelenmiştir. Şirket ilk bildiriminde çalışan ve müşteri verilerinin etkilendiğini bildirmiş, sonraki yazılarında hiçbir kişisel verinin etkilendiğini beyan etmiş, suç duyurusu dilekçesinde ise verilerin saldırganlarca ele geçirildiğini kabul etmiştir. Kurul bu üç beyanı birlikte değerlendirerek çelişkiyi ortaya koymuştur. Kurul, "tüzel kişiye ait bir verinin herhangi bir gerçek kişiyi belirlemesi ya da belirlenebilir kılması halinde bu verilerin de Kanun kapsamında koruma altında olduğu"nu hatırlatarak, fatura bilgilerinin kişisel veri olmadığı iddiasının belge örneği sunulmadan kabul edilemeyeceğini belirtmiştir. Güvenlik açığı testinde bulgu çıkmamasına rağmen sisteme girilebilmesi testin yetersizliğine; iki faktörlü doğrulamanın ancak ihalden sonra açılması ve dokuz şirketin birden etkilenmesi ise ağ segmentasyonunun yokluğuna bağlanmıştır. Kurul, veri sorumlusu hakkında 250.000 TL idari para cezası uygulanmasına karar vermiştir.

Herkese Açık Klasörler ve Uzak Masaüstü Servisleri

7 Kasım 2024 tarihli ve 2024/1899 sayılı kararda, Avrupa'daki grup şirketlerine kurumsal destek hizmeti veren bir şirketin pazarlama amaçlı kullanıcı hesabı kara listedeki bir IP adresinden ele geçirilmiştir. Saldırgan "herkese açık" olarak ayarlanmış klasörlere ve FTP sunucusuna erişmiş; yaklaşık 70.000 kişinin verisi etkilendirilmiştir. Kurul, ihlalin başlangıç tarihinin dahi belirlenememesini ve erişim günlüklerinin ihlal öncesinde yalnızca doksan gün saklanması takip ve kontrol eksikliği olarak değerlendirmiş ve 700.000 TL idari para cezası uygulanmasına karar vermiştir. Aynı tarihli 2024/1898 sayılı karar ise ilaç ve sağlık ürünleri alanındaki bir şirkete ilişkindir. Bu olayda sunucu fidye yazılımıyla şifrelenmiş; karar özetinde ihalden 520 kişinin etkilendiği belirtilmiştir. İnternete açık olmaması gereken uzak masaüstü servisi üzerinden kaba kuvvet yöntemiyle giriş yapılmış olabileceği ve sunucu log kayıtlarının silindiği dikkate alınarak 350.000 TL idari para cezası uygulanmıştır. İki kararda da Kişisel Veri Güvenliği Rehberi'nin "Kişisel Veri Güvenliğinin Takibi" başlığındaki log tutma, erişim yetki matrisi ve güçlü parola ilkeleri, yaptırımın somut ölçütü olarak kullanılmıştır.

the PDPL. In the authors' assessment, the controller's oversight of the processor's security measures carries particular weight in such structures.

Contradictory Statements and Measures Not Taken in Ransomware Attacks

The ransomware decisions examined in this note date from 2024 and appear among the decision summaries published by the Authority. In the incident that was the subject of the Board's decision No. 2024/2196 dated 26 December 2024, the systems of a company manufacturing plastic household goods were encrypted by ransomware. In its initial notification the company stated that employee and customer data had been affected; in subsequent letters it declared that no personal data had been affected; and in its criminal complaint it admitted that the data had been seized by the attackers. Considering these three statements together, the Board identified the contradiction. Recalling that "where data belonging to a legal person identifies or renders identifiable any natural person, such data is likewise protected under the Law", the Board stated that the claim that invoice details were not personal data could not be accepted without sample documents being submitted. The penetration of the system despite a vulnerability test producing no findings was attributed to the inadequacy of the test; the enabling of two-factor authentication only after the breach, and the fact that nine companies were affected at once, were attributed to the absence of network segmentation. The Board resolved to impose an administrative fine of TRY 250,000 on the data controller.

Publicly Accessible Folders and Remote Desktop Services

In decision No. 2024/1899 dated 7 November 2024, the marketing user account of a company providing corporate support services to its group companies in Europe was compromised from a blacklisted IP address. The attacker accessed folders set to "public" and the FTP server, and the data of approximately 70,000 persons was affected. The Board treated the inability to determine even the start date of the breach, and the retention of access logs for only ninety days before the breach, as a deficiency in monitoring and control, and resolved to impose an administrative fine of TRY 700,000. Decision No. 2024/1898 of the same date concerns a company in the pharmaceutical and health products field. In that incident the server was encrypted by ransomware; the decision summary states that 520 persons were affected. Having regard to the possibility that entry was gained by brute force through a remote desktop service that should not have been exposed to the internet, and to the deletion of the server log records, an administrative fine of TRY 350,000 was imposed. In both decisions, the log-keeping, access authorisation matrix and strong password principles under the heading "Monitoring of Personal Data Security" in the Personal Data Security Guide served as the concrete criteria for the sanction.

DOSYA FILE	KARAR DECISION	ETKİLENEN AFFECTED	SONUÇ OUTCOME
Yeni Mağazacılık (Eve Kozmetik) Yeni Mağazacılık (Eve Kozmetik)	2026/2039 - 2026/2081 2026/2039 - 2026/2081	6.263.305 kişi 6,263,305 persons	İlan; veri işleyen kaynaklı Announced; processor-originated
Shaya Mağazacılık Shaya Mağazacılık	2026/2039 - 2026/2081 2026/2039 - 2026/2081	2.298.726 çalışan ve müşteri 2,298,726 employees and customers	İlan; veri işleyen kaynaklı Announced; processor-originated
Canva Pty Ltd Canva Pty Ltd	2026/2037 2026/2037	Türkiye'de 424 organizasyon 424 organisations in Türkiye	İlan; üçüncü taraf araç Announced; third-party tool
Vergi Müfettişleri Derneği Association of Tax Inspectors	2026/2082 2026/2082	Azami 9.462 üye Up to 9,462 members	İlan; kimlik no. ve parola Announced; identity number and password
Plastik ev gereçleri üreticisi Plastic household goods manufacturer	2024/2196 2024/2196	Çalışan ve müşteri verileri Employee and customer data	250.000 TL; çelişkili beyan, segmentasyon yok TRY 250,000; contradictory statements, no segmentation
Kurumsal destek şirketi Corporate support company	2024/1899 2024/1899	Yaklaşık 70.000 kişi Approximately 70,000 persons	700.000 TL; herkese açık klasör, kısa log saklama TRY 700,000; public folders, short log retention
İlaç ve sağlık ürünleri şirketi Pharmaceutical and health products company	2024/1898 2024/1898	520 kişi 520 persons	350.000 TL; uzak masaüstü, silinen log TRY 350,000; remote desktop, deleted logs

VERİ İŞLEYEN KAYNAKLI İHLAL İLANLARI VE FİDYE YAZILIMI KARARLARI / PROCESSOR-ORIGINATED BREACH ANNOUNCEMENTS AND RANSOMWARE DECISIONS

06

Kurumun Diğer Duyuruları

The Authority's Other Announcements

Kurumun 10 Eylül 2026 tarihli Seçilmiş Güncel Gelişmeler bülteninde aşağıdaki gelişmeler yer almaktadır. 6 Eylül 2026 tarihli Resmî Gazete'de yayımlanan Orta Vadeli Program (2027-2029), 6698 sayılı Kanun'un Avrupa Birliği Genel Veri Koruma Tüzüğü ile uyumlaştırılmasının 2027 yılının üçüncü çeyreğinde tamamlanmasını öngörmektedir. Kurum ayrıca Kamu Kurum ve Kuruluşları ile Kamu Kurumu Niteliğindeki Meslek Kuruluşları için Kişisel Verilerin Korunması Kanununa Uyum Rehberi'ni yayımlamıştır. 18 Ağustos 2026 tarihli Resmî Gazete'de ise Türkiye Yapay Zekâ Eylem Planı (2026-2030) genelgesi yer almıştır. Kurul karar özetleri ve ilke kararları bölümlerinde 10 Ağustos 2026 tarihli yayından bu yana yeni bir içerik bulunmamaktadır.

The Authority's Selected Recent Developments bulletin of 10 September 2026 records the following developments. The Medium-Term Programme (2027-2029), published in the Official Gazette of 6 September 2026, envisages that the alignment of Law No. 6698 with the European Union General Data Protection Regulation will be completed in the third quarter of 2027. The Authority has also published the Guide on Compliance with the Personal Data Protection Law for Public Institutions and Organisations and Professional Organisations with Public Institution Status. The circular on the Türkiye Artificial Intelligence Action Plan (2026-2030) appeared in the Official Gazette of 18 August 2026. In the Board decision summaries and principle decisions sections, there has been no new content since the publication of 10 August 2026.

GENEL DEĞERLENDİRME VE SONUÇ / ASSESSMENT AND CONCLUSION

YAZARLARIN DEĞERLENDİRMESİ / AUTHORS' ASSESSMENT

İncelenen rehber ve kararlar birlikte okunduğunda iki öncelikli uyum adımı öne çıkmaktadır: avukatın işlediği verinin kaynağının belgelenmesi ve veri işleyen sözleşmelerindeki güvenlik ve bildirim hükümlerinin uygulamada izlenmesi.

Read together, the Guide and the decisions examined point to two priority compliance steps: documenting the source of the data a lawyer processes, and monitoring in practice the security and notification clauses of data processor agreements.

Rehber, avukatlık faaliyetlerindeki veri işleme süreçlerini mevcut Kurul kararlarıyla birlikte ele almakta ve avukatın sıfatından yapay zekâ araçlarının kullanımına kadar uzanan konulan sistematik biçimde açıklamaktadır. Yazarların değerlendirmesine göre Rehberin uygulama bakımından öne çıkan bir sonucu, sicil kaydından istisnanın diğer yükümlülüklerden muafiyet anlamına gelmediğinin açıkça belirtilmesidir. Bu açıklama karşısında hukuk bürolarının aydınlatma, saklama ve imha, başvuru ve ihlal bildirim süreçlerini yazılı politikalara bağlaması önerilmektedir. Kurula gelen şikâyetlerin verinin kaynağı noktasında yoğunlaşması, bu politikalar içinde verinin nereden elde edildiğini gösteren bir kayıt düzenine öncelik verilmesini gerektirmektedir. Üretken yapay zekâ araçları için ise Rehberdeki tedbir listesinin büro içi yazılı kurallara dönüştürülmesi yeterli bir başlangıç noktası olarak görülmektedir.

İhlal ilanları ve bu notta incelenen 2024 tarihli fidye yazılımı kararları ise veri işleyen kaynaklı ihlallerde sorumluluğun paylaşımını göstermektedir. Güvenlik tedbirlerinden veri sorumlusu ile veri işleyen müştereken sorumlu olmakla birlikte, bildirim yükümlülüğü ve idari para cezası veri sorumlusu üzerinde toplanmaktadır; incelenen kararlarda çelişkili beyanlar, sunulmayan envanter ve belgeler ile bulunmayan log kayıtları cezanın gerekçesi olarak kullanılmıştır. Yazarların değerlendirmesine göre bu durum, veri işleyen sözleşmelerini ve olay müdahale planlarını uyum programlarının öncelikli unsurları arasında taşımaktadır. Netice itibarıyla hukuk bürolarının, Rehberdeki açıklamaları yazılı politikalara ve verinin kaynağını gösteren bir kayıt düzenine dönüştürmesi önerilmektedir. E-ticaret ya da üyelik altyapısını dışardan alan veri sorumlularının ise veri işleyen denetimini, ağ segmentasyonunu, log saklama sürelerini ve yetmiş iki saatlik bildirim akışını bu notta incelenen kararlar ışığında gözden geçirmesi yerinde olacaktır.

The Guide addresses the data processing operations involved in legal practice together with the Board's existing decisions and explains systematically matters ranging from the lawyer's status to the use of AI tools. In the authors' assessment, one consequence of the Guide that stands out for practice is its express statement that exemption from registration does not mean exemption from other obligations. In the light of that statement, law firms are advised to set their privacy notice, retention and destruction, application and breach notification processes down in written policies. Since the complaints reaching the Board concentrate on the source of the data, those policies should give priority to a record-keeping system that shows where each item of data was obtained. For generative AI tools, converting the Guide's list of measures into written in-house rules is regarded as a sufficient starting point.

The breach announcements and the 2024 ransomware decisions examined in this note show how liability is allocated for breaches at data processors. Although the controller and the processor are jointly responsible for security measures, the notification obligation and the administrative fine fall on the controller; in the decisions examined, contradictory statements, unsubmitted inventories and documents, and missing log records were the grounds for the fine. In the authors' assessment, this places data processor agreements and incident response plans among the priority elements of a compliance programme. In conclusion, law firms are advised to translate the Guide's explanations into written policies and a record-keeping system that shows the source of the data. Controllers that outsource their e-commerce or membership infrastructure would do well to review their processor audits, network segmentation, log retention periods and seventy-two-hour notification workflow in the light of the decisions examined in this note.

ATIF YAPILAN MEVZUAT VE KARARLAR / LEGISLATION AND DECISIONS CITED

6698 sayılı Kişisel Verilerin Korunması Kanunu m. 4, 5/2(d), 8, 9, 12/1(a), 12/2, 12/5, 18 · 7499 sayılı Kanun · 1136 sayılı Avukatlık Kanunu m. 2/3, 39 · 5352 sayılı Adli Sicil Kanunu m. 7 · 2004 sayılı İcra ve İflas Kanunu m. 89 · Kişisel Sağlık Verileri Hakkında Yönetmelik m. 10 · KVKK Yayınları No. 115 (Uygulama Rehberi) · Kurul kararları 2018/32, 2019/10, 2019/166, 2019/308 (İlke Kararı), 2020/429, 2021/111, 2021/115, 2021/228, 2021/511-512-513, 2021/1111, 2022/655, 2023/78, 2023/437, 2024/1898, 2024/1899, 2024/2196, 2025/2451, 2026/2037, 2026/2039, 2026/2081, 2026/2082 · Danıştay 1. D. 2002/26 E., 2002/52 K.

Law No. 6698 on the Protection of Personal Data, Arts. 4, 5/2(d), 8, 9, 12/1(a), 12/2, 12/5, 18 · Law No. 7499 · Attorneyship Law No. 1136, Arts. 2/3, 39 · Criminal Records Law No. 5352, Art. 7 · Enforcement and Bankruptcy Law No. 2004, Art. 89 · Regulation on Personal Health Data, Art. 10 · PDPA Publication No. 115 (Implementation Guide) · Board decisions 2018/32, 2019/10, 2019/166, 2019/308 (Principle Decision), 2020/429, 2021/111, 2021/115, 2021/228, 2021/511-512-513, 2021/1111, 2022/655, 2023/78, 2023/437, 2024/1898, 2024/1899, 2024/2196, 2025/2451, 2026/2037, 2026/2039, 2026/2081, 2026/2082 · Council of State, 1st Chamber, E. 2002/26, K. 2002/52

İşbu makale genel bilgilendirme amacıyla hazırlanmış olup hukuki tavsiye niteliği taşımamaktadır. Makalede anılan kurul kararları, rehber ve duyurular yayın tarihi itibarıyla ilgili kurumların internet sitelerinde kamuya açık kaynaklara dayanmaktadır; karar özetlerinde yer alan tespitler Kurulların değerlendirmesi olup Devin Law & IP'nin görüşünü yansıtmaz. İşbu yazı avukat ile müvekkil arasında bir ilişki kurmamakta ve güncellenmesi hususunda herhangi bir taahhüt içermemektedir. 28 Eylül 2026.

This article has been prepared for general information purposes only and does not constitute legal advice. The board decisions, guides and announcements referred to are based on sources published on the relevant authorities' websites as at the date of publication; findings recorded in decision summaries are those of the Boards and do not reflect the views of Devin Law & IP. This article does not create an attorney-client relationship and contains no undertaking as to its updating. 28 September 2026.