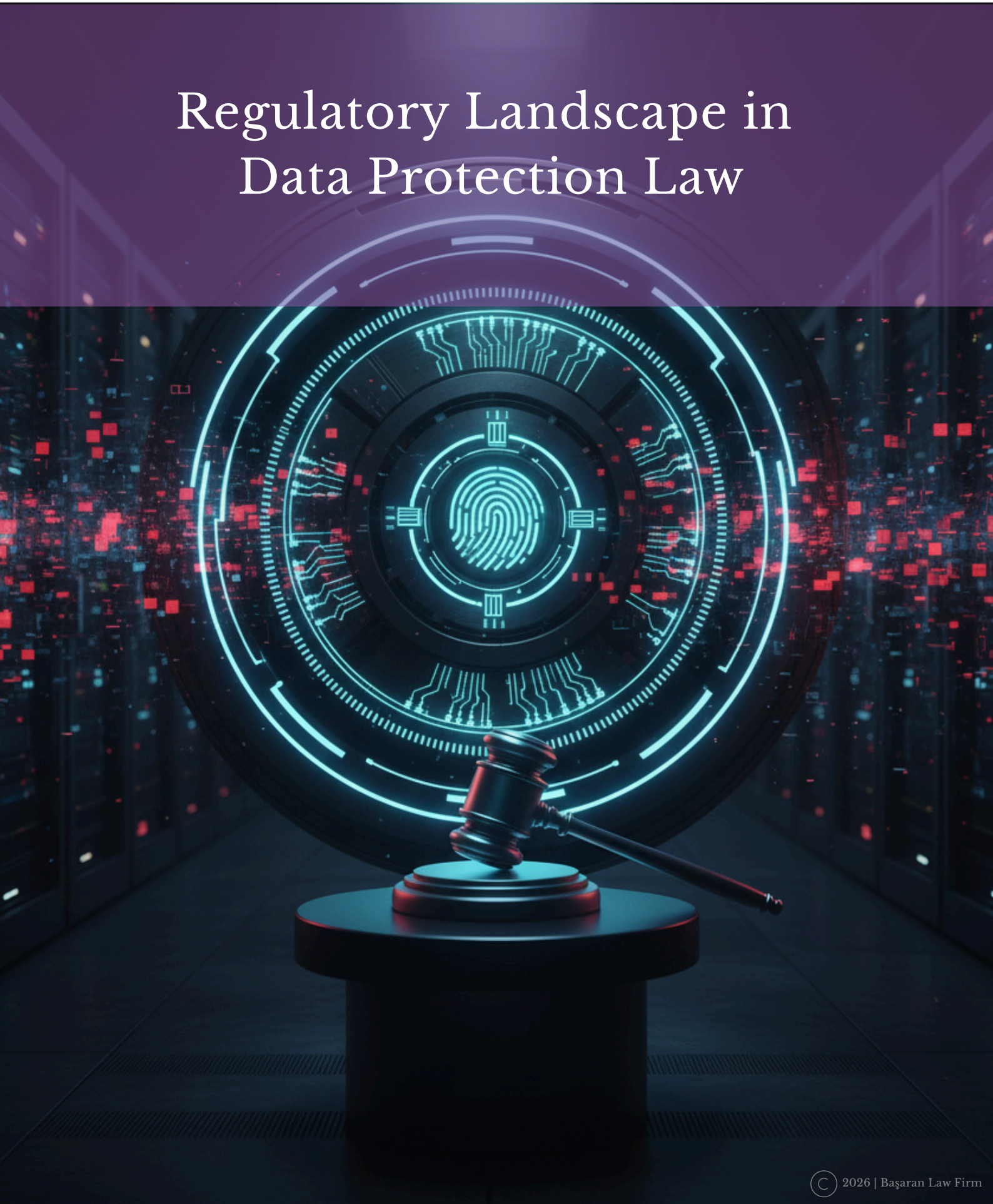
THE PULSE

BAŞARAN LAW FIRM

February 2026
Edition: 06

Regulatory Landscape in Data Protection Law



© 2026 | Başaran Law Firm

A New Era in Data Flows Between the European Union and Brazil

The European Union and Brazil have formally adopted mutual adequacy decisions in the field of personal data protection. This development is based on the determination that both parties ensure equivalent and adequate levels of data protection, enabling the secure and free flow of personal data between them.

With the publication of the decisions, personal data may now flow reciprocally between the European Union and Brazil without the need for additional transfer mechanisms or contractual safeguards. This development is set to create the world's largest "safe and free data flow area," covering approximately 670 million consumers.

On the EU side, the decision was implemented by the European Commission under the General Data Protection Regulation (GDPR) through an implementing act. On the Brazilian side, a parallel measure was adopted by the National Data Protection Authority (ANPD), established under the Brazilian General Data Protection Law (LGPD), recognizing the EU's data protection regime as adequate.

The European Commission stated that the decision will strengthen trade relations, support the digital economy, and reduce legal uncertainty for businesses.

The arrangement is also viewed as part of the broader framework of historic partnership agreements between the EU and Mercosur and is considered a significant milestone in the harmonization of global data protection standards.

Critical Updates from the ICO on Transfers, Access, and Enforcement

The beginning of 2026 witnessed notable developments in the United Kingdom's data protection regime. The country's data protection authority, the Information Commissioner's Office (ICO), updated its guidance and took important steps regarding its enforcement approach. At the center of these developments is the Data (Use and Access) Act 2025 a major reform of the UK data protection framework adopted in 2025.

Update to the Right of Access Guidance: As part of its alignment with the DUAA, the ICO updated its guidance on data subjects' right of access (DSAR). The revision clarifies the scope of "manifestly unfounded" access requests and emphasizes that organizations must adopt a "reasonable and proportionate" approach when responding to such requests.

Three-Step Test for International Data Transfers: The ICO also significantly simplified and clarified its guidance on international data transfers under the UK GDPR. The updated text introduces a three-step test to help organizations determine whether they are making a "restricted transfer."

A New Contractual Location-Based Approach: One of the most notable changes in the guidance is the shift from a geographically focused assessment to one based on contractual location. According to the ICO, what matters is not where the data is physically stored, but the country in which the recipient organization is legally established.

Under this approach, a restricted transfer may arise even if the data does not physically leave the UK, provided that the contractual counterparty is established in a third country deemed "not adequate." Conversely, if the contractual party is established in the UK, a restricted transfer may not occur even where data is hosted on servers located abroad.

Memorandum of Understanding Between the ICO and the UK Government: On 8 January, the ICO and the UK Government signed a Memorandum of Understanding aimed at strengthening cooperation in the field of data security. The agreement seeks to promote the secure development of data use in public services and to ensure that systemic lessons are learned from data breaches.

Section 138 of the DUAA Enters into Force: Meanwhile, Section 138 of the DUAA entered into force on 6 February 2026. The provision criminalizes the creation, or the solicitation of the creation, of an "image alleged to be obscene" without the consent of an adult. The measure is being viewed in the context of growing concerns surrounding AI-assisted content generation.

42 Million Euro Fine from the French Data Protection Authority

The French data protection authority, CNIL, imposed a total fine of €42 million on telecommunications companies Free Mobile and Free as part of its first enforcement actions of 2026. The decision follows a large-scale data breach that occurred in 2024.

The investigation found that the personal data of millions of customers had not been protected with adequate technical and organizational security measures. It was also determined that breach notifications were incomplete and that certain data had been retained longer than necessary.

CNIL imposed a €27 million fine on Free Mobile and a €15 million fine on Free, while also ordering the companies to strengthen their security measures. The decision underscores that serious sanctions continue to be enforced under the GDPR in cases involving failures to comply with data security obligations.

Data Deletion Warning Issued to Staples in Canada

On 13 January 2026, the Office of the Privacy Commissioner of Canada (OPC) announced the outcome of its investigation into Staples Canada. The investigation revealed that certain returned electronic devices had been resold without fully erasing customers' personal data. In its statement, the OPC concluded that the practice violated Canada's private sector privacy legislation.

The authority emphasized that second-hand laptops and similar devices must be thoroughly wiped in accordance with manufacturers' instructions before resale.

The regulator also called for clearer staff guidance and stronger technical controls in data deletion processes. Staples Canada reportedly accepted the recommendations and committed to updating its internal procedures. The decision serves as an important warning to businesses involved in the resale of electronic devices regarding their data security obligations.

Personal Data Deletion Now Just One Click Away in the U.S. with "DROP"

On 1 January 2026, the California Privacy Protection Agency (CPPA) officially launched the Delete Request and Opt-out Platform (DROP), a system developed to address the collection and sale of personal data by data brokers. The new platform allows residents to submit a single request to have their personal data deleted by hundreds of registered data brokers.

DROP was established under the 2023 Delete Act and requires data brokers to receive and process deletion requests through a centralized mechanism. After verifying their identity and residency, users can submit a bulk deletion request via the platform, eliminating the need to contact each company individually.

Authorities expect the initiative to help reduce risks associated with spam, targeted advertising, data profiling, and identity theft. The CPPA emphasized that DROP represents the first centralized deletion mechanism of its kind in the United States and may serve as a model for other states.

Interactive Advertising Bureau Europe Wins Appeal Against APD Decision

On 7 January 2026, the Belgian Market Court annulled the corrective action plan approved by the Belgian Data Protection Authority (APD) concerning the Transparency and Consent Framework (TCF) under the General Data Protection Regulation (GDPR).

In January 2023, the APD had approved an action plan submitted by IAB Europe to bring the TCF into compliance with the GDPR and had initiated a six-month implementation period. IAB Europe challenged the decision, arguing that the scope was overly broad and that it acted only as a joint controller with respect to the "TC String," the signal encoding users' consent preferences.

The court upheld the appeal and annulled the APD's approval decision, marking a significant development for the digital advertising sector and the interpretation of controller responsibilities under the GDPR.

The court also emphasized that the APD acted procedurally incorrectly by adopting its decision without giving IAB Europe the opportunity to present its views. The ruling requires the APD to reassess the action plan and to prepare a narrower framework aligned with IAB Europe's actual role as controller.

IAB Europe CEO Townsend Feehan stated that the judgment confirms the legal foundation of the TCF and demonstrates that the regulator's previous interpretation had been overly broad, adding that "the decision provides an opportunity for a constructive reset."

The ruling is regarded as an important precedent regarding the legal boundaries of consent management frameworks and GDPR compliance within the European digital advertising ecosystem.

Clear Warning from the Turkish DPA to Mobile Applications

The Turkish Data Protection Authority (KVKK) issued a public announcement concerning push notifications sent through mobile applications, stressing that obtaining notification consent for multiple purposes under a single approval is unlawful.

The Authority concluded that operational notifications forming a natural part of the service—such as order status updates—must be clearly distinguished from campaign or marketing notifications, and that each category must be subject to separate and independent consent.

Forcing users to accept marketing notifications in order to benefit from a core service undermines the "freely given" element of explicit consent and violates the principle of granular consent.

Accordingly, data controllers are expected to redesign mobile application architectures to allow users to manage different types of notifications separately and to restructure their consent mechanisms in line with this requirement.

KVKK: Data Breach Announcements to Be Removed After 60 Days

The Turkish Data Protection Authority (KVKK) has introduced a new practice regarding the notification and publication of personal data breaches. Under the Law and the Board's established decisions, data controllers are required to notify the Authority as soon as possible and no later than 72 hours after becoming aware of a personal data breach.

With the new approach, breach announcements published on the Authority's website will be removed after 60 days. The measure aims to balance transparency with the principles of proportionality and data minimization, while preventing long-term reputational harm once the public disclosure objective has been fulfilled.

Warning from the Turkish DPA on WhatsApp Use in Public Institutions

The Turkish Data Protection Authority (KVKK) issued a public statement following complaints that public sector employees were being required to use foreign-based messaging applications such as WhatsApp for administrative communications.

In its announcement, the Authority recalled that, pursuant to a Presidential Circular, the sharing of classified, sensitive, or personal data–containing information and documents through non-domestic or unauthorized communication platforms is not considered appropriate.

The KVKK emphasized that correspondence, instructions, and document sharing conducted via WhatsApp may constitute personal data processing activities. If such processing does not rely on one of the legal grounds set out under the Personal Data Protection Law, responsible public officials may face administrative sanctions under applicable disciplinary provisions.

The Authority also reiterated that mobile phone numbers of public employees qualify as personal data and stressed that public institutions must exercise the highest level of diligence in ensuring data security and compliance with data protection legislation.

Update to E-Government System: Termination Codes Removed from Social Security Records

Following a system update to the e-Government portal, access to termination reasons (exit codes) within Social Security Institution (SGK) service records has been restricted from third parties.

This change is considered to be aligned with the decision of the Danıştay dated 14 October 2024, which emphasized that recording termination reasons based solely on the employer's unilateral declaration—without having undergone judicial review—may create concerns in terms of the protection of personal data and the right to work.

Indeed, it had been recognized that codes such as "violation of moral and good faith principles" constitute personal data capable of affecting an individual's professional reputation and working life.

However, although this information is no longer visible in the standard service record, it remains accessible in practice through the termination notification document if specifically requested.

Proposal for Turnover-Based Fines for AI-Generated Content

A bill submitted to the grand national assembly of Türkiye on 8 January 2026 introduces new sanctions concerning AI-generated content.

The proposal seeks to amend Law No. 6698 on the Protection of Personal Data by providing that, where audio, visual, or textual content generated through artificial intelligence is shared without the explicit consent of the data subject, digital platforms enabling the dissemination of such content may be subject to administrative fines.

Under the proposal, fines could amount to up to 5 percent of the platform's global annual turnover for the preceding year. The aim is to replace the existing fixed fine regime with a heavier, turnover-based sanctioning mechanism.

The explanatory memorandum to the proposal emphasizes that deepfake content in particular poses increasing risks to personality rights and the security of personal data. The draft legislation is expected to proceed to the General Assembly agenda following deliberations in the relevant parliamentary committees.

Basaran Law Firm
Istanbul · Türkiye

For further details about our practice areas or to discuss how we may assist you
Please reach us at:

E-mail: info@basaranlawfirm.com
www.linkedin.com/company/basaran-law-firm
www.basaranlawfirm.com

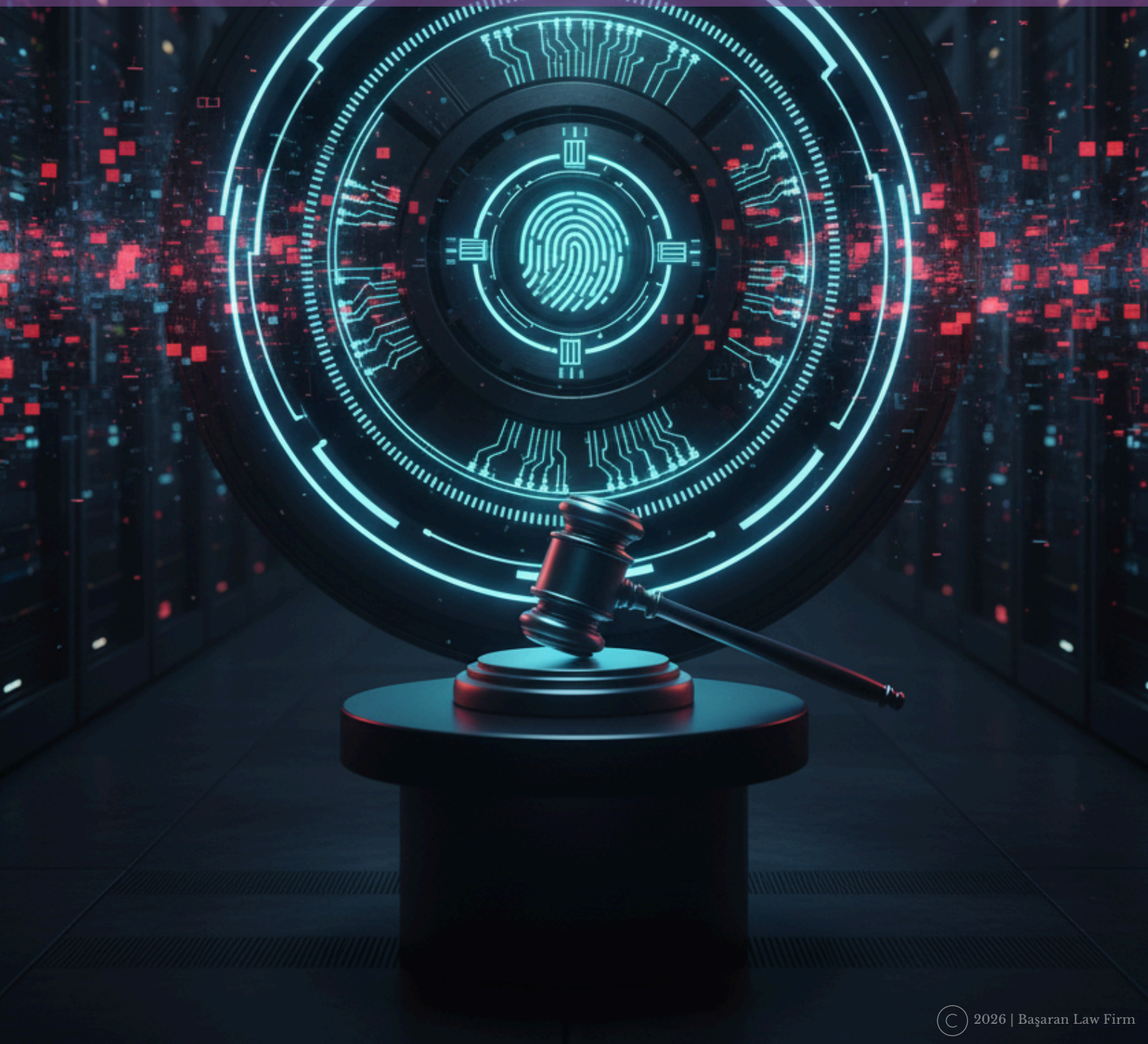
*This newsletter is prepared solely for informational purposes and does not constitute any legal advice for a specific case or client.

THE PULSE

BAŞARAN LAW FIRM

Şubat 2026
Sayı: 06

VERİ KORUMA ALANINDAKİ HUKUKİ DÜZENLEMELER



© 2026 | Başaran Law Firm

Avrupa Birliği ile Brezilya Arasında Veri Akışında Yeni Dönem

Avrupa Birliği ile Brezilya, kişisel verilerin korunması alanında karşılıklı yeterlilik (adequacy) kararlarını resmi olarak kabul etti. Bu gelişme, her iki tarafın da veri koruma standartlarının birbirine eşdeğer ve yeterli koruma sağladığını tespitine dayanıyor ve kişisel verilerin güvenli ve serbest biçimde akışını mümkün kılıyor.

Kararın yayınlanmasıyla birlikte Avrupa Birliği ve Brezilya arasında kişisel veriler, ek transfer hukuki gerekçelerine ya da sözleşmelere ihtiyaç olmadan karşılıklı olarak akabilecek. Bu durum, toplamda yaklaşık 670 milyon tüketiciyi kapsayan dünyanın en geniş "güvenli ve serbest veri akış bölgesini" ortaya çıkaracak.

AB tarafında karar, Avrupa Komisyonu tarafından GDPR (Genel Veri Koruma Yönetmeliği) kapsamında alınan uygulama kararı ile yürürlüğe kondu. Brezilya tarafında ise, LGPD (Brezilya Genel Kişisel Veri Koruma Kanunu) uyarınca kurulan veri koruma otoritesi ANPD'nin karşılıklı yeterlilik kabulü ile eşzamanlı bir düzenleme yapıldı. Böylece iki taraf da birbirlerinin veri koruma rejimlerini "yeterli" olarak tanıdı.

Avrupa Komisyonu, bu kararın ticaret ilişkilerini güçlendireceğini, dijital ekonomiyi destekleyeceğini ve işletmeler için hukuki belirsizlikleri azaltacağını belirtti.

Bu düzenleme, AB ile Mercosur arasında tarihî ortaklık anlaşmaları çerçevesinde atılan adımların bir parçası olarak da yorumlanıyor ve küresel veri koruma standartlarının uyumlaştırılmasında önemli bir eşik olarak değerlendiriliyor.

ICO'dan Transfer, Erişim ve Yaptırım Alanında Kritik Güncellemeler

2026 yılının başı, Birleşik Krallık veri koruma rejimi açısından dikkat çekici gelişmelere sahne oldu. Ülkenin veri koruma otoritesi olan Information Commissioner's Office (ICO), hem rehberlerini güncelledi hem de yaptırım yaklaşımına ilişkin önemli adımlar attı. Sürecin merkezinde ise 2025 tarihli veri reformu niteliğindeki Data (Use and Access) Act 2025 (DUAA) yer alıyor.

Erişim Hakkı Rehberinde Güncelleme: ICO, DUAA'ya uyum kapsamında veri sahiplerinin erişim hakkına (DSAR) ilişkin kılavuzunu güncelledi. Güncelleme ile "açıkça temelsiz" erişim taleplerinin kapsamı netleştirilirken, kuruluşların talepleri yanıtlarken "makul ve orantılı" bir yaklaşım benimsemesi gerektiği vurgulandı.

Uluslararası Veri Transferlerinde Üç Aşamalı Test: ICO, UK GDPR kapsamındaki uluslararası veri transferlerine ilişkin rehberini de önemli ölçüde sadeleştirdi ve netleştirdi. Güncellenen metin, kuruluşların "kısıtlı transfer" yapıp yapmadığını belirlemeleri için üç aşamalı bir test sunuyor.

Sözleşmesel Konum Esaslı Yeni Yaklaşım: Rehberdeki en dikkat çekici değişiklik ise transfer değerlendirmesinde coğrafi konumdan ziyade sözleşmesel konumun esas alınması oldu. ICO'ya göre önemli olan verinin fiziksel olarak nerede bulunduğu değil, alıcı kuruluşun kayıtlı olduğu ülke.

Bu yaklaşım, veriler fiilen Birleşik Krallık dışına çıkmasa bile, sözleşme karşı tarafının "yetersiz" bir üçüncü ülkede kayıtlı olması halinde kısıtlı transfer söz konusu olabileceği anlamına geliyor. Buna karşılık, sözleşme tarafı Birleşik Krallık'ta kayıtlıysa, veriler yurtdışı sunucularda barındırılsa dahi kısıtlı transfer oluşmayabiliyor.

Rehber ayrıca uzaktan erişimin de transfer teşkil ettiğini teyit ediyor ve transferi "başlatan" tarafın sorumluluğuna vurgu yapıyor.

ICO–Hükümet Arasında Mutabakat Anlaşması: 8 Ocak'ta ICO ile Birleşik Krallık Hükümeti arasında veri güvenliği alanında iş birliğini güçlendirmek amacıyla bir Mutabakat Anlaşması imzalandı. Anlaşma, kamu hizmetlerinde veri kullanımının güvenli şekilde geliştirilmesini ve veri ihlallerinden sistematik ders çıkarılmasını hedefliyor.

DUAA Madde 138 Yürürlüğe Girdi: Öte yandan DUAA'nın 138. maddesi de 6 Şubat 2026 itibarıyla yürürlüğe girdi. Söz konusu düzenleme, bir yetişkinin rızası olmadan "müstehcen olduğu iddia edilen görüntü" oluşturulmasını veya oluşturulmasının talep edilmesini suç haline getiriyor. Bu adım, yapay zekâ destekli içerik üretimine ilişkin artan endişeler bağlamında değerlendiriliyor.

Fransız Veri Koruma Otoritesi'nden 42 Milyon Euro Ceza

Fransa veri koruma otoritesi CNIL, 2026'nın ilk yaptırım kararları kapsamında telekom şirketleri Free Mobile ve Free'e toplam 42 milyon euro para cezası verdi. Karar, 2024 yılında yaşanan büyük ölçekli veri ihlaline dayanıyor.

Denetimde, milyonlarca müşteriye ait kişisel verinin yeterli teknik ve organizasyonel güvenlik önlemleri olmaksızın korunmadığı tespit edildi. Ayrıca ihlal bildirimlerinin eksik olduğu ve bazı verilerin gereğinden uzun süre saklandığı belirtildi.

CNIL, Free Mobile'a 27 milyon euro, Free'e ise 15 milyon euro ceza uygularken, şirketlere güvenlik önlemlerini güçlendirme talimatı verdi. Karar, GDPR kapsamında veri güvenliği yükümlülüklerinin ihlal edilmesi halinde ağır yaptırımların uygulanmaya devam ettiğini ortaya koydu.

Kanada'da Staples'a Veri Silme Uyarısı

13 Ocak 2026'da Office of the Privacy Commissioner of Canada (OPC), Staples Canada hakkında yürüttüğü incelemenin sonucunu açıkladı. Denetimde, şirketin bazı iade edilen elektronik cihazları müşterilere ait kişisel veriler tamamen silinmeden yeniden satışa sunduğu tespit edildi.

OPC açıklamasında, bu uygulamanın Kanada'nın özel sektörde kişisel verilerin korunmasını düzenleyen mevzuatına aykırı olduğu belirtildi. Kurum, özellikle ikinci el olarak satılan dizüstü bilgisayar ve benzeri cihazların, üretici talimatlarına uygun biçimde tamamen temizlenmesi gerektiğini vurguladı.

Yetkili makam, personelin veri silme süreçleri konusunda açık talimatlarla eğitilmesi ve teknik kontrollerin güçlendirilmesi çağrısında bulundu. Staples Canada'nın ise tavsiyeleri kabul ederek iç prosedürlerini güncelleme taahhüdünde bulunduğu bildirildi.

Karar, ikinci el elektronik ürün satışı yapan işletmelere veri güvenliği konusunda önemli bir uyarı niteliği taşıyor.

ABD'de "DROP" ile Kişisel Verileri Silmek Artık Bir Tıklamayla Mümkün

1 Ocak 2026'da California Privacy Protection Agency (CPPA), kişisel verilerin veri brokerları tarafından toplanması ve satılmasına karşı geliştirilen Delete Request and Opt-out Platform (DROP) sistemini resmen devreye aldı. Yeni platform, vatandaşlara tek bir başvuruyla yüzlerce kayıtlı veri brokerından kişisel verilerinin silinmesini talep etme imkânı tanıyor.

DROP, 2023 yılında kabul edilen Delete Act kapsamında oluşturuldu ve veri brokerlarının bireylerden gelen silme taleplerini merkezi bir sistem üzerinden almalarını zorunlu hale getiriyor. Kullanıcılar, kimlik ve ikamet doğrulamasının ardından platform üzerinden toplu silme talebi gönderebiliyor. Böylece her bir şirketle ayrı ayrı iletişime geçme zorunluluğu ortadan kalkıyor.

Yetkililer, uygulamanın özellikle spam mesajlar, hedefli reklamcılık, veri profilleme faaliyetleri ve kimlik hırsızlığı risklerinin azaltılmasına katkı sağlamasını bekliyor. CPPA, DROP'un ABD'de bu kapsamda hayata geçirilen ilk merkezi silme mekanizması olduğuna dikkat çekerek, uygulamanın diğer eyaletler için de model oluşturabileceğini belirtti.

Interactive Advertising Bureau Europe, APD Kararına Karşı Yargı Zaferi Kazandı

7 Ocak 2026'da Belçika Ticaret Mahkemesi, Belgian Data Protection Authority'nin General Data Protection Regulation (GDPR) çerçevesinde Transparency and Consent Framework (TCF) ile ilgili olarak APD tarafından onaylanan düzeltici eylem planını hukuka aykırı bularak iptal etti.

APD, Ocak 2023'te TCF'nin GDPR'ye uyumunu sağlamak için IAB Europe'un sunduğu eylem planını onaylamış ve altı aylık uygulama süresi başlatmıştı. IAB Europe, bu kapsamın aşırı geniş olduğunu ve kuruluşun yalnızca "TC String" (kullanıcı tercihlerini kodlayan veri sinyali) işleme konusunda ortak denetleyici olduğunu savunarak karara itiraz etti. Mahkeme, bu itirazı haklı bularak APD'nin onay kararını iptal etti.

Mahkeme ayrıca APD'nin IAB Europe'a görüşünü sunma fırsatı vermeden karar almasının, usul açısından da yanlış olduğunu vurguladı. İlgili karar, APD'nin eylem planını yeniden değerlendirmesini ve IAB Europe'un gerçek denetleyici rolüne uygun daha dar kapsamlı bir plan hazırlamasını gerektiriyor.

IAB Europe CEO'su Townsend Feehan, mahkemenin TCF'nin hukuki temelini onayladığını ve düzenleyicinin önceki yorumlarının gereğinden geniş olduğunu gösterdiğini belirterek, "Bu karar yapıcı bir reset için fırsat sağlıyor." dedi.

Karar, Avrupa dijital reklamcılık ekosisteminde rıza yönetimi ve GDPR uyumundan sorumlu çerçevelerin hukuki sınırları konusunda önemli bir emsal niteliği taşıyor.

KVKK'dan Mobil Uygulamalara Açık Uyarı

Mobil uygulamalardan gönderilen anlık bildirimlere ilişkin KVKK'nın yayımladığı kamuoyu duyurusunda, bildirim izinlerinin tek bir onay altında birden fazla amacı kapsayacak şekilde alınmasının hukuka aykırı olduğu vurgulanmıştır.

Kurum, sipariş durumu gibi hizmetin doğal bir parçası olan operasyonel bildirimler ile kampanya/reklam içerikli bildirimlerin ayrı ayrı ve bağımsız rızaya tabi olması gerektiğine karar vermiştir. Kullanıcının temel bir hizmetten faydalanabilmesi için pazarlama bildirimlerini kabul etmeye zorlanması, açık rızanın "özgür irade" unsurunu ortadan kaldırmakta ve parçalı açık rıza ilkesini ihlal etmektedir.

Bu nedenle veri sorumlularının, mobil uygulama mimarilerini kullanıcıların bildirim türlerini ayrı ayrı yönetebileceği şekilde düzenlemesi ve izin süreçlerini bu doğrultuda yeniden yapılandırması gerektiği açıkça ortaya konmuştur.

KVKK Kararıyla Veri İhlali İlanları 60 Gün Sonra Kaldırılacak

KVKK, kişisel veri ihlallerinin bildirimi ve ilanına ilişkin uygulamada yeni bir düzenlemeye gitti. Kanun ve Kurul'un yerleşik kararları uyarınca, veri sorumlularının kişisel veri ihlalini öğrendikleri tarihten itibaren en geç 72 saat içinde Kurula, ihlalden etkilenen kişilere ise makul olan en kısa sürede bildirim yapma yükümlülüğü devam ederken; 25.12.2025 tarihli ve 2025/2451 sayılı Kurul Kararı ile önemli bir değişiklik getirildi.

Buna göre, kişisel veri ihlali bildirimlerinin Kurumun internet sitesinde süresiz olarak ilan edilmesi uygulamasına son verilmiş, ilan süresi en fazla 60 günle sınırlandırılmıştır. Ayrıca veri sorumlusunun, bu süre dolmadan ilgili kişilere bildirim yaptığını belgelemesi halinde, ihlal ilanının Kurumun internet sitesinden daha erken kaldırılmasına karar verilmiştir.

Kamu Kurumlarında WhatsApp Kullanımına KVKK Uyarısı

Kişisel Verileri Koruma Kurumu, kamu kurumlarında görev yapan personelin idarî iş ve işlemler kapsamında WhatsApp gibi yurt dışı menşeli haberleşme uygulamalarını kullanmaya zorlanmasına ilişkin şikâyetler üzerine kamuoyunu bilgilendirmiştir.

Duyuruda, Cumhurbaşkanlığı Genelgesi uyarınca yerli ve yetkilendirilmiş uygulamalar dışında, bu tür platformlar üzerinden gizlilik dereceli, kritik nitelikte veya kişisel veri içeren bilgi ve belgelerin paylaşılmasının uygun olmadığı vurgulanmıştır.

WhatsApp üzerinden yapılan yazışma, talimat ve belge paylaşımlarının kişisel veri işleme faaliyeti sayılabileceği; bu işlemlerin KVKK'da öngörülen şartlara dayanmaması hâlinde sorumluluğu bulunan kamu personeli hakkında disiplin hükümleri kapsamında idari yaptırım uygulanabileceği ifade edilmiştir.

Ayrıca kamu personeline ait cep telefonu numaralarının da kişisel veri olduğu hatırlatılarak, kamu kurumlarının veri güvenliği ve KVKK'ya uyum konusunda azami dikkat ve özeni göstermesi gerektiği belirtilmiştir.

E-Devlet Güncellemesiyle SGK Hizmet Dökümünde İşten Çıkış Kodları Kaldırıldı

E-Devlet üzerinden erişilen SGK hizmet dökümünde yapılan sistem güncellemesiyle, işten çıkış nedenlerine (işten çıkış kodlarına) üçüncü kişiler tarafından erişim sınırlandırıldı.

Bu değişiklik, Danıştay'ın 14.10.2024 tarihli kararında vurguladığı üzere, işverenin tek taraflı beyanına dayanan ve henüz yargı denetiminden geçmemiş fesih nedenlerinin resmi kayıtlarda yer almasının kişisel verilerin korunması ve çalışma hakkı bakımından sakıncalar doğurabileceği tespitleriyle uyumlu bir uygulama olarak değerlendiriliyor.

Nitekim "ahlak ve iyi niyet kurallarına aykırılık" gibi kodların, kişinin mesleki itibarını ve çalışma hayatını etkileyebilecek kişisel veri niteliği taşıdığı kabul edilmişti. Ancak her ne kadar hizmet dökümünde bu bilgiler artık görünmese de, işten ayrılış bildirgesi talep edilmesi halinde fesih nedeninin bu belge üzerinden erişilebilir olmaya devam ettiği uygulamada dikkat çekiyor.

Yapay Zekâ İçeriklerine Ciroya Dayalı Ceza Teklifi

8 Ocak 2026 tarihinde Türkiye Büyük Millet Meclisi'ne sunulan kanun teklifi, yapay zekâ ile üretilen içeriklere yönelik yeni yaptırımlar öngörüyor.

Teklif, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda değişiklik yaparak, yapay zekâ aracılığıyla oluşturulan ses, görüntü ve metinlerin ilgili kişinin açık rızası olmadan paylaşılması halinde, bu içeriklerin yayılmasına imkân sağlayan dijital platformlara idari para cezası uygulanmasını düzenliyor.

Düzenlemeye göre ceza, platformların bir önceki yılki küresel cirosunun yüzde 5'i oranında hesaplanabilecek. Böylece mevcut sabit para cezası sisteminden farklı olarak, daha ağır ve oransal bir yaptırım mekanizması getirilmesi hedefleniyor.

Teklif gerekçesinde, özellikle deepfake içeriklerin kişilik hakları ve kişisel veri güvenliği açısından artan risk oluşturduğu vurgulanıyor. Düzenlemenin komisyon sürecinin ardından Genel Kurul gündemine gelmesi bekleniyor.

Basaran Law Firm
İstanbul · Türkiye

Hizmet alanlarımız hakkında daha fazla bilgi almak veya size nasıl yardımcı olabileceğimizi görüşmek için lütfen bizimle iletişime geçin:

E-posta: info@basaranlawfirm.com
www.linkedin.com/company/basaran-law-firm
www.basaranlawfirm.com

Bu bülten yalnızca bilgilendirme amacıyla hazırlanmıştır; herhangi bir somut olay veya müvekkile yönelik hukuki görüş niteliği taşımaz.