DL | Avukatlık Bürosu

KİŞİSEL VERİLERİ KORUMA HUKUKU
GÜNCEL GELİŞMELER
OCAK 2025

TÜRKİYE'DEKİ GELİŞMELER

VERİ İHLALİ BİLDİRİMLERİ

Trabzon Üniversitesi Rektörlüğü tarafından KVK Kurumu'na bildirilen veri ihlali, 16.01.2025 tarihinde Kişisel Verileri Koruma Kurumu'nun ("KVK Kurumu") internet sitesinde yayımlanmıştır.

Veri sorumlusu Trabzon Üniversitesi Rektörlüğü tarafından tarafından Kişisel Verileri Koruma Kurulu'na ("**KVK Kurulu**") veri ihlali ("**Veri İhlali**" veya "**İhlal**") bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 01.01.2025 tarihinde başladığı,
- İhlalin 06.01.2025 tarihinde tespit edildiği,
- Personel ve öğrencilere ait bazı bilgilerin siber saldırganlar tarafından internet üzerindeki yasadışı platformlarda satışa sunulduğu,
- İhlalden etkilenen kişisel verilerin; kimlik (ad-soyad, T.C. kimlik numarası, doğum tarihi, anne ve baba adı, doğum yeri), iletişim (e-posta adresi, telefon numarası (iş ve cep numarası)), özlük (kurumsal sicil numarası, unvan, öğretmen ve öğrenci ders programlarının bulunduğu dosyalar) ve lokasyon verileri olduğu,
- İhlalden etkilenen kayıt sayısının 25.237 olduğu,
- İhlalden etkilenen ilgili kişi grubunun; personeli ve öğrenciolduğu.

İlgili karara buradan ulaşabilirsiniz.

DUYURULAR VE HABERLER

KVK Kurumu tarafından Kişisel Verilerin Yurt Dışına Aktarılması Rehberi yayımlanmıştır.

Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 12.02.2024 tarihinde Resmi Gazete'de yayımlanmasıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**KVKK**") yurt dışına veri aktarımını düzenleyen 9. maddesindeki değişikliklere yönelik olarak yol gösterici nitelikte olması amaçlanan Kişisel Verilerin Yurt Dışına Aktarılması Rehberi ("**Rehber**") yayımlanmıştır. Bu Rehber'de şu hususlar dikkat çekmektedir:

- Değişiklik öncesi veri sorumlularının taahhüt vermelerine veya ilgili kişinin açık rızasını almak suretiyle yurtdışına veri aktarılmasının ticari hayatta zorluklara yol açtığı, KVK Kurulu'na gerçekleştirilen taahhüt başvurusunun çok azına izin verilmiş olması sebebiyle yurt dışına veri aktarım süreçlerinin hem yatırımcılar hem de ticari hayatı engelleyici bir hal aldığı, bu sebeplerle değişiklik yapılmasının

önem arz ettiği, değişikliklerin GDPR'ın ilgili hükümleri gözetilerek hazırlandığı belirtilmiştir.

- Yurt dışına veri aktarımında üç basamaklı bir yapı oluşturulduğu, bu yapıda; yeterlilik kararının bulunması, uygun güvencelerden birinin bulunması ve istisnai aktarım hallerinden birinin bulunması durumunda yurt dışına veri aktarımının önü açıldığı, veri sorumlularının Rehber'i örnek alması gerektiğine dikkat çekilmiştir.

İlgili Rehber'e buradan ulaşabilirsiniz.

KVK Kurumu tarafından 2025 yılı idari para cezalarına ilişkin bilgilendirme yayımlanmıştır.

KVK Kurulu tarafından 2025 yılı bakımından uygulanacak idari para cezaları KVK Kurumu'nun internet sitesinde yayımlamıştır. İlgili bilgilendirme tablosunda idari para cezaları aşağıdaki gibi belirtilmiştir:

- Aydınlatma yükümlülüğünü yerine getirmeme: 68.083 – 1.362.021 TL
- Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi: 204.285 – 13.620.402 TL
- Kurul kararlarının yerine getirilmemesi: 340.476 – 13.620.402 TL
- Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi: 272.380 – 13.620.402 TL,
- 9'uncu maddenin beşinci fıkrasında öngörülen bildirim yükümlülüğünün yerine getirimemesi: 71.965 – 1.439.300 TL

idari para cezası öngörülmüştür.

İlgili bilgilendirme tablosuna buradan ulaşabilirsiniz.

KVK Kurumu tarafından Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi güncellenmiştir.

KVK Kurumu, 12.03.2024 tarihli Resmi Gazete'de yayınlanan Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun ile KVKK'da yapılan değişiklikler göz önünde bulundurarak; Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi'ni güncellemiştir. Bu hususlar doğrultusunda aşağıdaki hususlar hakkında açıklamalara yer verilmiştir.

- **Veri Sorumlusu - Veri İşleyen İlişkileri**: Bankaların veri sorumlusu ve veri işleyen arasındaki ilişkileri düzenlerken dikkat etmeleri gereken hususlar ve yapılması gereken sözleşmeler detaylandırılmaktadır.
- **Açık Rıza:** Bankaların; ATM, mobil ve internet bankacılığı, çağrı merkezi gibi farklı kanallar üzerinden açık rıza alırken dikkat etmeleri gereken noktalar belirtilmektedir.
- **Hukuki Yükümlülükler:** Bankaların tabi olduğu mevzuat kapsamında, kişisel verilerin işlenmesine ilişkin yasal yükümlülükler ve bu yükümlülüklerin nasıl ele alınması gerektiği düzenlenmektedir.
- **Meşru Menfaat Kapsamında Veri İşleme:** Bankaların meşru menfaatleri doğrultusunda kişisel verileri nasıl işlemesi gerektiği ve bu işlemlerin sınırları tartışılmaktadır. Söz konusu tartışmalarda; meşru menfaat tespitinin yapılmasına ve kişisel verileri meşru menfaate dayalı olarak kullanabilmek için yapılacak incelemenin nasıl olması gerektiğine yer verilmektedir.
- **Özel Nitelikli Kişisel Verilerin İşlenmesi:** Bankaların özel nitelikli kişisel veri de işlemesi sebebiyle; özel nitelikli kişisel verilerin işlenme şartları, bu verilerin korunması için alınması gereken önlemler ve bankacılık sektöründe bu tür verilerin işlenmesine dair örnekler sunulmakta olup bu hususta açıklamalara yer verilmektedir.

- **Kişisel Verilerin Aktarılması:** Kişisel verilerin yurt içinde ve yurt dışında aktarılmasıyla ilgili usul ve esaslar, bankaların bu süreçlerde dikkat etmesi gereken noktalar belirtilmektedir.
- **Genel İlkeler:** Kişisel verilerin işlenmesinde uyulması gereken genel ilkeler, bankaların bu ilkelere uygun hareket etmesi için rehberlik edilmektedir. Özellikle aydınlatma yükümlülüğü hakkında detaylı açıklamalar bulunmaktadır.

İlgili Rehber'e buradan ulaşabilirsiniz.

Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi yayımlanmıştır.

Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi ("**Kararname**") ile Siber Güvenlik Başkanlığı kurulmuştur. İlgili Kararname'de; Türkiye nezdinde ulusal siber güvenlik politikasını güçlendirme, kritik altyapıları koruma altına alma ve devletin dijital ortamlardaki siber tehditlere karşı korunmasını sağlama amaçlarına dikkat çekilmektedir. Ayrıca Kararname'de, Siber Güvenlik Başkanlığının başlıca görevleri, teşkilat yapısı gibi hususlar detaylı biçimde düzenlenmiştir. Siber Güvenlik Başkanlığının başlıca görevleri arasında; siber güvenlik hakkında farkındalık yaratmak, bilgi güvenliğini destekleyici projeler yürütmek, AR-GE ve teknoloji transferleri yapmak, kamu, özel sektör ve üniversiteler arasındaki işbirliğini arttırmak, zafiyetleri tespit etmek, acil durum ve kriz yönetim planları oluştrmak ve kamu kurum ve kuruluşları tarafından verilecek teşviklere ilişkin görüş bildirmek gibi hususlar yer almaktadır.

İlgili Resmi Gazete'ye buradan, ilgili Kararname ile ilgili yazmış olduğumuz yazıya buradan ulaşabilirsiniz.

KVK Kurumu tarafından "Arabuluculuk Faaliyetleri Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmesine" ilişkin kamuoyu duyurusu yayımlanmıştır.

Yayımlanan duyuruda arabulucuların aydınlatma yükümlülüğüne dair değerlendirmeler paylaşılmıştır. Bu değerlendirmelere göre, arabuluculuk faaliyetleri 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nda ("**Arabuluculuk Kanunu**") düzenlenmektedir. Arabuluculuk Kanunu'nda, arabuluculara aydınlatma yükümlülüğü getirilmiştir. Bu yükümlülük asgari olarak; veri sorumlusunun ve varsa temsilcisinin kimliği, veri işleme amacı, verilerin kimlere ve hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukuki sebebi ile KVKK'nın 11'inci maddesinde sayılan diğer hakları konusunda ilgili kişilerin bilgilendirilmesi olarak tanımlanmaktadır. Ancak KVKK'nın kapsamı ile Arabuluculuk Kanunu'nun aydınlatma yükümlülüğü hususunda düzenlenen kapsamında farklılıklar bulunmaktadır. Bu sebeple, Arabuluculuk Kanunu kapsamında yapılan aydınlatma yükümlülüğünün yerine getirilmesi yeterli olmayıp, KVKK kapsamında öngörülen hususlar ile ilgili de ilgili kişilere ayrıca bilgi vermek suretiyle arabulucuların aydınlatma yükümlülüğünü yerine getirmesi gerekmekte olduğu duyuruda vurgulanmıştır.

İlgili duyuruya buradan ulaşabilirsiniz.

DÜNYADAKİ GELİŞMELER

DUYURULAR VE HABERLER

Avrupa Parlamentosu tarafından Avrupa Birliği'nde karanlık örüntünün (*dark pattern)* düzenlenmesini amaçlayan bilgi notu paylaşılmıştır.

Karanlık örüntü; kullanıcıların davranışlarını, çevrimiçi ortamlarda, genellikle kendilerinin bilgisi ve rızası olmaksızın etkileyen tekniklerdir. Avrupa Birliği mevzuatlarında yeknesak bir tanım olmaması sebebiyle ilgililer daha net tanımlar, daha güçlü güvenceler ve mevcut yasaların daha etkin şekilde uygulanması için çağrıda bulunmuştur.

Avrupa Birliği mevzuatlarında bulunan tanımlar karşılaştırıldığında iki temel kavram karşımıza çıkmaktadır. Bunlar; uygulamanın manipülatif veya aldatıcı niteliği ve bunun sonucunda ortaya çıkan olumsuz veya zararlı sonuç. Ancak bu kavramların çok geniş olması uygulamada sınıflandırma konusunda problem yaratmış olup, bunun önüne geçmek amacıyla çok sayıda kılavuz ve öneri yayınlanmış olduğu bildirilmektedir.

Karanlık örüntü ilk olarak Haksız Ticari Uygulamalar Direktifi'nde *(Unfair Commercial Practices Directive)* düzenlenmiştir. Karanlık örüntü ifadesi ilgili düzenlemede yer almasa dahi, ticari uygulamalarda yanıltıcı ve agresif uygulamalara dikkat çekme suretiyle dolaylı olarak düzenlenmiştir. Haksız Ticari Uygulamalar Direktifi'nde, tüketiciyi bu tür haksız ticari uygulamalara karşı korumayı amaçlayan hükümlere yer verilmiştir.

AB Dijital Hizmetler Yasası *(Digital Services Act)* ise çevrimiçi platformlarda karanlık örüntü kullanımını yasaklarken, AB Genel Veri Koruma Tüzüğü *("**General Data Protection Regulation** veya **GDPR**")* her somut olay özelinde değerlendirme yapılması gerektiğini vurgulamıştır.

Örneklerde de verilmiş olduğu gibi Avrupa Birliği mevzuatlarında yeknesak bir düzenleme bulunmamaktadır. Bu durum karşısında akademisyenler bazı uyarılarda bulunmuştur.

- Inge Graef, düzenlemede oluşan tutarsızlıkların uygulamaya da yansıyabileceği,
- Martin Brennche, karanlık örüntünün hukuka uygun ikna teknikleri ile hukuka uygun olmayan manipülasyon yöntemleri arasındaki gri alanda olması sebebiyle düzenlenmesinin zor olacağı,
- Mark Leiser ve Cristiana Santos ise karanlık örüntünün net bir şekilde sınıflandırılmasının yanı sıra hızlı değişen ve gelişen örüntüler konusunda mevzuatların güncellenmesi ve kamuoyunun bilgilendirilmesi gerektiği konusunda uyarılarda bulunmuştur.

İlgili bilgilendirme yazısına buradan ulaşabilirsiniz.

Avrupa Veri Koruma Kurulu ("EDPB") tarafından GDPR ile uyumlu maskeleme *(pseudonymisation)* hakkında bilgilendirme yazısı yayımlamıştır.

EDPB Ocak ayında gerçekleşen toplantıda, maskeleme ile ilgili olarak bazı yönergeler~~i~~ kabul edilmiştir. GDPR kapsamında maskeleme, kişisel verileri koruma alanında gerekli koruma sağlamak amacıyla düzenlenmiştir. EDPB'nin kabul ettiği yönergeler çerçevesinde iki önemli hukuki açıklamaya değinilmiştir.

1. Maskelenmiş veriler, ek bilgiler kullanmak suretiyle kimliği belirlenebilir gerçek kişi ile ilişkilendirilebilmesi durumunda kişisel veri olma niteliğini korumaktadır.
2. Maskeleme işlemi, kişisel veri işlenirken hukuki dayanak olarak meşru menfaati dayanak olarak göstermeyi diğer yükümlülüklere de uymak şartıyla kolaylaştırmaktadır. Bunun sebebi, maskemele yöntemi ile ilgili kişilerin verilerinin kişiler ile bağdaştırılması zorlaşmaktadır. Veri sorumluları meşru menfaatleri doğrultusunda kişisel veri işlerken, ilgili kişilerin hak ve özgürlüklerine yönelik riskler azalmakta olduğu belirtilmiştir.

Ayrıca yönergeler, kişisel veri işlenirken maskeleme kullanma yöntemini kullanırken alınması gereken teknik ve idari önlemler hakkında da bilgi vermektedir.

Söz konusu yönergeler, 28 Şubat tarihinde kamuoyunun da görüşünü almak için halka açılacaktır.

İlgili bilgilendirme yazısına buradan ulaşabilirsiniz.

EDPB tarafından, ilgili kişilerin erişim hakkı ile ilgili veri sorumlularını bilgilendirmeyi ve farkındalık kazandırmayı amaçlayan rapor yayımlanmıştır.

EDPB tarafından yayımlanan söz konusu rapor kapsamına ilgili kişilerin erişim hakkına ilişkin aşağıdaki hususlar zorluk olarak tespit edilmiştir:

1. Sağlanacak erişimin kapsamı hakkında farkındalığın olmaması,
2. Erişim talepleriyle ilgili süresiz, aşırı veya tutarsız saklama sürelerinin olması,
3. Belgelenmiş iç prosedürlerin eksikliği,
4. Erişim hakkının kolaştırılmasının önünde engeller olması,
5. Erişim hakkına ilişkin sınırlamaların tutarsız ve aşırı yorumlanması,
6. Erişim taleplerinin belirli hale getirilmesi talebinin aşırı yorumlanması,
7. İlgili kişilere yeterince detaylandırılmamış veya özelleştirilmemiş bilgi sağlanması.

İlgili EDPB Raporu'na buradan ulaşabilirsiniz.

GÜNCEL KARARLAR

Avrupa Veri Koruma Denetçisi (*"European Data Protection Supervisory veya EDPS"*), Frontex'e Avrupa Birliği mevzuatlarıyla uyumlu olmaması sebebiyle kınama cezası vermiştir.

Frontex, Avrupa Sınır ve Sahil Güvenlik Ajansı *(the European Border and Coast Guard Agency)* şüphelilerin sınır ötesi suçlara ait kişisel verilerini Europol'a aktarımını yaparken Avrupa Birliği mevzuatlarına uygun aktarım yapmaması sebebiyle EDPS tarafından kınama cezasına hükmedilmiştir.

2022 yılının Ekim ayında EDPS'nin Frontex üzerinde yapmış olduğu denetim sonucunda, sınır ötesi suçlardan şüpheli sıfatıyla yapılan sorgularda veri toplantığı ortaya çıkmıştır. Frontex, toplanan verileri sistematik bir şekilde, veri aktarımının gerekliliği gözetilmeksizin ve Frontex Tüzüğü'ne aykırı bir şekilde Europol ile paylaşmıştır. Bu durum sonucunda EDPS, Frontex aleyhine soruşturma başlatmıştır.

Yapılan soruşturmada yetkililer, bu şekilde paylaşımın ilgili kişilerin suç teşkil eden faaliyetlerle ilişkilendirme riski oluşabileceği, kişisel ve aile yaşamlarının zarar görebileceği konusunda açıklamada bulunmuştur.

2023 yılı Ekim ayında denetim raporunun paylaşılması üzerine, Frontex'in Europol ile olan veri aktarımını durdurması göz önünde bulundurularak yalnızca kınama kararı verilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi *(Agencia Española de Protección de Datos veya AEPD),* Banco Pichincha aleyhine € 50.000 idari para cezasına hükmetmiştir.

20 Ocak 2023 tarihinde Banco Pichincha ("**Banka**")'da hesabı olan ilgili kişi, hesabına giriş yapamadığına dair Banka ile iletişime geçmiştir. Yapılan inceleme sonucunda, ilgili kişi gibi davranan bir kişinin Banka ile iletişime geçtiğini ve Banka'nın kimlik tespiti için sorması gereken güvenlik sorularını sormaksızın Banka giriş bilgilerini değiştirdiği tespit edilmiştir. İlgili kişi gibi davranan kimse, Banka hesabından € 50.000 çekmiştir.

Banka, yapılan işlemde kişisel verileri hukuka uygun olarak işlediğini ve ilgili kişi gibi davranan kimsenin kişisel veriyi hukuka aykırı olarak işlediğini iddia etmiştir. AEPD tarafından verilen kararda, Banka hukuki dayanak olmaksızın kişisel veri işlediği ve arayanın kimliğini tespit etmek için gerekli özeni göstermediği belirtilmiştir.

Sonuç olarak, Banco Pichincha aleyhine €50.000 idari para cezasına hükmedilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

Fransız Veri Koruma Otoritesi *("The French Supervisory Authority veya CNIL")* tarafından, KASPR aleyhine € 240.000 idari para cezasına hükmedilmiştir.

KASPR müşterilerine, bir bedel karşılığı LinkedIn üzerinden ziyaret edilen profillere ait profesyonel iletişim bilgileri sağlayan bir Chrome tarayıcı uzantısı pazarlayan bir şirkettir. Diğer websitelerinden toplamış oldukları veri tabanı üzerinden müşterilerine söz konusu bilgileri sağlamaktadır. Veri tabanında yaklaşık 160 milyon iletişim bilgisi bulunmaktadır.

CNIL, iletişim bilgileri edinilen kişiler tarafından birçok şikayet almıştır. Bunun üzerine yapılan soruşturmada birden fazla ihlal tespit edilmiştir. Bu ihlaller aşağıdaki gibidir:

- Hukuki dayanak yükümlülüğüne uyulmaması,
- Veri işleme amacına orantılı bir veri saklama süresi belirleme ve buna uyma yükümlülüğüne uyulmaması,
- Kişilere şeffaflık ve bilgi sağlama yükümlülüğüne uyulmaması,
- Bireylerin erişim hakkına uyulmaması.

Bu sayılan ihlaller sonucunda, KASPR aleyhine € 240.000 idari para cezasına hükmedilmiştir. Ayrıca iletişim bilgilerine görünürlük kısıtlaması getiren kullanıcıların verilerinin toplanmasının durdurulmasına, bu şekilde toplanan verilerin silinmesine, ilgili kişilere verilerinin toplandığına dair bilgilendirme yaparak buna itiraz edebilecekleri konusunda bilgi verilmesine, otomatik olarak saklamanın durdurulmasına ve bilgi almak isteyen ilgili kişilere eksiksiz olarak yanıt verilmesini emretmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

CNIL tarafından, ORANGE aleyhine € 50.000.000 idari para cezasına hükmedilmiştir.

Fransız telekomünikasyon şirketi olan ORANGE, kullanıcılarına "mail orange" adlı çevrimiçi mesajlaşma hizmeti sunmaktadır. CNIL tarafından yapılan incelemeler sonucunda, kullanıcı e-posta kutularında e-postaların yanı sıra reklam amaçlı e-postaları görüntülediği sonucuna ulaşmıştır.

ORANGE, reklam amaçlı e-postaları göstermek suretiyle; ilgili kişilerin rızası olmadan ticari pazarlama mesajları atması sebebiyle ve rızasını geri almış kullanıcıların çerezlerinin okunmaya devam etmesi sebebiyle GDPR hükümlerine uymamıştır.

İnceleme sonucunda ORANGE aleyhine € 50.000.000 idari para cezasına hükmedilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.