GÜN + PARTNERS

TÜRKİYE'DE KİŞİSEL VERİLERİN KORUNMASI VE GİZLİLİK HUKUKU ÖNEMLİ GELİŞMELER VE ÖNGÖRÜLER

2026

Kişisel Verilerin Korunması ve Gizlilik

Büromuzun, yalnızca Kişisel Verilerin Korunmasına Kanununa ilişkin konuları (uyum, verilerin korunmasına ilişkin danışmanlık, veri sahiplerinin hakları ve talepleri, yurt dışına veri aktarımları, lokalizasyon yükümlülükleri, farklı sektörlere özgü kurallar ve düzenlemeler, siber güvenlik konuları ve veri ihlali bildirimleri ile Kişisel Verilerin Korunması Kurulu (Kurul) tarafından alınan kararlara karşı yargı yollarına başvurulması gibi) kapsamakla kalmayıp, aynı zamanda verilere ilişkin lisans sözleşmeleri, iktisaplar, verilerin kullanımı ve veri sahipliği konuları gibi işlemlerle de ilgilenen gizlilik ve verilerin korunması hukuku alanında özel olarak çalışmalarını yoğunlaştırmış bir çalışma grubu bulunmaktadır.

Kişisel verilerin korunmasına ilişkin uyum projelerinin yönetilmesi ve yürütülmesi ve çok uluslu müvekkillere günlük iş ve işleyişlerinde veri koruması alanında tavsiyelerde bulunulması dâhil veri koruma hukukunun her yönüyle ilgilenmekteyiz. Hem global hem de yerel veri gizliliği ekipleriyle çalışmakta ve şirketlerin kanuna uygunluklarını sağlamak üzere bu ekipler ile iş birliği yapmaktayız.

Müvekkillerimize yeni geliştirilen cihazla ve/veya programlarına ilişkin tavsiyeler vermekte ve ilgili mobil uygulamalar veya web siteleri için gerekli politikalar ile belgeleri hazırlamaktayız.

Müvekkillerimizi, ihlal bildirimleri ve Bağlayıcı Şirket Kuralları onayları dâhil uluslar arası aktarım izni başvurularına ilişkin olarak Türkiye'deki Kişisel Verileri Koruma Kurumu ("KVKK") nezdinde temsil etmekteyiz. Davaların yürütülmesi konusundaki derin deneyimimiz sayesinde, müvekkillere - KVKK tarafından verilen aleyhteki kararlara itiraz etmek üzere temyiz stratejileri sağlamaktayız. KVKK'nın kararlarına karşı açılan iptal davalarında müvekkillerimizi Sulh Ceza Mahkemesi nezdinde temsil etmekteyiz. Ekibimiz dahilinde bize cezai soruşturmalar kapsamında destek veren ceza avukatlarımız da bulunmaktadır.

Müvekkillerimize, Veri Sorumlusu olarak Veri Sorumluları Sicili'ne tescil edilme yükümlülüklerini yerine getirmeleri konusunda destek vermekte ve onları KVKK nezdinde temsil etmekteyiz. Türkiye'de tescile tabi olan yabancı veri sorumlularına Temsilci olarak atanmaktayız.

Ayrıca, müvekkillerimize birleşme ve satın alma projeleri kapsamında veri aktarımı ve veri koruma kanununa uygunluk konularında danışmanlık hizmeti sağlamaktayız.

Özellikle ilaçlar ve tıbbî cihaz sektörü, bankacılık, teknoloji, medya ve telekom sektörleri regüle edilen güçlü olduğumuz sektörler arasındadır.

Giriş

Türkiye'de kişisel verilerin korunması alanındaki son gelişmeler, alınan kararlar ve yayınlanan kılavuzlar yanında kişisel verilerin korunması hukukunun temel düzenlemeleri ve prensipleri ve gelişmeleri ile bu alandaki güncel hususları ve beklentileri ve değerlendirmeleri ele aldığımız bu yazımızda geçtiğimiz yılın (2025) önemli gelişmeleri ile 2026 yılının ilk yarısına kadar gerçekleşen güncel konularına değiniyor olacağız.

2025 yılı, Türkiye'de kişisel verilerin korunması alanında hem düzenleyici hem de uygulamaya yönelik önemli gelişmelerin yaşandığı bir dönem oldu. Kişisel Verileri Koruma Kurumu (KVKK), yayımladığı rehberler, ilke kararları ve kamuoyu duyurularıyla özellikle yurt dışına veri aktarımı, veri güvenliği, dijital platformlar ve yapay zekâ uygulamalarına ilişkin uyum süreçlerine yön vermiştir. Aynı dönemde veri sorumlularına yönelik denetim faaliyetleri yoğunlaşmış; 876 veri sorumlusuna toplam 352,5 milyon TL idari para cezası uygulanmış, yüzlerce veri ihlali bildirimi incelenmiş ve standart sözleşmeler yurt dışına veri aktarımında en yaygın güvence mekanizması haline gelmiştir.

Ayrıca bankacılık, ödeme hizmetleri, özel nitelikli kişisel veriler ve üretken yapay zekâ gibi alanlara ilişkin rehberler yayımlanırken, SMS doğrulama kodlarıyla ticari ileti onayı alınması ve otellerde kimlik fotokopisi alınması gibi uygulamalara ilişkin önemli ilke kararları verilmiştir.

2026 yılının ilk yarısında ise veri koruma hukukunda kullanıcı doğrulama, biyometrik veri işleme, açık rıza süreçleri ve yapay zekâ sistemlerinin denetimi ön plana çıkmıştır. Sadakat kartı doğrulama süreçleri, biyometrik verilerle mesai takibi ve aydınlatma metinlerinin açık rıza metinlerinden ayrılması konularında yeni ilke kararları yayımlanırken; Google Assistant, Grok ve çocukların kişisel verilerinin işlenmesine ilişkin resen incelemeler, yapay zekâ ve dijital platformların daha sıkı denetleneceğinin sinyallerini vermiştir. Bunun yanında Anayasa Mahkemesi'nin Viennalife kararı, KVKK kapsamındaki idari para cezalarının kanuni dayanağına ilişkin önemli bir tartışma başlatmış; Siber Güvenlik Kanunu ve Siber Güvenlik Başkanlığı'nın kurulması ise veri güvenliği, kritik altyapılar ve siber dayanıklılık alanlarında yeni yükümlülükler getirerek Türkiye'nin dijital düzenleme çerçevesini önemli ölçüde güçlendirmiştir.

GÜN + PARTNERS

İçindekiler

Türkiye'de Kişisel Verilerin Korunması Hukukundaki Gelişmeler

2025 yılı Kişisel Verileri Koruma Kurumu'nun ("**Kurum**") veri sorumlularına yönelik yol gösterici mahiyetteki rehber ve yayınları, Kişisel Verileri Koruma Kurulu'nun ("**Kurul**") ilke kararları ve kamuoyu duyuruları, kişisel verilerin korunması alanındaki farkındalığın ve etkinliğin artırılmasına yönelik çalışmalar ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**Kanun**") etkin bir şekilde uygulanması ve başta rekabet, siber güvenlik, yapay zekâ, dijital etik ve diğer ilgili hukuk alanları ile kesişim noktalarının doğru biçimde ele alınmasına yönelik önemli gelişmelerin yaşandığı bir yıl oldu.

2025 yılında Türkiye'de yapay zekâ alanında düzenleyici çerçevenin oluşturulması bakımından önemli adımların atılmaya devam edildi. Her ne kadar henüz kapsamlı ve müstakil bir yapay zekâ kanunu yürürlüğe girmemiş olsa da, kanun teklifleri, ulusal yapay zeka eylem planları, veri koruma otoritesinin yaklaşımı ve bu alana özgü yayınladığı rehber ve yayınlar, Avrupa Birliği düzenlemelerinin etkisi birlikte değerlendirildiğinde, Türkiye'nin yakın gelecekte daha bütüncül, risk temelli ve uluslararası standartlarla uyumlu bir yapay zekâ düzenlemesini gündeme alma yolunda olduğunu gösterdi.

Veri sorumluları için özellikle yurt dışına veri aktarımı da dahil yoğun uyum çalışmalarının yürütüldüğü bir dönem oldu.
Kullanıcıların hayatlarında her geçen gün daha da merkezi bir rol oynayan ve büyük ölçekli veri toplama, işleme ve paylaşma süreçleri nedeniyle bireylerin mahremiyetine yönelik riskleri açısından, dijital platformlar özellikle Kurul'un odağında yer aldı.

Kurum'un yayımladığı 2025 yılına ilişkin faaliyet raporu, kişisel verilerin korunması alanında hem denetim ve yaptırım faaliyetlerinin hem de rehberlik ve farkındalık çalışmalarının yoğun şekilde devam ettiğini işaret ediyor. 2024 yılında yürürlüğe giren önemli Kanun değişikliklerinin ardından, 2025 yılı uygulamada özellikle yurt dışına veri aktarımı, standart sözleşmeler, VERBİS yükümlülükleri, veri ihlali bildirimleri ve ilgili kişi başvuruları bakımından yeni uygulama

eğilimlerinin daha görünür hale geldiği bir yıl oldu. Kurum'un 2025 yılına ilişkin raporunda yayımladığı veriler, bir yandan veri sorumluları nezdinde uyum farkındalığının arttığını, diğer yandan ise özellikle usuli yükümlülükler, sicile kayıt/bildirim yükümlülüğü ve veri güvenliği süreçleri bakımından yaptırım riskinin önemini koruduğunu ortaya koymaktadır.

2025 Yılı Kurul Verileri

Bu çerçevede, 2025 yılı içerisinde Kurul tarafından toplamda 876 veri sorumlusu hakkında 352.510.494 TL idari para cezası uygulandığı Kurum'un yıllık raporunda ifade edilmiştir. İlgili cezaların dağılımına bakıldığında ise cezaların ağırlıklı olarak veri sorumluları siciline ve bildirim yükümlülüğünü aykırı hareket etme kapsamında verildiği görülmektedir.

2025 yılında Kurum'a 12.512 ihbar ve şikâyet intikal ettiği; geçmiş yıllardan devrolan dosyalarla birlikte toplam 15.578 dilekçe hakkında inceleme süreci yürütüldüğü belirtilmiştir. Sonuçlandırılan başvuruların büyük çoğunluğunun usul şartlarını taşımaması veya Kanun kapsamı dışında kalması nedeniyle reddedilmiş olması, ilgili kişi haklarının doğru kullanımı konusunda farkındalık ihtiyacının devam ettiğini göstermektedir.

Veri ihlalleri bakımından 2025 yılında Kurum'a 328 veri ihlali bildirimi yapıldığı belirtilmiş; bunların 105'i sonuçlandırılmış, 51'i Kurum tarafından ilan edilmiş ve 223'ünün incelemesi yıl sonu itibarıyla devam etmiştir. Bu veriler, veri sorumluları açısından veri ihlali müdahale planlarının, iç bildirim mekanizmalarının ve Kurum'a bildirim süreçlerinin önemini koruduğunu ortaya koymaktadır.

Yurt dışına veri aktarımı alanında ise standart sözleşme mekanizmasının uygulamada önemli ölçüde benimsendiği görülmektedir. 2025 yılında Kurum'a 2.497 standart sözleşme bildirimi yapıldığı belirtilmiştir. Buna karşılık, taahhütname mekanizması bakımından 90 başvurudan yalnızca 13'üne izin verilmiş, 76 başvuru reddedilmiş ve 1 başvurunun incelemesi devam etmiştir. Bu durum, standart sözleşmelerin yurt dışına aktarım süreçlerinde daha pratik ve yaygın bir uygun güvence aracı haline geldiğini göstermektedir. Ayrıca Kurul'a kendisine sunulan yurt dışına veri aktarım hususundaki bağlayıcı şirket kurallarını 20 Mayıs 2026'da onaylandığı duyurulmuştur. Bu Kurul tarafından onaylanan ilk bağlayıcı şirket kuralıdır.

Veri İhlal Bildirimlerinin Yayınlanmasında Yeni Karar

2025 yılında Kurum'un veri ihlal bildirimlerinin web sitesinde yayınlanması ile ilgili yaklaşımında önemli bir değişiklik meydana gelmiştir. Kurum internet sitesinde yayınlanmasına karar verilen veri ihlal bildirimleri bakımından süresiz ilan uygulamasına son vererek, bu süreyi 1 ay ile sınırlamıştır ve Kanun'un temel ilkeleriyle daha uyumlu bir yaklaşım sunmuş, veri sorumluları üzerindeki orantısız itibar etkilerini azaltarak marka ve ticari itibarlarının korunmasına katkı sağlamıştır.

Önemli Rehberler

Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi güncellenmiş, özel nitelikli kişisel verilerin işlenmesi ile ilgili kanun değişikliği ile uyumlu olarak, özel nitelikli kişisel verilerin işlendiği durumlarda veri sorumlularının doğru hukuki sebeplere dayalı olarak özel nitelikli kişisel veri işlemeleri ve Kanun'a uygun şekilde yükümlülüklerini yerine getirmeleri için yol gösterici olması amacıyla Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber hazırlanmıştır.

Bireylerin para havalesi hizmetleri, POS hizmetleri, fatura aracılık hizmetleri ve mobil ödeme hizmetleri gibi hizmetlerden yararlanırken kişisel verilerinin korunması ve ilgili sektörde faaliyet gösteren veri sorumlularına yol gösterilmesi amacıyla Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi yayınlanmıştır.

Üretken yapay zekâ sistemlerinin kişisel verilerin korunması bağlamındaki etkilerinin değerlendirilmesi, bu sistemlerin geliştirilmesi ile kullanılmasında bireylerin mahremiyetine saygılı bir yaklaşımın teşvik edilmesi ve yaşam döngüsü boyunca gerçekleştirilen kişisel veri işleme faaliyetleri bakımından veri sorumlusu niteliğini haiz aktörlere yol gösterilmesi amacıyla "Üretken Yapay Zekâ ve Kişisel Verilerin Korunması Rehberi yayınlanmıştır.

İlke Kararları ve Kamuoyu Duyuruları

Kurul, Haziran 2025'te yayınlanan **Ürün ve Hizmet Sunumu Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesi Hakkında 10/06/2025 Tarihli ve 2025/1072 sayılı İlke Kararı** ile ürün ve hizmet sunumu sırasında ilgili kişilere SMS ile doğrulama kodu gönderilmesi suretiyle kişisel verilerin işlenmesine ilişkin yaygın uygulamalardaki hukuka aykırılıkları gidermeyi amaçlamıştır.

Karar, özellikle doğrulama kodlarının gerçekte ticari elektronik ileti izni veya açık rıza almak amacıyla kullanılması ve bu sürecin hizmetin zorunlu bir parçası gibi sunulmasını eleştirmekte; bu tür uygulamaların açık rızanın özgür iradeye dayanması ve bilgilendirmeye dayalı olması şartlarını ihlal ettiğini ortaya koymaktadır. Bu kapsamda Kurul, SMS doğrulama kodunun amacı ve sonuçları hakkında ilgili kişilere açık ve anlaşılır şekilde aydınlatma yapılmasını, farklı veri işleme faaliyetleri (örneğin üyelik, veri işleme izni ve ticari ileti onayı) için ayrı ayrı açık rıza alınmasını ve ticari ileti izninin ürün veya hizmet sunumunun zorunlu unsuru gibi sunulmamasını zorunlu kılmıştır.

Aralık 2025'te yayınlanan **Turizm ve Otelcilik Sektöründe Konaklama Hizmeti Alan Kişilerin T.C. Kimlik Belgesi Fotokopisinin Kaydedilmesi Hakkında İlke Kararı** ile konaklama hizmeti alan kişilerden kimlik belgesi fotokopisi alınmasının gereğinden fazla veri işleme teşkil ettiğini ve bu işlem için herhangi bir hukuki dayanak bulunmadığı değerlendirilmiştir. Ayrıca kimlik fotokopilerinde yer alabilecek din, kan grubu

gibi özel nitelikli kişisel verilerin de işlenmesi riski bulunduğuna dikkat çekilmiştir. Bu çerçevede Kurul, konaklama tesislerinin kimlik fotokopisi alma uygulamasına son vermesi ve geçmişte bu şekilde elde edilen verilerin Kanun'un 7. maddesi uyarınca imha edilmesi gerektiğine karar vermiştir.

Kurum, Ocak 2025'te yayınladığı "**Arabuluculuk Faaliyetleri Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmesine" İlişkin Kamuoyu Duyurusu**'nda arabuluculuk faaliyetleri kapsamında işlenen kişisel verilere ilişkin arabulucu tarafından Kanun'un 10 uncu maddesinde sayılan hususlarda ilgili kişilere ayrıca bilgi verilmesi suretiyle aydınlatma yükümlülüğünün yerine getirilmesi gerektiği belirtilmiştir.

Ağustos 2025'te alacaklı vekilleri tarafından yürütülen mesleki faaliyetler sırasında borcun tahsiline yönelik yapılan iş ve işlemlerde, borçlu sıfatını haiz ilgili kişilerin ve konu ile ilgisi olmayan ilgili kişinin yakını sıfatını haiz üçüncü kişilerin kişisel verilerinin işlenmesi bakımından Kanun'a uygun şekilde kişisel veri işleme faaliyetinin gerçekleştirilmesi için **Alacaklı Vekilleri Tarafından Borçlu Olan İlgili Kişilerin Yakınlarına Ait Telefon Numaralarına Erişilmek Suretiyle Borç Bilgisinin Paylaşılmasına İlişkin Kamuoyu Duyurusu** yayınlanmıştır.

Son Gelişmeler - 2026 İlk yarısı- Önemli İlke Kararları

Sadakat Kart Üyeliği Bulunan Bir Kişinin Cep Telefonu Numarasının veya Sadakat Kart Numarasının Üçüncü Bir Kişi Tarafından Alışveriş Esnasında Kullanılması Hakkında Kişisel Verileri Koruma Kurulunun 11/02/2026 Tarihli ve 2026/266 sayılı İlke Kararı ile, sadakat kart numarası veya cep telefonu numarası kullanılarak üçüncü kişiler tarafından doğrulama yapılmaksızın alışveriş yapılmasına imkân tanıyan uygulamaların hukuka aykırı olduğu değerlendirilmiş ve veri sorumlularına, işlemlerin ilgili kişinin bilgisi ve rızası dahilinde gerçekleştiğini teyit edecek etkin doğrulama mekanizmaları kurma yükümlülüğü getirilmiştir. Bu karar, veri güvenliği yükümlülüklerinin yalnızca teknik tedbirlerle sınırlı olmadığını, aynı zamanda kullanıcı işlemlerinin doğruluğunu ve yetkilendirilmesini sağlayacak süreçleri de kapsadığını açıkça ortaya koymaktadır ve 2026 yılı itibariyle veri koruma hukuku alanında çalışan profesyonellerin en önemli gündem maddelerinden biri olmuştur.

Veri Sorumluları Tarafından Açık Rıza ve Aydınlatma Metinlerinin Ayrı Ayrı Düzenlenmesi Gerektiği Hakkında Kişisel Verileri Koruma Kurulunun 18.02.2026 Tarihli ve 2026/347 Sayılı İlke Kararı ile uygulamada doğru şekilde uygulanmadığı görülen aydınlatma metinlerinin rıza metinlerinden ayrı şekilde hazırlanması konusunda detaylı açıklamalarda bulunulmuştur.

Mesai Takibi Amacıyla Biyometrik Veri İşlenmesi Hakkında Kişisel Verileri Koruma Kurulunun 29.04.2026 Tarihli ve 2026/921 Sayılı İlke Kararı ile biyometrik verilerin

işyerinde mesai takibi amacıyla işlenmesi detaylıca ele alınmıştır ve genel ilkelere işaret edilerek biyometrik veri gibi özel nitelikli verilerin işlenmesindeki kısıtlamalara yer verilmiştir.

Kurum'un yapay zekâ temelli sistemlere ilişkin yaklaşımının da 2026 yılında daha görünür hâle geleceği beklenmektedir. Yılın ilk çeyreğindeki gelişmeler bu öngörüyü destekler nitelikte olup, **Google Assistant hakkında yayımlanan kamuoyu duyurusunda**, cihazların yanlış tetiklenmesi sonucu kullanıcıların özel konuşmalarının izinsiz kaydedildiği iddiaları üzerine re'sen inceleme başlatıldığı belirtilmiş; bu durum, yapay zekâ destekli sesli asistanların mahremiyet, veri güvenliği ve hukuka uygunluk bakımından doğrudan denetim konusu hâline geldiğini göstermiştir.

Benzer şekilde **Grok yapay zekâ sistemine ilişkin kamuoyu duyurusunda** da kullanıcı verilerinin model eğitimi amacıyla işlenmesine yönelik uygulamalar inceleme konusu yapılmış; şeffaflık ve kullanıcı kontrolü (opt-out mekanizmaları) eksikliklerinin önemli bir uyum riski oluşturduğu vurgulanmıştır.

2026'nın dikkat çeken bir diğer gelişmesi ise çocukların dijital ortamda korunmasına yönelik artan düzenleme eğilimidir. Kurum tarafından Şubat 2026'da yayımlanan duyuruda, çocukların sosyal medya kullanımında kişisel verilerinin işlenmesine ilişkin olarak başta büyük platformlar olmak üzere çeşitli hizmet sağlayıcılar hakkında re'sen inceleme başlatılmıştır. Bu gelişme, veri koruma hukukunda "çocuğun üstün yararı" ilkesinin artık daha aktif şekilde uygulandığını ve özellikle platform ekonomisinin çocuk kullanıcılar bakımından daha sıkı bir denetime tabi tutulacağını göstermektedir.

Tüm bu gelişmeler birlikte değerlendirildiğinde, veri koruma hukukunun; yalnızca klasik veri işleme faaliyetlerinden ziyade, yapay zekâ uygulamaları, kullanıcı doğrulama süreçleri, dijital platformlar ve hassas kullanıcı grupları (özellikle çocuklar) gibi alanlara odaklanan daha dinamik ve müdahaleci bir yapıya evrildiği görülmektedir. Önümüzdeki dönemde, bu yaklaşımın daha da güçlenerek devam etmesi, özellikle yapay zekâya özgü düzenlemelerin somutlaşması ve sektörel bazda daha detaylı yükümlülüklerin gündeme gelmesi beklenmektedir.

Yeni Gelişmeler – Anayasa Mahkemesi Kararı- Suçta ve Cezada Kanunilik ilkesi

Anayasa Mahkemesi'nin 27.01.2026 tarihli ve 2020/32193 başvuru numaralı Viennalife Emeklilik ve Hayat A.Ş. başvurusuna ilişkin kararı, 16.06.2026 tarihli ve 33282 sayılı Resmî Gazete'de yayımlandı. Kararda, kişisel verilerin hukuka aykırı işlenmesinin önlenmesi yükümlülüğü kapsamında uygulanan idari para cezası yönünden suçta ve cezada kanunilik ilkesinin ihlal edildiğine hükmedilerek Kurum'un şimdiye kadar uygulayageldiği idari para cezalarının dayanağının kanunda

yer almadığına işaret edildi ve bu karar önemli tartışmaları beraberinde getirdi. Bu karar kabahatlerin Kanun kapsamında daha detaylı düzenlenmesi yönündeki ihtiyacın altını çizmiştir ve bu vesile ile GDPR'a uyum değişikliklerini de hızlandırabilir şeklinde yorumlanmaktadır.

Siber Güvenlik Kanunu – Siber Güvenlik Kurumu

2025 yılında yürürlüğe giren ve Türkiye'nin ilk detaylı siber güvenlik düzenlemelerini içeren Siber Güvenlik Kanunu ile siber uzayda faaliyet gösteren kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşları geniş şekilde kapsamına almakta; kritik altyapılar, kritik kamu hizmetleri, siber olaylar, veri ve log kayıtları, siber tehdit istihbaratı ve siber dayanıklılık gibi konuları düzenlemektedir.

Kanun kapsamında yine 2025 yılında Siber Güvenlik Başkanlığı (SGB) kurulmuştur. Dijital Dönüşüm Ofisi de kapatılarak yetkileri SGB'ye devredilmiştir. Bu düzenleme, veri güvenliği, kritik altyapı, log yönetimi, olay müdahalesi ve veri yönetişimi konularını dijital dönüşüm projelerinin ayrılmaz parçası haline getirmektedir. Veri güvenliği ve dijital altyapı konusunda teknik ve idari yükümlülükler getiren düzenleme yeni denetim ve bildirim yükümlülükleri ile idari para cezası yaptırımlarını içermektedir.

2026 yılının ortasında ise Meclise sunulan teklif ile Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) internet ile ilgili olan yetkileri SGB kapsamı ve yetkisi altına girmesi amaçlanmaktadır. BTK'nın ise elektronik haberleşme ile ilgili piyasa düzenleyicisi yapısının güçlendirilmesi 5651 sayılı Internet Kanunu'nun icracısının da SBG olması amaçlanmaktadır. Bu şekilde, SBG'nin dijital alanda geniş yetkileri haiz olacağı görülmektedir.

Türkiye'de Kişisel Verilerin Korunması - Genel Yaklaşım, Güncel Uygulamalar ve Özel Nitelikli Kişisel Verilerin İşlenmesi

Türkiye'de kişisel verilerin korunmasına ilişkin temel düzenleme 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur ("Kanun").

95/46/EC sayılı Avrupa Konseyi Veri Koruma Direktifi temel alınarak hazırlanan Kanun, 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ("GDPR") hükümlerinden ve uygulaması ise hem GDPR hem de Avrupa veri koruma otoritelerinin kararlarından etkilenmektedir.

Kanun, GDPR ile benzer amaç ve temel kavramları benimsemekte, kişisel verilerin korunmasına ilişkin temel prensipler açısından oldukça benzer düzenlemeler içermektedir. Bununla birlikte Kanun'un genel itibariyle GDPR'a nazaran daha sınırlı, kontrolcü ve daha az detaylı bir yapıya sahiptir.

Avrupa veri koruma hukuku gelişmeleri ve yaklaşımları Kişisel Verileri Koruma Kurumu ("Kurum") tarafından takip edilmektedir.

2024 yılında yürürlüğe giren 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ("Değişiklik"), Türkiye'de kişisel verilerin korunması hukukunun GDPR standartlarına yakınlaştırılması bakımından bugüne kadarki en önemli adımlardan biri olmuştur.

Değişiklik Kanunu ile özel nitelikli kişisel verilerin işlenmesi, yurt dışına veri aktarımı, idari yaptırımlar ve idari para cezalarına karşı yapılacak başvurular bakımından önemli değişiklikler 1 Haziran 2024 tarihinde yürürlüğe girmiştir. Değişiklik ile paralel olarak Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik de hazırlanmış ve 10 Temmuz 2024 tarihli Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Kurul'un 2025 yılı ve 2026 başındaki karar ve duyuruları, özellikle uygulamada karşılaşılan problemli konuları ele almaktadır. Bunların başında aydınlatma yükümlülüğü, açık rıza,

ticari elektronik ileti onayı ve pazarlama izinlerinin birbirine karıştırılması gelmektedir.

Kurul, ürün ve hizmet sunumu sırasında ilgili kişilere SMS ile doğrulama kodu gönderilmesine ilişkin ilke kararında, ödeme, üyelik, kayıt açma veya fatura oluşturma gibi işlemler sırasında gönderilen SMS kodlarının amacının ilgili kişilere açıkça bildirilmesi gerektiğini; üyelik sözleşmesi onayı, kişisel veri işleme izni ve ticari elektronik ileti onayı gibi farklı hukuki işlemlerin tek bir eylemle alınmasına yönelik uygulamalara son verilmesi gerektiğini vurgulamıştır. Bu yaklaşım, açık rızanın belirli bir konuya ilişkin, bilgilendirmeye dayalı ve özgür iradeyle açıklanmış olması gerektiği yönündeki temel ilkenin uygulamadaki somut yansımasıdır.

Benzer şekilde, 2026 başında mobil uygulamalar üzerinden gönderilen anlık bildirimlere ilişkin yayımlanan kamuoyu duyurusunda da operasyonel bildirimler ile reklam, kampanya ve pazarlama amaçlı bildirimlerin tek bir onay altında birleştirilmesinin hukuka uygun olmayacağı belirtilmiştir. Sipariş durumu, kargo takibi veya hizmetin ifasıyla doğrudan bağlantılı bildirimler ile kampanya ve reklam bildirimleri farklı amaçlara hizmet etmektedir. Bu nedenle, kullanıcıların hizmetten yararlanabilmek için pazarlama bildirimlerini kabul etmek zorunda bırakılması, açık rızanın özgür irade unsurunu zedeleyebilecektir. Bu doğrultuda veri sorumlularının, özellikle dijital platformlar ve mobil uygulamalar bakımından, tercih yönetimi mekanizmalarını "parçalı açık rıza" ve "belirlilik" ilkelerine uygun şekilde tasarlamaları gerekmektedir.

Kurul'un turizm ve otelcilik sektöründe konaklama hizmeti alan kişilerin T.C. kimlik belgesi fotokopisinin kaydedilmesine ilişkin ilke kararı da 2025 yılındaki önemli diğer gelişmelerden biridir. Kurul, konaklama hizmeti bakımından kimlik bilgilerinin kaydedilmesinin mevzuattan kaynaklanan yükümlülükler çerçevesinde hukuka uygun olabileceğini kabul etmekle birlikte, kimlik belgesinin fotokopisinin alınarak kayda geçirilmesinin gereğinden fazla veri işlenmesi sonucunu doğurduğunu ve bu uygulamanın hukuki dayanağının bulunmadığını değerlendirmiştir. Bu karar, veri minimizasyonu, işleme amacıyla bağlantılılık ve ölçülülük ilkelerinin günlük ticari uygulamalarda da sıkı şekilde gözetilmesi gerektiğini göstermektedir.

Özel nitelikli kişisel verilerin işlenmesi de 2025 yılında Kurum'un özellikle üzerinde durduğu alanlardan biri olmuştur. Kanun'da özel nitelikli kişisel veriler; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler olarak sınırlı şekilde sayılmıştır.

Değişiklik Kanunu öncesinde özel nitelikli kişisel verilerin işlenmesi bakımından uygulama büyük ölçüde açık rıza ekseninde şekillenmekte; özellikle açık rızanın pratik veya

hukuken sağlıklı bir dayanak olmadığı işçi-işveren ilişkileri, sağlık verisi işleme süreçleri ve kanuni yükümlülüklerden kaynaklanan işleme faaliyetleri bakımından önemli sorunlar yaşanmaktaydı.

Değişiklik ile özel nitelikli kişisel verilerin işlenme şartları genişletilmiş, sağlık ve cinsel hayata ilişkin veriler ile diğer özel nitelikli kişisel veriler arasındaki önceki ayrım kaldırılmıştır. Böylece tüm özel nitelikli kişisel veriler bakımından uygulanabilecek daha geniş bir hukuki sebep seti oluşturulmuştur. İlgili kişinin açık rızası halen geçerli bir işleme şartı olmakla birlikte; kanunda sayılan hukuki sebeplerin mevcut olduğu durumlarda açık rıza almaksızın veri işlenmesi öncelikli uygulama haline gelmiştir. Buna göre, (sağlık verileri ve cinsel hayata ilişkin kişisel veriler de dahil) tüm özel nitelikteki kişisel veriler, aşağıdaki hukuki nedenlerin bulunması durumunda işlenebilecektir:

i. İlgili kişinin açık rızasının olması,
ii. Kanunlarda açıkça öngörülmüş olması,
iii. Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
iv. İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,
v. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
vi. Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,
vii. İstihdam, iş ve sosyal güvenlik veya sosyal hizmetler alanındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,
viii. Siyasi parti, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kar amacı gütmeyen kuruluş ya da oluşumların, tabi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması.

2025 yılında yayımlanan Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber, bu değişikliklerin uygulamadaki karşılığını biraz daha detaylandırmıştır. Rehber'de açık rıza ile diğer işleme şartları arasında hiyerarşik bir fark bulunmadığı; ancak açık rıza dışında uygun bir işleme şartı mevcutsa, veri sorumlusunun ayrıca açık rızaya başvurmaması gerektiği vurgulanmıştır. Bu yaklaşım, uygulamada sık görülen "her ihtimale karşı açık rıza alma" pratiğinin hukuka ve dürüstlük kuralına aykırılık riski yaratabileceğini göstermektedir.

Dolayısıyla veri sorumlularının her bir özel nitelikli kişisel veri işleme faaliyeti bakımından somut hukuki sebebi ayrı ayrı tespit etmesi, açık rızayı yalnızca gerçekten gerekli olduğu hallerde kullanması ve aydınlatma metinlerini bu hukuki sebebe uygun şekilde kurgulaması gerekmektedir.

Bu kapsamda veri sorumlularının mevcut uyum dokümanlarını yalnızca şeklen güncellemesi yeterli olmayacaktır. Özel nitelikli kişisel veri işleme süreçleri bakımından kişisel veri işleme envanterlerinin, aydınlatma metinlerinin, açık rıza metinlerinin, saklama ve imha politikalarının ve veri güvenliği tedbirlerinin yeniden değerlendirilmesi gerekmektedir.

Özellikle istihdam süreçlerinde iş sağlığı ve güvenliği yükümlülükleri kapsamında işlenen sağlık verileri, çalışanların ceza mahkûmiyeti veya güvenlik tedbiri bilgileri, sendika üyeliği verileri, biyometrik erişim sistemleri ve sağlık sektöründeki veri işleme faaliyetleri bakımından açık rıza dışındaki hukuki sebeplerin uygulanabilirliği dikkatle analiz edilmelidir.

Sonuç olarak, 2025 yılı ve 2026 başındaki gelişmeler, Kurul'un son karar ve duyuruları, veri sorumlularının artık yalnızca genel nitelikli aydınlatma metinleri ve standart açık rıza formlarıyla yetinemeyeceğini; her veri işleme faaliyetinin amacı, hukuki sebebi, ilgili kişi üzerindeki etkisi, veri minimizasyonu ve tercih yönetimi mekanizmaları bakımından ayrı ayrı değerlendirilmesi gerektiğini ortaya koymaktadır. Özellikle özel nitelikli kişisel veriler bakımından uyum çalışmalarının belge bazlı değil, süreç bazlı şekilde yürütülmesi 2026 yılı bakımından da veri sorumlularının en önemli gündem maddelerinden biri olmaya devam etmesi beklenmektedir.

Kişisel Verilerin Yurt Dışına Aktarımı

Değişiklik öncesi dönemde Kanun uyarınca kişisel veriler çoğunlukla veri sahibinin açık rızası ile yurtdışına aktarılabilmekteydi çünkü mevzuatta yer alan diğer hukuki nedenlerin uygulama alanı ya mevcut değil ya da uygulanabilir değildi. Kanun'un yayım tarihi olan 2016'dan bu yana Kurul tarafından, yeterli koruma sağlayan ülkelerin bir listesinin halen belirlenmemiş olması, uygulamada yurtdışına kişisel veri aktarımı hususunu oldukça dar ve zorlu bir alana sıkıştırmaktaydı ve açık rıza alınması yurtdışına kişisel veri aktarımı konusunda uygulanabilecek tek yöntem olarak kalmasına sebebiyet vermekteydi.

Ticari ilişkileri de olumsuz yönde etkileyen bu konuya ilişkin önemli adımlar da Değişiklik ile birlikte 1 Haziran 2024 tarihinde yürürlüğe girmiştir.

Değişiklik ile yurtdışına veri aktarımı açısından üç aşamalı bir değerlendirme sistemi öngörülmüştür. Bu çerçevede, yürürlüğe giren değişiklikler ile kişisel verilerin, Kanun'daki hukuki işleme sebeplerinden birinin varlığı halinde, Kurul tarafından verilecek yeterlilik kararının bulunması durumunda yeterlilik kararının kapsamına uygun olarak yurt dışına aktarılabileceği , yeterlilik kararının bulunmadığı hallerde ise, yine Kanun'daki işleme şartlarından birinin varlığına ek olarak, ilgili kişinin aktarım yapılacak ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla uygun güvencelerden birinin sağlanması gerekmektedir.

Uygun güvencelerin de sağlanamadığı hallerde ise ancak arızi olmak kaydıyla sınırlı istisnalara başvurulabilecektir.

Değişiklik ile birlikte uygun güvenceler; kamu kurum ve kuruluşları veya uluslararası kuruluşlar arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmalar, bağlayıcı şirket kuralları, standart sözleşmeler ve Kurul tarafından izin verilen taahhütnameler olarak düzenlenmiştir. Bu yönüyle Kanun, yurt dışına aktarım rejimini açık rıza merkezli bir yapıdan çıkararak, GDPR'a daha yakın, kurumsal güvence mekanizmalarına dayalı bir yapıya taşımıştır.

2025 yılı, bu yeni yurt dışına veri aktarım

sistematiğinin uygulamadaki ilk tam yılı olması bakımından önem taşımaktadır. Kurum'un 2025 Yılı Faaliyet Raporu'na göre, yıl içinde Kurum'a 2.497 standart sözleşme bildirimi yapılmıştır. Buna karşılık, taahhütname mekanizması bakımından 2025 yılında Kurum'a 90 başvuru yapılmış; bunlardan 13'ü bakımından aktarıma izin verilmiş, 76'sı bakımından izin verilmemiş, 1 başvurunun incelemesi ise yıl sonu itibarıyla devam etmiştir.

Bu tablo, taahhütname mekanizmasının daha sınırlı ve sıkı değerlendirmeye tabi bir yöntem olmaya devam ettiğini; standart sözleşmelerin ise uygulamada en pratik ve yaygın uygun güvence aracı haline geldiğini göstermektedir. Kurum'un 2025 yılında yayımladığı faaliyet raporunda Kurum'a intikal eden standart sözleşme bildirimlerinden 70'i hakkında resen inceleme başlatıldığı, bunların 21'i sonuçlandırıldığı ve sonuçlandırılan incelemelerin 3'ünde toplam 150.000 TL idari para cezası uygulandığı belirtilmiştir.

Söz konusu eksikliklerin ve kesilen cezaların daha çok gerekli usuli süreçlerin yerine getirilmemesinden, Kurula zamanında bildirim yapılmamasından ileri geldiği görülmektedir.

Kurum'un 2026 yılında bir bağlayıcı şirket kuralları başvurusunun Kurul tarafından onaylandığını duyurması ise, özellikle çok uluslu şirket grupları bakımından bağlayıcı şirket kurallarının da daha somut bir aktarım mekanizması olarak kullanılmaya başlanabileceğine işaret etmektedir. Hazırlık ve onay süreçlerinin standart sözleşmelere kıyasla daha uzun ve kapsamlı olması beklense de bağlayıcı şirket kuralları grup içi veri aktarımları bakımından daha kalıcı ve kurumsal bir çözüm sunabilecek nitelikte olabileceği de göz önünde bulundurulmalıdır.

Yeni yurt dışı veri aktarım sistematiğinde açık rıza artık olağan ve düzenli aktarımlar için temel dayanak olmaktan çıkarılmıştır. Açık rızaya dayalı yurt dışı aktarım, yeterlilik kararı bulunmaması ve uygun güvencelerden birinin sağlanamaması halinde, ancak ilgili kişinin muhtemel riskler hakkında bilgilendirilmesi koşuluyla ve ancak arızi aktarım halleri için başvurulabilecek istisnai bir yöntem olarak düzenlenmiştir. Bu nedenle veri sorumlularının, süreklilik arz eden iş süreçleri kapsamındaki yurt dışı veri aktarımlarını açık rızaya dayandırmaya devam etmeleri önemli bir uyum riski yaratacaktır.

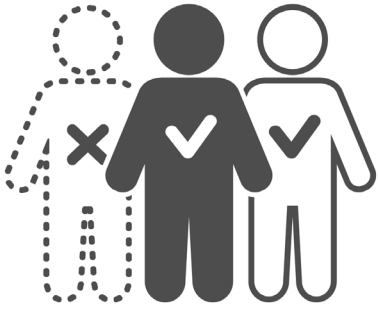
Türk hukukunda kişisel veriler bakımından genel ve mutlak bir veri lokalizasyonu yükümlülüğü bulunmamaktadır. Kanun, kişisel verilerin Türkiye'de saklanmasını genel bir kural olarak zorunlu kılmamakta; bunun yerine yurt dışına aktarımı belirli şartlara bağlamaktadır.

Buna karşılık, Türk hukukunda bazı sektörlerde açık veri lokalizasyonu veya yurt içinde sistem bulundurma yükümlülükleri mevcuttur. Bankacılık, ödeme ve elektronik para, sermaye piyasaları, elektronik haberleşme ve belirli kamu/kritik altyapı faaliyetleri bakımından sektörel düzenlemeler kapsamında bilgi sistemlerinin, birincil ve ikincil sistemlerin, yedeklerin, log kayıtlarının veya belirli kayıt ve belgelerin Türkiye'de tutulmasına ilişkin özel kurallar bulunmaktadır.

Bu sebeple, özellikle regüle sektörlerde faaliyet gösteren şirketlerin, yurt dışına veri aktarımı değerlendirmesini yalnızca Kanun'un 9'uncu maddesi çerçevesinde değil, ilgili siber güvenlik yükümlülükleriyle birlikte yapması gerekmektedir.

Sonuç olarak, 2025 yılı ve 2026 başındaki gelişmeler, Türkiye'de yurt dışına veri aktarımı rejiminin artık daha kurumsal, belgeli ve denetlenebilir bir yapıya dönüştüğünü göstermektedir. Her ne kadar bildirim ve bazı prosedürel yükümlülükler ile hala uygulama süreçte zorluklar yaşansa da, standart sözleşmeler uygulamada ana yöntem haline gelirken, bağlayıcı şirket kuralları ve kamu/uluslararası kuruluş anlaşmaları gibi diğer güvence mekanizmalarının da görünürlüğü artmaktadır.

Veri Sorumluları Sicili (VERBİS)



Kanun'un 16. maddesi uyarınca, belirlenen eşikleri aşan Türkiye'de mukim veri sorumluları ve yurt dışına mukim olan ve Türkiye'de veri sorumlusu olarak kişisel veri işleyen veri sorumluları için herhangi bir eşik kriterine tabi olmadan Veri Sorumluları Sicili'ne ("**VERBİS**") kayıt zorunluluğu bulunmaktadır.

Kamuya açık olarak tutulan VERBİS sistemine ilişkin usul ve esaslar ise 30 Aralık 2017 tarihli "Veri Sorumluları Sicili Hakkında Yönetmelik" ("**VERBIS Yönetmeliği**") ile belirlenmektedir. Kurul'un 2018 tarihli kararları ile çeşitli meslek grupları, dernekler, vakıflar, siyasi partiler VERBİS kayıt yükümlülüğünden muaf tutulmuş ve kayıt yükümlülüğü ile kayıt yükümlülüğünden istisna olacakların belirlenmesinde Türkiye'de yerleşik veri sorumluları açısından çalışan sayısı ve bilanço bazlı minimum kriterler getirmiştir.

Kurul'un 04.09.2025 tarih ve 2025/1572 sayılı Kararı ile ana faaliyet konusu özel nitelikli kişisel veri işleme olmakla birlikte yıllık çalışan sayısı 10'dan az ve yıllık mali bilanço toplamı 10 milyon Türk Lirasından az olan gerçek veya tüzel kişi veri sorumlularının da Sicile kayıt ve bildirim yükümlülüğünden istisna tutulmasına karar verilmiştir.

Mevcut durumda, yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 100 milyon Türk lirasından az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar ile ana faaliyet konusu özel nitelikli kişisel veri işleme olmakla birlikte yıllık çalışan sayısı 10'dan az ve yıllık mali bilanço toplamı 10 milyon Türk lirasından az olan gerçek veya tüzel kişi veri sorumluları VERBİS kayıt yükümlülüğünden istisnadır.

Kurul 04.09.2025 tarihli ve 2025/1572 sayılı kararının uygulanması ile ilgili iletilen görüş talepleri üzerine söz konusu kararın uygulama esaslarına ilişkin bir kamuoyu duyurusu yayınlamıştır. Buna göre, VERBİS kayıt yükümlülüğünden istisna olacak veri sorumlularının belirlenmesinde, bilanço esasına göre defter tutan veri sorumluları bakımından hem "yıllık çalışan sayısı" hem de "yıllık mali bilanço toplamı" kriteri kümülatif şekilde esas alınmakla birlikte, bilanço esasına göre defter tutmayan veri sorumluları bakımından yıllık mali bilanço toplamı bilgisi bulunmaması sebebiyle yalnızca "yıllık çalışan sayısı" kriterinin esas alınmasına karar verilmiştir.

Yurtdışında yerleşik veri sorumluları açısından ise VERBİS kayıt yükümlülüğün değerlendirilmesinde söz konusu kriterlerin uygulanmadığına dikkat edilmesi gerekmektedir.

Kurum 2025 yılında sicile kayıt ve bildirim yükümlülüğünün yerine getirilmesi hususunda veri sorumlularının faydalanmaları amacıyla yayımladığı Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) ve Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Kılavuzu'nu, VERBİS ekranlarında veri sorumlularının sisteme kayıt ve bildirim süreçlerini kolaylaştırmak amacıyla yapılan değişiklikler göz önünde bulundurularak güncellemiştir. Kurum "8.Yılında Kişisel Verileri Koruma Kurumu" isimli çalışmasında kuruluşundan bu yana gerçekleştirilen faaliyetler ve gelişmelere yönelik istatistikleri paylaşmış olup, 30.04.2025 tarihi itibariyle VERBİS kayıt başvurusu kapsamında 197.971 adet veri sorumlusunun kaydının yapıldığı belirtilmiştir.

2026 yılı için VERBİS kayıt yükümlülüğünün ihlali halinde uygulanması öngörülen idari para cezası aralığı 341.809 TL ile 17.092.242 TL olacaktır. Kurul, ceza miktarını belirlemek adına bazı algoritmalar kullanmaktadır ve buna göre belirtilen ceza aralığı içerisinde mali bilanço aktif toplamı ne kadar fazla ise belirlenecek ceza miktarı da üst sınıra o kadar yakın olarak belirlenmektedir.

Kurul, Türkiye'de yerleşik veri sorumlularını Sosyal Güvenlik Kurumu ve vergi dairelerine yaptıkları beyanlar ışığında aktif olarak takip etmekte ve eşikleri geçen veri sorumlularına kayıt yükümlülüklerini yerine getirmemeleri halinde uyarı vermeksizin idari para cezası verebilmektedir. Kurul aynı zamanda yurtdışında yerleşik olan ve Türkiye'de mukim kişilerin verilerini işleyen veri sorumlularını da araştırmakta ve bu veri sorumlularına da ceza uygulayabilmektedir. Dolayısı ile ceza riskini bertaraf edebilmek adına, kayıt yükümlülüğünün düzenli olarak kontrol ve takip edilmesi önerilmektedir.

Bu noktada belirtmek gerekir ki, Kanun, uyruğuna bakılmaksızın, Türkiye'de ikamet etmemelerine rağmen Türkiye'deki veri sahiplerini hedef alan veri sorumluları (Türkiye'de yerleşik veya Türkiye'ye mal ve hizmet sunan) bakımından da uygulama alanı bulmaktadır. Böylece, yurt dışında yerleşik veri sorumlularının Türkiye'de doğrudan ya da şubeleri aracılığıyla kişisel veri işleme faaliyetinde bulunmaları veyahut kendilerine aktarılan kişisel verileri kendi amaçları doğrultusunda işlemeleri halinde VERBİS'e kayıt yükümlülüğü doğmaktadır.

Yurtdışında yerleşik tüzel kişiler, kişisel verileri kendi amaçları doğrultusunda veri sorumlusu olarak işlemeleri halinde VERBİS'e kaydolmakla yükümlü olacaklardır. Bu noktada dikkat edilmesi gereken ayrım tüzel kişinin faaliyetlerinin Türkiye'deki veri sahiplerini hedefliyor olması ve ilgili kişisel verileri kendi amaçları doğrultusunda veri sorumlusu olarak işliyor olmasıdır. Kişisel verilerin sadece

yurt dışında yerleşik tüzel kişin veri kayıt sisteminde tutuluyor olması ise VERBİS yükümlülüğü doğurmayacaktır.

Son olarak belirtmekte fayda var ki, VERBİS'e kaydolmakla yükümlü bulunan yurtdışında yerleşik veri sorumluları VERBIS Yönetmeliği uyarınca Kurul, Kurum ve veri sahipleri ile olan ilişkilerinde bir iletişim noktası olarak hareket etmek üzere bir veri sorumlusu temsilcisi atamak zorundadır. Veri sorumlusu temsilcisi Türkiye'de yerleşik bir tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı bir gerçek kişi olabilir. Temsilci ataması veri sorumlusunun noter onaylı ve apostilli (veya başka biçimde tasdik ettirilmiş) kararı ile gerçekleştirilmelidir. Bir tüzel kişinin temsilci olarak atanması halinde, yabancı veri sorumlusu tarafından irtibat kişisi olarak görev almak üzere bir de gerçek kişi atanmalıdır.

Henüz VERBİS'e kaydolmayan yurt içinde yerleşik veri sorumlularının yıllık çalışan sayıları ve yıllık mali bilançoları verilerini her yıl değerlendirerek VERBİS kayıt yükümlülükleri olup olmadığını tespit etmeleri gerekmektedir. Özellikle yurt dışı veri aktarımlarında gerçekleşen gelişmeler çerçevesinde yurt dışı aktarımları ile ilgili imzalanan ve Kurum'a bildirilen standart sözleşmeler ile birlikte VERBIS yükümlülüğünü yerine getirmemiş olan veri sorumluları dikkat çekecektir. Dolayısıyla, veri sorumlusu olarak hareket eden ve yurtdışında bulunan kurumların VERBIS yükümlülüklerini kontrol etmesi ve en geç ilgili standart sözleşmelerin imzalanarak Kurum'a bildiriminin tamamlanmasından önce VERBIS kayıt yükümlülüğünün değerlendirilerek tamamlanmasını öneririz.

Yapay Zeka Alanında Kişisel Verilerin Korunması

Yapay zekanın kullanımının hızla yaygınlaşması ve hayatın her alanında kendine yer bulması ile birlikte, bu teknolojinin karmaşıklığı ve özel nitelikleri göz önünde bulundurularak, yapay zeka sistemlerinin güvenli ve etik bir şekilde geliştirilmesi, dağıtılması ve kullanılmasını düzenleyen yasal bir çerçevenin oluşturulması zorunlu hale gelmiştir.

Yapay zeka teknolojilerinin güvenli, şeffaf ve insan haklarına saygılı bir şekilde gelişimini teşvik etmenin yanı sıra kullanıcıların ve toplumun genel güvenliğini, haklarını ve özgürlüklerini korumayı hedefleyerek, yapay zekanın etik gelişimini ve kişisel verilerin korunmasını sağlamak üzere bu alandaki ilk detaylı yasal düzenleme niteliğini taşıyan ve 1 Ağustos 2024 tarihinde yürürlüğe giren Avrupa Birliği Yapay Zeka Yasası'dır ("AI Act"). Henüz Avrupa Birliği'ndeki gelişmelerin aksine Türkiye'de yapay zeka özelinde bir düzenleme bulunmamaktadır. Ancak Türkiye'de de yapay zeka uygulamalarının yaygınlaşmasıyla birlikte, bu alanda hukuki ve düzenleyici çerçevelerin oluşturulması gündeme gelen hususlardan biri olmuştur.

On İkinci Kalkınma Planı'nın (2024-2028) "2.1. Küresel Eğilimler ve Türkiye Etkileşimi" başlığı altında yer alan Düzenleyici, Denetleyici ve Güvenilir Kamu Yönetimi başlığı altında "Büyük miktarda verinin toplanması, depolanması ve işlenmesini sağlayan teknolojik gelişmeler ve dijitalleşme süreci; veri uygulamalarının güvenli, güvenilir ve etik bir şekilde yönetilmesini gerektirmekte, kişisel veri güvenliği ve mahremiyeti, siber güvenlik, yapay zekâ, dijital rekabet ve dijital etik gibi konularda kapsamlı ve yenilikçi kamu politikalarının geliştirilmesi ve yasal düzenlemelerin yapılması" hedefi, Türkiye'de dijital dönüşümün yalnızca teknolojik bir gelişim alanı olarak değil, aynı zamanda güçlü bir hukuki ve yönetişim çerçevesi gerektiren stratejik bir politika alanı olarak ele alındığını ortaya koymaktadır. Bu yaklaşım, Türkiye'nin düzenleyici perspektifinin Avrupa Birliği'ndeki risk temelli ve insan odaklı modele paralel şekilde şekillendiğini göstermekte; özellikle yapay zekâ ve veri ekonomisine ilişkin gelecekte daha bütüncül ve sektörel

etkileri gözeten bir mevzuat altyapısının oluşturulacağına işaret etmektedir.

Türkiye'de henüz yapay zekâya özgü bir mevzuat olmamasına rağmen veri koruma ve siber güvenlik bakımından dikkate değer gelişmeler bulunmaktadır. Kurum, üretken yapay zekâ uygulamalarının yenilikçi fırsatlar ve faydalar sunmakla birlikte etik, hukuki ve toplumsal açılardan bazı riskleri de beraberinde getirdiğini vurgulayarak bu uygulamaları geliştiren ve kullanan veri sorumluları için bir rehber oluşturmak adına 24 Kasım 2025 tarihinde Üretken Yapay Zekâ ve Kişisel Verilerin Korunması Rehberi'ni ("Rehber") yayınlamıştır.

Rehber, büyük veri kümeleri üzerinde eğitilen ve prompt'a yanıt olarak metin, görsel, video, ses ya da kod üretebilen sistemlere odaklanmakta; yalnızca teknolojiyi tanımlamakla kalmayıp aynı zamanda halüsinasyon, tutarsızlık, önyargı, veri gizliliği ve güvenliği, fikri mülkiyet ihlalleri ve deepfake gibi riskleri de veri koruma hukuku bakımından nasıl ele almak gerektiğini açıklamaktadır. Bu yönüyle Rehber teknik bir dokümandan ziyade veri sorumlularına yönelik yönlendirici bir uyum metni olarak değerlendirilebilir.

Rehber kapsamında, üretken yapay zekâ sistemlerinin eğitimi, değerlendirilmesi, izlenmesi ve kullanılması sırasında Türkiye'de mukim kişilere ait veriler sürece dahil oluyorsa, bu faaliyet KVKK anlamında bir kişisel veri işleme faaliyeti olarak görülmelidir. Ayrıca yalnızca anonim veya anonimleştirilmiş veri kullanıldığının ileri sürülmesinin tek başına yeterli olmadığı; anonimleştirmenin kendisinin de bir işleme faaliyeti olduğunu ve verinin gerçekten anonim sayılıp sayılmadığının teknik yöntemlerle nesnel biçimde ortaya konulması gerektiğini vurgulanmaktadır.

Üretken yapay zekâ ekosistemi çok katmanlı olduğundan, veri sorumlusu- veri işleyen sıfatlarının belirlenmesinde Rehber kritik bir ilke ortaya koyarak taraflar arasındaki sözleşmesel etiketlerden çok, veri işleme üzerindeki fiili kontrol ve karar alma gücünün esas alınması gerektiğini belirtmektedir.

Rehber'de yapay zekâ sisteminin yaşam döngüsündeki her adımın tek bir bütün işlem gibi değil, ayrı ayrı değerlendirilmesi gereken süreçler olarak ele alınması gerektiği: kullanıcının girdiği verinin modeli çalıştırmak için işlenmesi, bu verinin model geliştirmede kullanılması, model çıktısının kişiselleştirme amacıyla değerlendirilmesi veya çıktının yeniden model eğitimi için kullanılması gibi her aşamanın kendi başına ayrı hukuki sebep analizini gerektirdiği belirtilmiş olup, yapay zeka sistemleri bakımından veri sorumlularının kullanıcılara yapacakları bilgilendirmelerde "tek bir aydınlatma metni + tek bir hukuki sebep" yaklaşımıyla yetinmemeleri gerektiğini gösteren önemli değerlendirmelere yer verilmiştir.

Rehber'de özellikle üç uyum alanını öne çıkmış olup, şeffaflık, ilgili kişi haklarının

etkin kullanımı ve veri güvenliği özelinde aydınlatma yükümlülüğünün açık ve ayrı şekilde yerine getirilmesi, otomatik karar almaya dayalı süreçlerde bireylere itiraz ve yeniden değerlendirme imkânı tanınması, insan müdahalesi mekanizmalarının korunması, "tasarımdan itibaren mahremiyet" yaklaşımının benimsenmesi ve risk temelli güvenlik önlemlerinin uygulanması gerekmektedir.

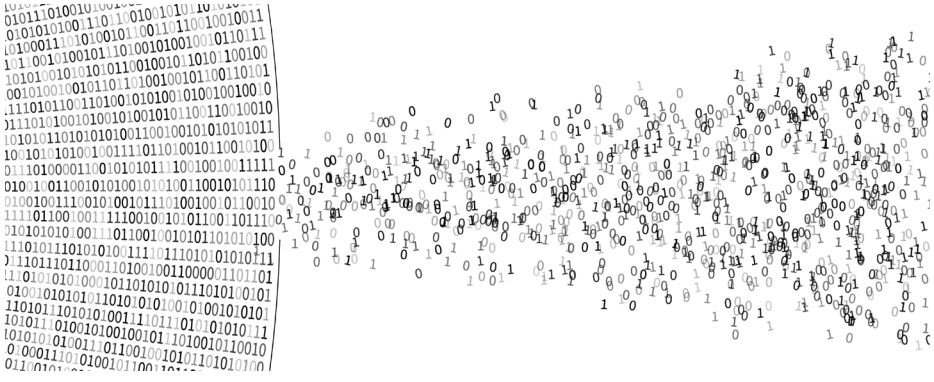
Kurum ayrıca, yapay zekâ teknolojilerinde kişisel verilerin korunmasına yönelik hukuki, teknik ve etik hususların alanında uzman akademisyenler tarafından çeşitli boyutlarıyla değerlendirildiği "Yapay Zeka Teknolojilerine Akademik Bakış" isimli kitap hazırlayarak yayınlamıştır.

2024 yılında sunulan ve AI Act düzenlemelerine paralel ama çok temel bir yaklaşımı benimseyen ilk yapay zekâ kanun teklifine ek olarak, 2025 yılında sunulan yeni bir kanun teklifinde de yapay zekâ sistemlerinin beraberinde getirdiği risklerin başka Türk Ceza Kanunu olmak üzere çeşitli kanunlar çerçevesinde ele alınması gerektiği vurgulanmış ve pek çok kanunda yapay zekaya doğrudan işaret eden ancak yaptırım odaklı düzenlemeler yapılması teklif edilmiştir.

Kanun teklifinde, kişisel verilerin korunması bakımından yapay zeka uygulamasında kullanılacak veri setlerinin anonimliği, ayrımcılık yasağı ve meşruiyet ilkelerine uygunluk, şeffaflık, denetlenebilirlik, yanlış, manipülatif ve halüsinasyon risklerinin engellenmesi vb. öncelikli konular ele alınmıştır.

Söz konusu kanun teklifinin mevcut hali ile yasalaşması beklenmemektedir. Türkiye'de önümüzde yapay zekâ hukuku bakımından "düzenleyici olgunlaşma ve uyum" sürecinin hız kazandığı bir geçiş dönemi olacağı kuşkusuzdur. Her ne kadar henüz kapsamlı ve müstakil bir yapay zekâ kanunu çalışmaları henüz başlamamış olsa da, kanun teklifleri, veri koruma hukuku uygulamaları ve Avrupa Birliği düzenlemelerinin etkisi birlikte değerlendirildiğinde, Türkiye'nin yakın gelecekte daha bütüncül, risk temelli ve uluslararası standartlarla sektör ihtiyaçlarına ve teknolojik gelişmeler ile uyumlu bir yapay zekâ düzenleme çerçevesine kavuşacağı öngörülmektedir.

Veri İhlali ve Doğuracağı Sonuçlar



Kanun, veri sorumlularının ilgili veri ihlalinden haberdar olunur olunmaz mümkün olan en kısa sürede Kurul'a ve ilgili veri sahibine bilgi vermesini gerekli kılmaktadır. Kurul, 24 Ocak 2019 tarihli ve 2019/19 sayılı kararında ("Karar"), veri ihlali durumlarında uygulanacak kurallar ve izlenecek prosedürleri açıklığa kavuşturmuştur.

Kurul, ihlal bildirimlerinin zamanlaması bakımından GDPR yaklaşımını benimsemektedir ve Kanun'da yer alan "en kısa süre" ibaresinin veri ihlalinin tespit edilmesinin ardından 72 saat içerisinde olarak yorumlanması gerektiğini açıklamıştır.

Kanun ayrıca veri sorumlularının, maruz kalınan risk düşük olsun veya olmasın veri ihlalinden etkilenen veri sahiplerini tespit eder etmez en kısa sürede veri sahiplerine bildirimde bulunmalarını gerekli kılmaktadır. Kurul, anılan Karar'ında veri ihlalinden etkilenen veri sahiplerinin belirlenmesinden sonra yapılacak bildirimin süresi ile ilgili olarak belli bir süre öngörmemiş, makul olan en kısa süre içerisinde bildirim yapılması gerektiğini belirtmiştir. Makul süre her somut olay özelinde değerlendirilmesi gereken bir husus olmakla birlikte, veri ihlalinin Kurul'a bildiriminden sonra ivedilikle ilgili kişilere bildirim yapılması uygun olacaktır.

Kurul'un kararı, veri ihlallerine hazırlıklı olmaları için veri sorumlularının önceden bir yol haritası çizmelerini, kurum içi raporlama mekanizmaları ile izlenecek prosedürleri önceden netleştirmelerini gerekli kılmaktadır. Veri sorumluları, veri ihlalleri ile alınan tedbirlerin kayıtlarını tutmakla yükümlüdürler.

Veri ihlalinin bildirilmesi yükümlülüğü, yurt dışında ikamet eden veri sorumluları için de geçerlidir. Yurt dışındaki veri sorumlularının bir veri ihlali olayı yaşamaları ve söz konusu veri ihlalinin Türkiye'de ikamet eden veri sahiplerini ve Türkiye'deki veri sahipleri tarafından kullanılan malları/hizmetleri etkilemesi durumunda, yurt dışındaki veri sorumluları aynı şekilde Kurul tarafından duyurulan veri ihlali bildirimi prosedürlerini izlemek zorundadırlar.

Yurt dışındaki veri sorumluları bakımından kritik

olan husus, veri ihlali yurt dışında gerçekleşse bile, veri ihlalinden etkilenen veri sahiplerinin Türkiye'de bulunması halinde, Kurul'a bildirim yapılması gerektiğidir. Veri ihlal bildirimleri bakımından Kanun'un uygulama alanının bu anlamda genişletildiği görülmektedir.

Kurul'un, bildirimde bulunurken veri sorumlularının doldurmaları gereken "Kişisel Veri İhlali Bildirim Formu" mevcuttur.

2025 yılı sonunda veri ihlali bildirimlerinin Kurum internet sitesinde ilan edilmesine ilişkin uygulamada önemli bir değişikliğe gidilmiştir. Değişiklik öncesi veri ihlal bildirimleri herhangi bir süre kısıtlaması olmaksızın ilan edilmekte iken Kurul'un 25/12/2025 tarihli ve 2025/2451 sayılı Kararı ile veri ihlali bildirimlerinin belirli bir süre ile ilan edilmesine, bu sürenin 60 gün ile sınırlı olmasına ve bu süreden daha kısa süre içinde ilgili kişilere bildirim yapıldığının veri sorumlusu tarafından tevsik edilmesi halinde ilanın Kurum'un internet sitesinden kaldırılmasına karar verilmiştir.

Süresiz ilan uygulamasının sona erdirilmesi, veri sorumluları üzerindeki orantısız itibar etkilerini azaltarak Kanun'un temel ilkeleriyle daha uyumlu bir yaklaşım sunmaktadır. Veri sorumlularının, ihlal sonrası süreçlerini hızlı ve etkin şekilde yönetmeleri, hem ilgili kişilerin korunması hem de kamuya açık ilan süresinin kısaltılması açısından büyük önem taşımaktadır. Geçmişte Kurum'un internet sitesinde yayınlanan veri ihlal bildirimlerinin çoğunlukla özel şirketler tarafından yapılmış olmasına karşın hastane ve üniversite gibi kuruluşlarca da ihlal bildirimleri yapılmıştır. Diğer taraftan ihlallerden etkilenen kişi kategorileri ağırlıklı olarak ilgili veri sorumlularının çalışanları, hastaları, aboneleri, müşterileri, öğrencileri, klinik araştırma katılımcıları ve iş ortaklarından oluşmaktadır. Etkilenen veri kategorileri bakımından ise, ağırlıklı olarak kimlik, eğitim, sağlık, dernek üyelik, işlem ve fiziksel mekân güvenliği, ceza mahkûmiyeti ve güvenlik tedbiri, ırk ve etnik köken, muhasebe ve finans bilgileri ile genetik, biyometrik veriler veri ihlal bildirimlerinin konusunu oluşturmaktadır. Söz konusu veri ihlali bildirimleri hem yurtiçinden hem de yurtdışından yapılmıştır.

Bugüne kadar Kurum internet sitesinde yayınlanmış veri ihlali bildirimleri çok çeşitli tür ve sektördeki veri sorumluları tarafından yapılmıştır.

Veri ihlalleri bakımından 2025 yılında Kurum'a 328 veri ihlali bildirimi yapılmış; bunların 105'i sonuçlandırılmış, 51'i Kurum tarafından ilan edilmiş ve 223'ünün incelemesi yıl sonu itibarıyla devam etmiştir. Bu veriler, veri sorumluları açısından veri ihlali müdahale planlarının, iç bildirim mekanizmalarının ve Kurum'a bildirim süreçlerinin önemini koruduğunu ortaya koymaktadır.

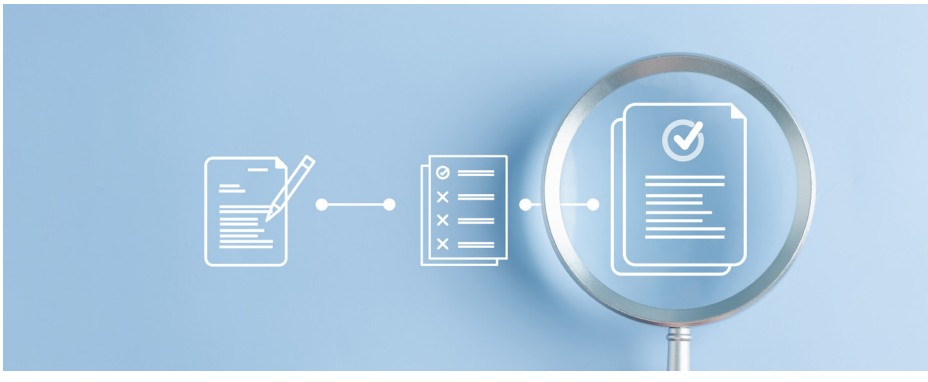
Veri ihlali doğuracağı sonuçlar yönünden de veri sorumlusu hakkında idari para cezası uygulanma riski ve de Türk Ceza Kanunu kapsamında cezai sorumluluk bakımından hassasiyetle ele alınması gereken süreçlerdir. Bilindiği üzere Kanun, hem idari para cezaları verilmesine hem de cezai sorumluluğa

ilişkin hükümler içermektedir. Kanun, cezai sorumluluğa ilişkin olarak, Türk Ceza Kanunu'nun kişisel verilerin hukuka aykırı olarak kaydedilmesi, hukuka aykırı olarak verilmesi veya ele geçirilmesine ilişkin yaptırımların yer aldığı ilgili hükümlerine atıfta bulunmaktadır.

Cezai yaptırımlara ek olarak, Kanun'da ayrıca ihlal durumunda uygulanacak idari para cezalarına ilişkin ayrıntıların yer aldığı hükümler bulunmaktadır. Kanun kapsamında veri güvenliğine ilişkin yükümlülüklerini yerine getirilmemesi, veri ihlalleri ve ihlalin zamanında Kurum'a bildirilmemesi bakımından 85.437 – 17.092.242 TL'ye kadar (2026 yılı için güncellenmiş) idari para cezası ile veri sorumlularını karşı karşıya bırakır.

Kurul'un veri ihlal bildirimleri üzerine ele aldığı ve ilan ettiği dosyalarda genel eğiliminin, ihlal bildirimlerine ilişkin daha yapıcı bir yaklaşım benimseyen Avrupa'daki veri koruma otoritelerine kıyasla, ağırlıklı olarak ceza verme yönünde olduğu görülmektedir. Bununla birlikte Kurul'un veri ihlalinden etkilenen kişi sayısı, ihlalin veri ilgilisi üzerinde olumsuz bir etki yaratıp yaratmadığı, veri sorumlusunun müdahalesinin mümkün olup olmadığı, ihlale konu verinin silinip silinmediği, veri sorumlusunun süresi içinde bildirimde bulunup bulunmadığı, makul idari ve teknik tedbirlerin alınıp alınmadığına ilişkin hususları dikkate alarak idari para cezası uygulamadığı kararları bulunduğunu da not etmek gerekir.
Veri ihlali süreçlerinin doğru ve zamanında ele alınması, veri sorumluları bakımından kritik düzeyde önemli olup, kişisel verilerin işlenmesi, silinmesi, yok edilmesi ve imhasına ilişkin veri sorumluları tarafından belirlenen ve uygulamaya alınan ilke ve prosedürlere ek olarak, veri ihlali durumunda izlenecek prosedürlerin de net bir şekilde belirlenmesi gerekmektedir. Veri sorumlularının uyum süreçlerinde olası bir veri ihlali durumunda hızlı ve etkin bir müdahale için bir veri ihlali müdahale planı oluşturmaları veri ihlalinin doğuracağı risklerin azaltılması açısından olumlu bir katkı sağlayacaktır.

Kurul Kararlarının Yargısal Denetimi ve Hukuk Yolları



Kanun uyarınca Kurul'un idari yaptırımlara karar verme yetkisi bulunmaktadır. Kurul'un, aydınlatma yükümlülüğünün, veri güvenliğine ilişkin yükümlülüklerin, Kurul tarafından verilen kararların yerine getirilmemesi, Veri Sorumluları Siciline kayıt ve bildirim yükümlülüklerine aykırılık ya da standart sözleşmelere ilişkin bildirim yükümlülüğüne aykırılıktan dolayı idari para cezası verebileceği düzenlenmiştir. Kurul, idari para cezası yaptırımı haricinde ise idari eylem niteliğinde olarak veri sorumlusunun ihlali ortadan kaldırmasına karar verme, veri işlemenin ve aktarımının durdurulmasına karar verme şeklinde de kararlar tesis edebilmektedir.

Kanun sistematiği içerisinde, Kurul tarafından verilecek idari para cezaları "Kabahatler" başlığı altında düzenlenmektedir. Buna göre, 213 sayılı Vergi Usul Kanunu'nun mükerrer 298. Maddesi ile düzenlenen yeniden değerleme oranı çerçevesinde Kanun'un ilgili maddelerinde yer alan idari para cezaları 2026 yılında aşağıdaki şekilde uygulanacaktır:

6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamındaki İdari Para Cezaları- 2026 Yılı Ceza Tutarları

Yasal Dayanak	İhlal	Güncel İdari Para Cezası
KVKK Madde 18/1/a	Aydınlatma yükümlülüğünü yerine getirmemek	85.437TL – 1.709.200TL
KVKK Madde 18/1/b	Veri güvenliğine ilişkin yükümlülükleri yerine getirmemek	256.357 TL – 17.092.242TL
KVKK Madde 18/1/c	Kurul tarafından verilen kararları yerine getirmemek	427.263TL – 17.092.242TL
KVKK Madde 18/1/ç	Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket etmek	341.809TL – 17.092.242TL
KVKK Madde 18/1/d	Standart Sözleşmeleri 5 iş günü içerisinde Kurum'a bildirmemek	90.308TL – 1.806.177TL

Diğer yandan, Değişiklik öncesi dönemde Kanun'da, Kurul tarafından uygulanacak idari para cezalarına ve idari yaptırımlara karşı başvuru yolları gösterilmemiş ve Kanun kapsamında bu konu düzenlenmemiş idi. Uygulamada ise idari para cezasını gerektiren ihlaller "kabahat" niteliğinde düzenlendiğinden, bu ihlaller için öngörülen yaptırımlara karşı 5326 sayılı Kabahatler

Kanunu kapsamında düzenlenen yargı yollarına gidilmekte idi ve bu idari para cezalarına karşı açılacak davalarda sulh ceza mahkemelerinin görevli olduğu kabul edilmekteydi. Bu duruma karşı uygulamacıların kişisel verilerin

korunması alanının teknik ve uzmanlık gerektiren bir konu olması karşısında, kuruluş amacı itibariyle ceza hukuku alanında faaliyet gösteren Sulh Ceza Hakimliklerinin Kurul tarafından verilen kararların yargısal denetimi açısından doğru mercii olmadığı konusunda uzun süredir haklı eleştirileri bulunmaktaydı.

İlk derece mahkemesi statüsünde olan Sulh Ceza Mahkemelerinin basit yargılama usulü ile gerçekleştirdikleri yargısal denetim süreci kararın kesinleşmesiyle sonlandığında, üst mahkeme denetimi anlamında başvurulabilecek tek yol doğrudan Anayasa Mahkemesi idi. Nitekim Anayasa Mahkemesi yakın tarihli bir kararında, Kurul'un veri güvenliğini sağlama yükümlülüklerini ihlal ettiğini tespit ettiği bir veri sorumlusu hakkında uygulamış olduğu idari para cezasına karşı yürütülen yargılama sürecinin mülkiyet hakkının ihlaline sebebiyet verdiğini tespit etmiştir. Anayasa Mahkemesi kararında, idari para cezalarının mülkiyet hakkına müdahale teşkil ettiğini, dolayısıyla mülkiyet haklarına yapılan müdahalelerde Anayasa'nın 13. maddesinde düzenlenen temel hak ve özgürlüklerin sınırlandırılmasına ilişkin genel ilkelerin göz önünde bulundurulması gerektiği, ilgili müdahalenin ölçülülük ilkesine uygun olması gerektiği değerlendirmiştir.

Ölçülülük ilkesi kapsamında ise, müdahalelerin orantılı olması gerektiğini ve hukuka aykırılık iddialarının bir mahkeme tarafından etkili biçimde incelenmesinin müdahalenin orantılılığı bakımından büyük bir önem arz ettiği ifade edilmiştir. Anayasa Mahkemesi sonuç itibariyle, Sulh Ceza Hakimliklerince yapılan yargısal denetimin itiraz eden tarafın iddiaları çerçevesinde hiçbir değerlendirme içermemesi sebebiyle adil yargılanma kapsamında mülkiyet hakkının korunmasına yönelik güvencelerin yerine getirilmediğine ve mülkiyet hakkının ihlal edildiğine karar vermiştir

Anayasa Mahkemesi'nin ilgili kararı ile ortaya konulduğu üzere, hukuka aykırılık iddialarının bir mahkeme tarafından etkili biçimde incelenmesi temel hak ve özgürlüklere yapılan müdahalelerin orantılılığının sağlanması bakımından büyük bir önem arz etmektedir.

Uygulamadaki Kurul'un idari para cezalarına karşı yargı yolundaki söz konusu aksaklıklara yönelik yapılan tespitler, dile getirilen eleştiriler ve Sulh Ceza Hakimliklerinin kişisel verilerin korunması alanında yargı denetimi için doğru mercii olmadığı, Anayasa Mahkemesi'nin söz konusu kararı ile de ortaya konmuştur.

Değişiklik ile birlikte bu sorunlara bir çözüm olarak Kurul'un idari para cezalarına karşı idare mahkemelerinde dava açılabileceğine ilişkin açık bir düzenleme eklenmiştir.

Böylelikle, Kurul tarafından verilen idari para cezalarının bir idari işlem mahiyetinde olması ışığında bu idari işlemin de idari yargı denetimine tabi olacağı açıkça düzenlenerek uygulamadaki tereddütler giderilmiştir ve Kurul kararlarının daha etkin bir şekilde denetlenmesini sağlayacak bir usul ortaya

konmuştur. İlgili değişiklik ile birlikte değişiklik öncesi dönemde yaşanan hukuki belirlilik temelindeki sorunların azalması ve uygulamaya ışık tutacak içtihatların artması beklenmektedir.
Değişiklik Kanunu'nun 1 Haziran 2024 tarihinde yürürlüğe girmesi itibariyle, yürürlük tarihinden önce hali hazırda sulh ceza hakimlikleri nezdinde görülmekte olan başvuruların bu hakimliklerce görülmeye devam edileceğine yönelik bir geçişi hükmü ile öngörülmüştür.

Geçiş hükmü gereğince, 1 Haziran 2024 itibarıyla sulh ceza hakimlikleri nezdinde derdest bulunan davalar, sulh ceza hakimliklerince nihai hükme bağlanacaktır ancak 1 Haziran 2024 sonrası açılacak davalar ise idare mahkemeleri nezdinde görülecektir.

Kanun'un zaman bakımından uygulaması yapılan değişiklikler ve eklenen geçiş hükmü ile belirlenmiş olsa da, özellikle kişisel verilerin yurtdışına aktarım süreçleri için de getirilen ve 01.09.2024 tarihine kadar eski uygulamanın devam etmesini öngören diğer geçiş hükümleri sebebiyle Kanun'un zaman bakımdan uygulanması hususunda uygulamada soru işareti yaratmıştır.

Söz konusu tereddütlerin giderilmesi adına Kurum tarafından 19.12.2024 tarihinde uygulamaya rehber olması amacıyla bir bilgi notu yayımlanmıştır. 5237 sayılı Türk Ceza Kanunu'nda zaman bakımından uygulamaya ilişkin bulunan düzenlemelerin dikkate alınacağının altı çizilmiştir.

Bu çerçevede, uygulanması gerekecek idari yaptırım kararı Türk Ceza Kanunu ilkeleri temelinde, fiilin işlenme zamanı ve şikayet zamanına bağlı olarak belirlenecektir. Buna göre;

i. Fiilin Kanun değişikliğinden önce gerçekleşmiş ve bitmiş olduğu hallerde;
ii. Kanun değişikliğinden önce gerçekleşen ve biten fiillerde, şikayetin ne zaman yapıldığına bakılmaksızın, yargılama neticesinde verilecek kararın Değişiklik Kanunu'nun yürürlüğe girdiği tarihten sonra veriliyor olması halinde lehe olan Kanun uygulanacaktır.
iii. Fiilin Kanun değişikliğinden önce başlamış ve devam ediyor olduğu hallerde (mütemadi hareketli – devam eden fiil hallerinde);
iv. Fiilin Kanun değişikliğinden önce kesilmesi halinde lehe olan Kanun uygulanacaktır, ve
v. Fiil Kanun değişikliği sonrasında kesiliyor ise değişiklik sonrası yeni Kanun uygulanacaktır.
vi. Fiilin Kanun değişikliğinden sonra gerçekleşmiş olması halinde;
vii. Bu hallerde zaman bakımından uygulama sorunu ortaya çıkmayacak ve yeni Kanun uygulanacaktır.

2025 yılı, Kurul kararlarının yargısal denetimi bakımından geçiş döneminin etkilerinin daha somut şekilde görüldüğü bir yıl olmuştur. Kurum'un 2025 Yılı Faaliyet Raporu'na göre, Kurum tarafından takip edilen toplam dava sayısı 1.678'dir. Bu davaların önemli bir kısmı

idare mahkemeleri ve sulh ceza hâkimlikleri nezdinde görülmektedir. Raporda, idare mahkemeleri nezdinde 797 dosya, sulh ceza hâkimlikleri nezdinde 804 dosya ve Danıştay nezdinde 29 dosya takip edildiği belirtilmiştir.

Buna karşılık yeni dönemde idare mahkemelerinin KVKK idari para cezalarının yargısal denetiminde merkezi rol üstlenmeye başladığı görülmektedir.

Sonuç olarak, 2025 yılı Kurul kararlarının yargısal denetimi bakımından geçiş döneminin uygulamaya yansıdığı bir yıl olmuştur. İdare mahkemeleri KVKK idari para cezalarının denetiminde yeni ve asli yargı mercii haline gelmiştir.

Anayasa Mahkemesi ise gördüğü bireysel başvuru davaları ile, Kurul kararlarına karşı ileri sürülen esaslı iddiaların yargı mercileri tarafından somut ve yeterli gerekçeyle karşılanması gerektiğini ve cezaların kanuniliği ilkelerini bir kez daha ortaya koymuştur. Önümüzdeki dönemde idare mahkemeleri, bölge idare mahkemeleri ve Danıştay kararlarının artmasıyla birlikte, Kurul'un idari para cezası uygulamalarında gerekçelendirme, ölçülülük, usuli güvenceler ve lehe kanun ilkesi bakımından daha belirgin içtihat oluşması beklenmektedir.

EKİBİMİZ

BEGÜM YAVUZDOĞAN OKUMUŞ
ORTAK AVUKAT

begum.yavuzdogan@gun.av.tr

DİRENÇ BADA
ORTAK AVUKAT

direnc.bada@gun.av.tr

YALÇIN UMUT TALAY
ORTAK AVUKAT

umut.talay@gun.av.tr

UĞUR ERKIRLI
KIDEMLİ AVUKAT

ugur.erkirli@gun.av.tr

Hakkımızda

Türkiye'nin en eski ve en büyüklerinden biri olan büromuz, uluslararası alanda, önde gelen avukatlık bürolarından birisi olarak tanınmaktadır.

Kurumlara ticaret, şirketler, fikri mülkiyet, düzenlenmiş piyasalar hukuku alanlarında uyuşmazlık yönetimi, danışmanlık, sözleşmeler, tescil ve araştırma hizmetleri vermekteyiz.

Merkezimiz İstanbul'da olup Ankara, İzmir ve Türkiye'nin diğer önemli ticari merkezlerindeki bürolarla işbirliği yapmaktayız.

Büromuz, temelde Türkçe ve İngilizce olarak hizmet vermekte olup, Almanca ve Fransızca dillerinde de hukuki hizmet sağlamaktadır.

Müvekkillerimize, ilaç, tıbbi cihaz ve sağlık, sigorta ve reasürans, enerji, inşaat ve gayrimenkul, lojistik, teknoloji, medya ve telekomünikasyon, otomotiv, hızlı tüketim ürünleri, kimyasal ve savunma sektörleri başta gelmek üzere değişik iş ve ticaret sektörlerinde hizmet vermekteyiz.

Vizyonumuz, hizmetlerinde lider, topluma, çevreye ve çalışanlarına duyarlı, yenilikçi ve sürdürülebilir bir kurum olmaktır.

Müvekkillerimizin başarısını, kendi başarımızdan önde görürüz. Müvekkillerimizin değişen ihtiyaçlarına daha doğru ve etkin bir şekilde cevap verebilmek için onların faaliyet gösterdiği sektörlerdeki gelişmeleri yakından takip eder, bu sektörlerde sadece hukuki değil ticari bilgileri de edinerek bilgilerimizi derinleştiririz. Bu amaçlarla ulusal ve uluslararası mesleki ve ticari dernek ve kuruluşların çalışmalarına etkin olarak katılır, bilgi ve tecrübelerimizi paylaşarak katkıda bulunuruz.

Büromuz, hizmetlerini müvekkillerimizin değişen ihtiyaçlarına uygun olarak geliştirmeye ve yenilikçi, kaliteli hizmetler sunmaya kararlıdır.

GÜN + PARTNERS

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Türkiye

T: + 90 (212) 354 00 00
F: + 90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr