GÜN + PARTNERS
AVUKATLIK BÜROSU

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

2025

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

Bu yılın raporunda, kişisel verilerin korunması alanındaki son gelişmeler, alınan son kararlar ve yayınlanan kılavuzlar yanında kişisel verilerin korunması hukukunun temel düzenlemeleri ve prensipleri, Türkiye'deki gelişmeler ile bu alandaki güncel önemli hususlara ve geleceğe yönelik beklentiler, değerlendirmeler ve trendlere odaklanmaktayız.

2024 yılı kişisel verilerin korunması alanında yine önemli gelişmelerin yaşandığı bir yıl oldu. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("Kanun") beklenen değişikliklerin yürürlüğe girdiği, ikincil mevzuata yönelik çalışmalar, Kişisel Verileri Koruma Kurumu'nun ("Kurum") veri sorumlularına yönelik yol gösterici mahiyetteki rehber ve yayınları, kişisel verilerin korunması alanındaki farkındalığın ve etkinliğin artırılmasına yönelik çalışmalar ile Kanun'un etkin bir şekilde uygulanması ve başta rekabet hukuku olmak üzere temas ettiği diğer hukuk alanları ile ilişkisinin doğru şekilde kurulması yönünde çalışmaların gerçekleştiği bir yılı ardımızda bıraktık.

AB'deki düzenlemelerin yankılarının ülkemizde de ses bulmasıyla, yapay zeka temelli tartışmalar henüz istenen seviye ve olgunlukta olmasa da, 2024 yılında biraz daha ön plana çıkmıştır. Tüm dünyayı etkisi altına alan yeni sanal düzen içerisinde kişisel verilerin korunması konusunda nasıl adımlar atılması gerektiği, teknoloji ve mahremiyet arasında nasıl bir denge kurulacağı önümüzdeki yıllarda da sıcak bir gündem maddesi olmaya devam edecektir.

Kanun'a uyum noktasında her geçen yıl veri sorumluları bakımından olumlu gelişmelere tanık olmakla birlikte, Kanun'da yapılan değişiklikler ile yılın ikinci yarısı veri sorumluları için özellikle yurt dışına veri aktarımı konusunda yoğun uyum çalışmalarının yürütüldüğü bir dönem olmuştur.

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 tüm dünyada olduğu gibi Kişisel Verileri Koruma Kurulu'nun ("Kurul") da dikkatini çekmeye devam etmektedir. Dijital ekonominin büyümesiyle birlikte dijital platformların veri toplama ve işleme süreçleri veri koruma hukuku ile rekabet hukuku arasında önemli bir etkileşim yaratmıştır. Özellikle sosyal ağ sağlayıcısı META hakkında Rekabet Kurumu tarafından yürütülen soruşturmanın kişisel verilerin korunması alanında da etkilerinin doğacağı şüphesizdir.

Kurum'un 2024 yılındaki faaliyetlerine ilişkin yayınladığı bilgi notundaki istatistikler ise, ihbar, şikayet ve başvuru sayısında bir önceki yıla kıyasla artış olduğunu göstermektedir. 2024 yılında Kurul incelemelerine yoğun bir şekilde devam etmekle birlikte, kararlardan sadece 2'si kamuoyuna ilan edilmiştir.

Uygulamada ortaya çıkan ihtiyaçlar ve Kanun'un Avrupa Birliği Genel Veri Koruma Tüzüğü ("GDPR") ile uyumunun sağlanması hedefi neticesinde Kişisel verilerin korunması alanında 2024 yılında önemli mevzuat değişiklikleri gerçekleşmiştir. 1 Haziran 2024 tarihinde yürürlüğe giren yasa değişiklikleri, kişisel verilerin korunması alanında yeni bir dönemi başlatmış ve 1 Eylül 2024 tarihine kadar uyumun

gerçekleştirilmesi düzenlenmiştir. Bu çerçevede 10 Temmuz 2024 tarihinde, "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" yayımlanmıştır. Değişikliklere uyum için sağlanan kısıtlı uyum süreci hem veri sorumlularını hem de uygulamacıları zor durumda bırakmıştır. Kaldı ki uyum süreci pek çok veri sorumlusu bakımından halen devam etmektedir.

Kurum 2024 yılında da veri koruma alanındaki farkındalığın gelişmesi ve uygulayıcılara yol gösterici olması amacıyla çeşitli rehberler, dokümanlar ve bilgi notları yayımlamıştır. Türkiye Cumhuriyeti Kimlik Numaralarının İşlenmesi Hakkında Rehber, elde edilmesi halinde önemi gereği veri sahibinin diğer kişisel verilerine de erişim imkânı sağlayabilmesi nedeniyle mağduriyete yol açabilecek olan T.C. kimlik numaralarının işlenmesi faaliyetinde dikkat edilmesi gereken hususları açıklarken, Seçim Faaliyetlerinde Kişisel Verilerin Korunması Rehberi, seçim faaliyetlerinde yer alan kamu idarelerine, siyasi partilere, adaylara ve seçmenlere Kanun kapsamında yerine getirmeleri gereken yükümlülükleri veya sahip oldukları hakları hatırlatmıştır. Kurum, ayrıca Deepfake Bilgi Notu, Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu, 6698 Sayılı Kanun Kapsamında Kabahatlerin Zaman Bakımından Uygulanması Bilgi Notu, Sohbet Robotları (ChatGPT Örneği) Hakkında Bilgi Notu ve Kurula İletilen Şikayet ve İhbarlarda Sık Yapılan Hatalar başlıklı yayınları ile uygulayıcılara pratik bilgiler sunan içerikler yayımlamıştır.

Yurt dışına veri aktarımı kapsamında, Kanun'da düzenlenen uygun güvencelerden biri olan standart sözleşmelerin Kurum'a elektronik ortamda bildirilmesine olanak sağlayan "Standart Sözleşme Bildirim Modülü" sistemi oluşturulmuştur.

Kurul tarafından 2024 yılında 552.668.000 Türk lirası idari para cezası uygulanmış olup, söz konusu ceza tutarları ağırlıklı olarak sicile kayıt ve bildirim yükümlülüğü olduğu halde bu yükümlülüğünü yerine getirmeyen veri sorumluları hakkında uygulanan cezalardan oluşmaktadır.

Kurum, Ağustos 2024'te yayınladığı Veri Sorumluları Sicili Hakkında Kamuoyu Duyurusu'nda, sicile kayıt ve bildirim yükümlülüğünü yerine getirmeyen veri sorumluları hakkında Kurul tarafından re'sen inceleme yapıldığını, sicile kayıt ve bildirim yükümlülüğü olduğu halde bu yükümlülüğünü yerine getirmeyen yurt içinde ve yurt dışında yerleşik gerçek ve tüzel kişi veri sorumlularına Kurul tarafından, 01.08.2024 tarihi itibariyle 503.935.000 TL idari para cezası uygulandığını duyurmuştur. 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. Yurt dışında yerleşik veri sorumlularının da, Türkiye'de kişisel verileri işledikleri sürece VERBİS'e kayıt yaptırmaları gerekmektedir.

Yurt dışı veri aktarımlarında yaşanan gelişmeler neticesinde 2024 yılında (fiilen Haziran – Aralık dönemi içinde Kurum kayıtları uyarınca) Kurum'a 1345 adet standart sözleşme bildirilmiştir. Veriler uyum çalışmalarının veri sorumluları nezdinde halen devam ettiğine işaret etmektedir.

İçindekiler

Türkiye'de Kişisel Verilerin Korunması – Genel Yaklaşım

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 trendleri Kişisel Verileri Koruma Kurumu ("Kurum") tarafından takip edilmektedir. Ayrıca, Kişisel Verileri Koruma Kurulu'nun ("Kurul") ilke kararları ile Avrupa ve Dünya genelindeki veri koruma trendleri takip edilirken, diğer bir yandan da Adalet Bakanlığı tarafından yayımlanan İnsan Hakları Eylem Planı ve Uygulama Takvimi ile Kanun'un Avrupa standartları ile uyumlu hale getirileceği ve GDPR'a paralel düzenlemeler yapılacağı resmi olarak da ilan edilmiş durumdadır.

Kanun'un GDPR standartlarına yakınlaştırılması yolunda en büyük adım ise 12.03.2024 tarihli Resmi Gazete'de yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ("Değişiklik Kanunu") ile atılmıştır. 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 Kanunu 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. Kişisel verilerin işlenmesi hukuku alanında Kanun'un

yayımından itibaren süregelen ve uygulamada dar boğaz etkisi yaratan özel nitelikli kişisel verilerin işlenmesi ile kişisel verilerin yurtdışına aktarımı konuları getirilen değişikliklerle birlikte bir nebze çözüme ulaştırılmış ve Türkiye'nin veri koruma hukukunda Avrupa standartlarına yaklaşma hedefleri kapsamında adımlar atılmıştır. Aşağıda Değişiklik Kanunu ile yürürlüğe giren yenilikler daha detaylı bir şekilde ele alınmaktadır.

Bununla birlikte yapay zeka düzenlemeleri bakımından henüz somut bir gelişme ya da çalışma olduğunu henüz söylemek mümkün olmayıp, yapay zeka halihazırda, Kanun kapsamında yalnızca bir madde (madde 11) dahilinde uygulama alanı bulan bir konu olmaya devam etmektedir.

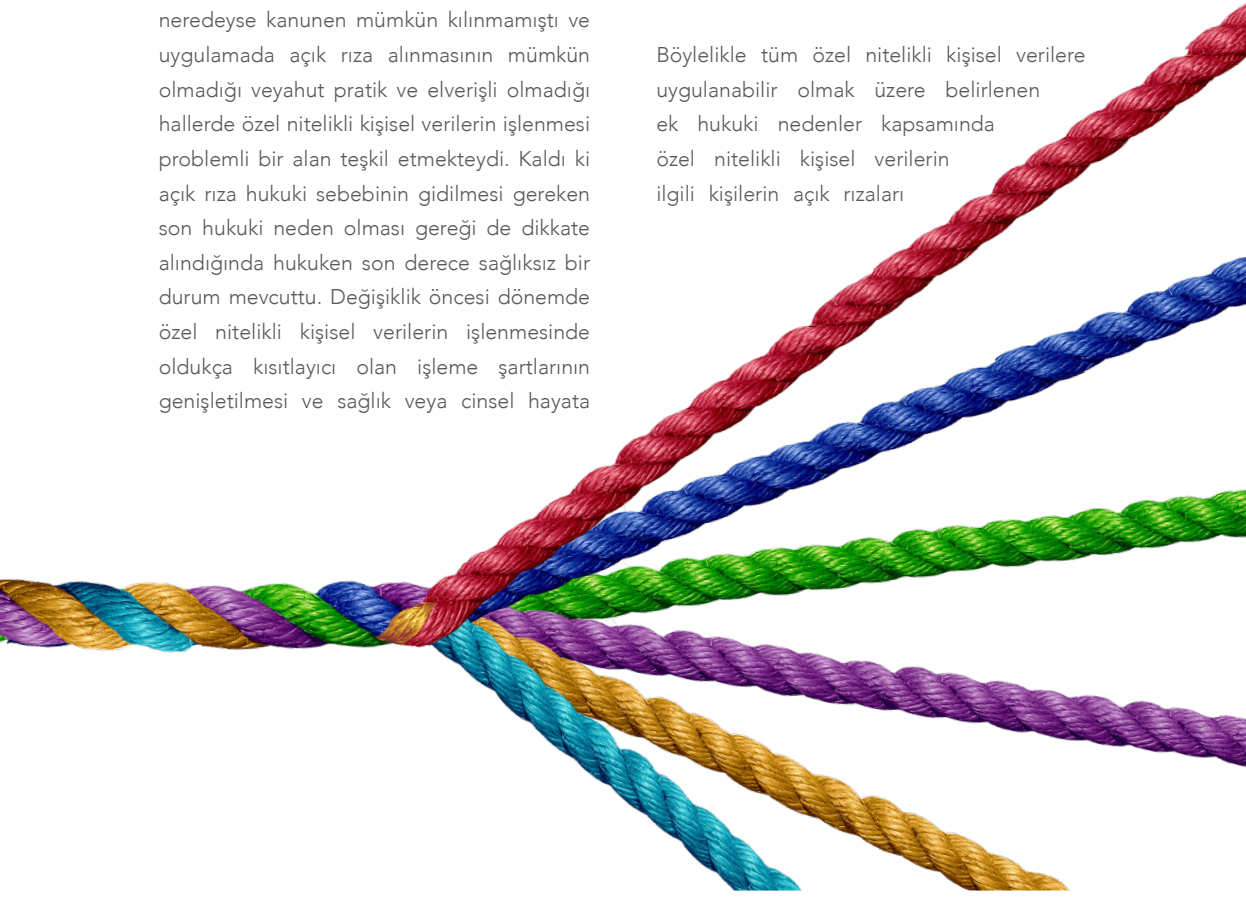
Özel Nitelikli Kişisel Verilerin İşlenmesi

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 tanımlanmıştır.

Değişiklik Kanunu'nun yürürlüğe girmesinden önceki dönemde Kanun kapsamında özel nitelikli kişisel verilerin işlenmesi temel olarak veri sahibinin açık rızasının alınmasına şart koşulmuş ve açık rıza dışında işlenmesi neredeyse kanunen mümkün kılınmamıştı ve uygulamada açık rıza alınmasının mümkün olmadığı veyahut pratik ve elverişli olmadığı hallerde özel nitelikli kişisel verilerin işlenmesi problemli bir alan teşkil etmekteydi. Kaldı ki açık rıza hukuki sebebinin gidilmesi gereken son hukuki neden olması gereği de dikkate alındığında hukuken son derece sağlıksız bir durum mevcuttu. Değişiklik öncesi dönemde özel nitelikli kişisel verilerin işlenmesinde oldukça kısıtlayıcı olan işleme şartlarının genişletilmesi ve sağlık veya cinsel hayata ilişkin kişisel veriler ile diğer özel nitelikli kişisel veriler arasında bulunan ayrımın kaldırılması ihtiyacı uygulamada gündem konusuydu.

Hem uygulamada yaşanmakta olan dar boğazın giderilmesi hem de Avrupa standartlarına ve GDPR standartlarına yakınlaşma amacıyla yürürlüğe giren Değişiklik Kanunu ile birlikte özel nitelikli kişisel verilere ilişkin olarak özel nitelikli kişisel verilerin işleme şartları genişletilmiş ve sağlık veya cinsel hayata ilişkin kişisel veriler ile diğer özel nitelikli kişisel veriler arasında bulunan ayrım kaldırılmıştır.

Böylelikle tüm özel nitelikli kişisel verilere uygulanabilir olmak üzere belirlenen ek hukuki nedenler kapsamında özel nitelikli kişisel verilerin ilgili kişilerin açık rızaları



aranmaksızın işlenmesi mümkün hale 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.

Değişiklik öncesi dönemde özel nitelikli kişisel verilerin işlendiği çoğu durumda açık rıza hukuki sebebine dayanmak durumunda kalmış olan veri sorumlularının değişiklik ile birlikte çoğu işleme faaliyeti kapsamında farklı hukuki nedenlere dayanmaları mümkün hale gelmiştir. Özellikle kanunlarda açıkça öngörülmüş olma, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, istihdam iş ve sosyal güvenlik veya sosyal hizmetler alanındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması gibi hukuki sebepler veri sorumlularının uygulamada yaşadığı zorlukları aşmalarını sağlayabilecek yenilikler olarak ortaya çıkmaktadır.

İşçi-işveren ilişkileri çerçevesinde çoğu zaman bir gereklilik nedeniyle işçilerin özel nitelikli kişisel verilerinin işlenmesinin, yasa değişikliği öncesi ancak açık rıza ile mümkün olabilmesi, bunun yarattığı operasyonel güçlükler ve işçinin işverene bağlı olduğu bir ilişkide rızanın özgür iradeyle verilmesi yönünden geçerliliğine ilişkin tartışmalar değişiklik ile birlikte çözüme kavuşturulmuştur. Böylece, iş sağlığı ve yükümlülükleri kapsamında işçilerinin sağlık verilerini elde eden ve işleyen işverenler, artık "istihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım

alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olduğu" hukuki sebebine dayanabilecek ve açık rızaya ihtiyaç duymayacaktır.

Dolayısıyla veri sorumlularının özel nitelikli kişisel verilerin işlenmesinde güncel düzene uyum sağlamak adına mevcut uyum pratiklerinde ve özellikle kişisel verilerin işlenmesine ilişkin politikalarında, aydınlatma metinlerinde ve açık rıza uygulamalarında güncellemeler yapması ve ayrıca yeni tanımlanan hukuki sebepleri her bir işleme süreci özelinde değerlendirmesi önem taşımaktadır.

Kişisel Verilerin Yurt Dışına Aktarımı

Değişiklik Kanunu 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 Kanunu ile birlikte 1 Haziran 2024 tarihinde yürürlüğe girmiştir. Bu kapsamda Değişiklik Kanunu 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 ve yeterlilik kararının bulunmadığı durumlarlarda ise, Kanun'da sayılan uygun güvencelerden birinin ilgili taraflarca sağlanması halinde yurt dışına aktarılabileceği düzenlenmiştir.

Değişiklik ile birlikte yürürlükteki yeni yurtdışına aktarım şartları sistematiği kapsamında;

i. Yeterlilik Kararının bulunması halinde kişisel verilerin yurtdışına aktarılması

Kanun'un 5'inci ve 6'ıncı maddelerinde belirtilen hukuki sebeplerden birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektör veya uluslararası kuruluş hakkında yeterlilik kararı bulunması halinde kişisel veriler, sonraki aktarımlar da dâhil olmak üzere yurt dışına aktarılabilecektir. Kurul, diğer bazı kriterler ile birlikte esas olarak karşılıklılık prensibi çerçevesinde yeterlilik kararı verme hususunda karara varacaktır. Söz konusu yeterlilik kararının periyodik olarak gözden geçirilmesi de düzenlemeler arasında yer almaktadır.

Kurul tarafından verilecek yeterlilik kararlarının ülkelere ek olarak uluslararası kuruluş veya ülke içerisindeki sektörler hakkında da verilebileceği, verilen bu kararlara uygun olarak yurt dışına veri aktarımı yapılabileceği öngörülmüştür.

ii. Yeterlilik Kararının bulunmaması halinde Uygun Güvencelerden birinin sağlanması ile kişisel verilerin yurtdışına aktarılması

Kurul tarafından bir yeterlilik kararı bulunmadığı hallerde, kişisel veriler aşağıda sıralanan uygun güvencelerden birinin sağlanması ve Kanun'daki hukuki sebeplerden birinin de bulunması koşuluyla yurt dışına aktarılabilecektir:

a. Yurt dışındaki kamu kurum ve kuruluşları

veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi.

b. Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü oldukları, kişisel verilerin korunmasına ilişkin hükümler ihtiva eden ve Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı.

i. Şirketler topluluğuna mensup veri sorumluları grup içi veri aktarımları konusunda ilan edilen kılavuzlara uygun olarak bağlayıcı şirket kuralları hazırlayarak Kurul'un onayın sunabilecektir. Bu bağlayıcı şirket kurallarının Kurul tarafından onaylanması sonrasında bu şirketler topluluğuna üye şirketler arasında yurt dışı veri aktarımı yapılabilecektir. Hazırlık ve onay süreçlerinin uzun sürmesi öngörülse de grup içi veri aktarımları için kalıcı bir yöntem olarak şekillenmektedir.

c. Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı,

i. Değişiklik Kanunu ile birlikte getirilen en önemli değişikliklerden biri olarak değerlendirilen standart sözleşmeler GDPR bünyesinde bulunan "Standard Contractual Clauses" benzeri bir mekanizma olarak karşımıza çıkmaktadır.

ii. Ancak Kanun kapsamındaki standart sözleşmelerin uygulamasında, GDPR kapsamındaki Standard Contractual Clauses uygulamasından önemli farklılıklar bulunmaktadır. Kurul tarafından ilan edilmiş bulunan standart sözleşme metinlerinin üzerlerinde özellikle izin verilen haller haricinde hiçbir değişiklik yapılmadan imzalanması ve imzalanan sözleşmelerin de imzacıların imza yetkilerini tevsik edici belgeler ile birlikte Kurum'a imza tarihinden itibaren 5 iş günü içerisinde bildirilmesi zorunlu tutulmuştur.

iii. Ayrıca ilan edilen standart sözleşmeler veri alıcısı ve veri aktaran taraflara ilişkin olarak oldukça kapsamlı bir hazırlık gerektirmekte ve aşağıdaki konulara ilişkin bilgilerin sağlanmasını gerektirmektedir:

i. veri aktaran tarafın ve veri alıcısı olan tarafın aktarılan kişisel verilere ilişkin faaliyetleri,

ii. aktarılan kişisel verilerin ilgili kişi grupları,

iii. aktarılan kişisel veri kategorileri ve varsa aktarılan özel nitelikli kişisel veri kategorileri,

iv. aktarımın hukuki sebebi,
v. aktarım sıklığı,
vi. veri işleme faaliyetinin niteliği,
vii. veri aktarımının ve devamında gerçekleştirilecek işleme faaliyetinin amaçları,
viii. kişisel verileri saklama süresi,
ix. alıcılar veya alıcı grupları,
x. x. veri aktaranın Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) bilgileri,
xi. eri İşleyene ve Alt Veri İşleyene aktarımlarda işleme faaliyetinin konusu, niteliği ve süresi,
xii. alınan teknik ve idari tedbirler, ve varsa özel nitelikli kişisel verilerin aktarılması halinde bunlar bakımından ayrıca alınan teknik ve idari tedbirler ve
xiii. varsa, alt veri işleyenlerin listesi

d. Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi.

Son olarak, bir yeterlilik kararı bulunmaması veya aktarım yapacak olan veri sorumluları tarafından uygun güvenlerden herhangi birinin sağlanamaması durumunda, arızi olmak kaydıyla, bir diğer anlatımla düzenli olmayan, tek veya birkaç sefer gerçekleşen, süreklilik arz etmeyen ve olağan faaliyet akışı içerisinde bulunmayan bazı sınırlar haller için bazı istisnalar öngörülmüştür. Ancak söz konusu istisna halleri sınırlı haller için geçerli olabileceğinden veri sorumlularının olağan ve düzenli iş süreçleri dahilindeki yurt dışı veri aktarım süreçlerinde aşağıdaki sebeplere dayanmaması ve Kanun'da belirtilen diğer uygun güvenceleri sağlayacak şekilde süreçlerini düzenlemesi önerilmektedir:

- ilgili kişilerin muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermeleri,
- aktarımın ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması,
- aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması,
- aktarımın üstün bir kamu yararı için zorunlu olması,
- bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması,
- fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması,
- kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması.

Dikkat edilmesi gerekir ki, Değişiklik Kanunu ile birlikte açık rıza hukuki sebebine dayalı aktarımlar yalnızca arızi durumlarda kabul

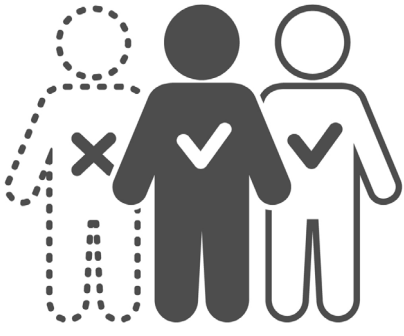
edilen şekilde düzenlenmiştir. Değişiklik öncesi dönemde uygulamadaki yurt dışı veri aktarımlarının çoğu açık rızaya dayanmakta olduğundan Değişiklik Kanunu kapsamında Kanun'a bir geçici madde eklenerek yurt dışı veri aktarımlarında bir geçiş süreci öngörülmüş ve 1 Eylül 2024 tarihine kadar açık rıza hukuki sebebine dayanılarak yurt dışı veri aktarımına devam etme imkanı sağlanmıştır.

Bu çerçevede, 1 Eylül 2024 tarihinden sonraki dönemde veri sorumlularının düzenli şekilde gerçekleştirdikleri yurt dışı veri aktarımı süreçlerinde, henüz bir yeterlilik kararı da olmadığı göz önünde bulundurularak, mutlaka Kanun'da öngörülen uygun güvencelerden birini sağlamaya dikkat etmeleri gerekmektedir. Güncel durumda geçiş hükmü ile sağlanan uyum periyodunun da sona erdiği göz önünde bulundurularak yurt dışı veri aktarım süreçlerini uyumlu hale getirmemiş bulunan veri sorumlularının ivedilikle yurt dışı veri aktarım süreçlerinin kapsamlarını detaylı bir şekilde belirlemesi, hangi şirketlere veri aktarımı yaptığını tespit etmesi ve öngörülen uygun güvencelerden birini sağlamak üzere çalışmalarını hızlıca tamamlaması önerilmektedir.

Son olarak, Değişiklik Kanunu ile birlikte Kanun'a yeni idari para cezası eklenmiştir. Yukarıda belirtildiği üzere veri sorumluları ve veri işleyenlere getirilen yurt dışı aktarımı için imzalayabilecekleri standart sözleşmeleri 5 iş günü içerisinde Kurum'a bildirme yükümlülüğüne aykırı davranılması halinde hem veri sorumluları hem de veri işleyenler hakkında yeniden değerleme oranı ile birlikte 2025 yılı için 71.965 TL ile 1.439.300 TL olarak uygulanacaktır. Veri sorumlularının mevcut yurt dışı veri aktarımı süreçlerinde uygun bir güvencenin 1 Eylül 2024 tarihine kadar sağlanmamış olduğunun tespiti halinde ise 2025 yılı için 204.285 TL'den 13.620.402 TL'ye kadar idari para cezası uygulanması riski mevcuttur.

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 de 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.

Söz konusu minimum kriterlere ilişkin olarak ise Kurul, 2023 yılında yayımlandığı karar ile VERBİS kayıt yükümlülüğünden istisna tutulan veri sorumlularının belirlenmesinde kullanılan kriterlerden yıllık mali bilanço toplamı 25 milyon Türk Lirasından fazla olma kriterindeki yıllık mali bilanço toplamı tutarı güncellenerek 100 milyon Türk Lirası seviyesine çıkartılmıştır. Mevcut hali ile belirlenen kriterlerin altında olan, yani 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 olmayan veri sorumluları VERBİS kaydından istisna tutulmaktadır. Türkiye'de yerleşik veri sorumluları açısından çalışan sayısı ya da yıllık mali bilanço toplamına ilişkin sınırlardan sadece birisinin geçilmiş olmasının VERBİS kayıt yükümlülüğünün başlaması için yeterli olduğuna, ve ayrıca yurtdışına yerleşik veri sorumluları açısından ise yükümlülüğün değerlendirilmesinde söz konusu kriterlerin uygulanmadığına da dikkat edilmesi gerekmektedir.

2025 yılı için VERBİS kayıt yükümlülüğünün ihlali halinde uygulanması öngörülen idari para cezası aralığı 272.380 TL ile 13.620.402 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.

Dolayısıyla, yurt içinde yerleşik bir veri sorumlusunun ortağı olan yurtdışında yerleşik tüzel kişiler, kendilerine aktarılan 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 gerçekten 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.

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 tamamlanmasını öneririz.

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.

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 yasal düzenleme niteliğini taşıyan ve 1 Ağustos 2024 tarihinde yürürlüğe giren Avrupa Birliği Yapay Zeka Yasası'nın ("AI Act"), öncü mevzuat olarak bir çok ülke için, yapay zeka ve bağlantılı hususlarda ulusal politika ve stratejilerini belirlemede ve mevzuat çalışmalarında rehber olacağı değerlendirilmektedir.

Henüz Avrupa Birliği'nde yapılan düzenlemelerin 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.

2024 yılı Türkiye'de, yapay zeka teknolojisinin geliştirilmesi ve uygulanması konusunda aktif adımların atıldığı bir yıl olmuştur. 2021-2025 yılları için hazırlanan "Ulusal Yapay Zeka Stratejisi" kapsamında Türkiye, bu teknolojinin geliştirilmesi ve kullanılması için 2024-2025 eylem planı da oluşturarak bir yol haritası çizmiştir. Eylem planında, yapay zeka uygulamalarının hukuken değerlendirilmesine ilişkin rapor oluşturulması ve bu uygulamaların yasalara uyumunun denetlenmesine ilişkin eylemler olmakla birlikte yapay zekaya özgü kanun düzeyinde bir düzenleme yapılması henüz öngörülmemiştir. Öte yandan, eylem planından bağımsız olarak yapay zekanın hukuken düzenlenmesine yönelik bazı çalışmalar yapılmış ve bu konuya özgü ilk kanun teklifi hazırlanarak 2024 yılında meclise sunulmuştur. Bu kanun teklifinin henüz yeterli bir çerçeve sunmadığı düşünülse de,

bu ilk teklif açısından da Türkiye'nin, yapay zeka düzenlemeleri konusunda da Avrupa Birliği'ne paralel bir yaklaşım sergileyeceği değerlendirebilir.

Yapay zeka alanında yaşanan gelişmelere Kişisel Verileri Koruma Kurumu da kayıtsız kalmamış, Yapay Zeka Alanında Kişisel Verilerin Korunmasına Yönelik Tavsiyeler başlıklı yayınında yapay zeka alanında faaliyet gösteren, geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcılar için Kanun kapsamında kişisel verilerin korunması amacına yönelik önerilerini kamuoyu ile paylaşmıştır. Yayınlanan tavsiye metninde yer alan temel ilkelerin esasen GDPR madde 22 altında düzenlenen otomatik yollarla kişisel verilerin işlenmesinde uygulanan kurallara işaret ettiği görülmektedir ki bu henüz kanun sistematiğinde yer almamış olsa da Kurul tarafından GDPR maddelerinin yapay zeka uygulamalarında dikkate alındığını göstermektedir. Kurulun ilettiği tavsiyeler uyarınca, temel hak ve özgürlüklerinin korunması bakımından yapay zeka uygulamalarının insan merkezli bir anlayışla yönetilmesi gerekmektedir. Ürün ve hizmetlerin tasarımından başlayarak yaşam döngüsü boyunca veri koruma hukukuna uygunluk açısından hesap verebilirliği sağlayacak algoritmalar benimsenmelidir.

Uygulamalardan etkilenmesi muhtemel olan bireylerin ve grupların katılımına dayalı risk değerlendirmeleri yapılmalıdır. Kullanılan kişisel verilerin kalitesi, niteliği, kaynağı ve miktarı değerlendirilerek asgari veri kullanımına gidilmesi, geliştirilen modelin doğruluğu izlenmelidir. Bireylerin münhasıran kendi görüşleri dikkate alınmaksızın otomatik işlemeye dayalı olarak kendilerini etkileyecek bir karara maruz kalmamalarını sağlayacak ürün ve hizmetler tasarlanmalıdır. Yapay zeka teknolojilerinin geliştirilmesinde aynı sonuca kişisel veri işlenmeksizin ulaşılabiliyorsa, veriler anonim hale getirilerek işlenmelidir.

Yapay zeka çalışmalarında tüm sistemler tasarımdan itibaren veri koruma ilkesine göre geliştirilmelidir. Karar alma süreçlerinde insan müdahalesi rolü tesis edilmesini, bireylerin, yapay zeka uygulamaları ile sunulan önerilerin sonucuna güvenmeme özgürlüğü korunmalıdır. Kullanılan kişisel verilerin kalitesi, niteliği, kaynağı ve miktarı değerlendirilerek asgari veri kullanımına gidilmesi, geliştirilen modelin doğruluğu izlenmelidir. Yapay zeka çalışmalarında kişisel verilerin korunması açısından yüksek risk öngörülüyorsa mahremiyet etki değerlendirmesi uygulanmasını ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmelidir. Kişisel verilerin korunması farkındalığı oluşturmak bakımından veri mahremiyeti çerçevesinde eğitimler ve bilgilendirme çalışmalarının teşvik edilmelidir.

Yapay zeka sistemlerinin kişisel verileri toplama, analiz etme ve kullanma süreçleri, bireylerin mahremiyet hakları ve veri koruma mevzuatına uyum açısından ciddi soruları gündeme getirmektedir. Kişisel Verilerin Korunması Kanunu, yapay zekanın geliştirilmesi ve kullanımında şeffaflık, veri minimizasyonu, hukuka uygunluk ve hesap verebilirlik gibi prensipleri zorunlu kılmakta, yapay zeka sistemlerinin hukuki perspektiften de sürdürülebilir bir şekilde yönetilmesi büyük önem taşımaktadır ve bu konuda detaylı kuralların getirilmesi gerçek bir ihtiyaç durumundadır.

Çerezler

Çerezler, dijital dünyada kullanıcı deneyimini kişiselleştirmek ve iyileştirmek için kritik bir rol oynamaktadır. Çerezlerin kullanımı, internet deneyimini kişiselleştirmeye ve kullanıcıların çevrimiçi tercihlerini hatırlamaya büyük katkı sağlasa da, bu süreç aynı zamanda çeşitli gizlilik ve veri koruma endişelerini de beraberinde getirmiştir. Kişisel verilerin çerezler yoluyla işlenmesiyle ilgili en büyük endişelerden biri, kullanıcıların çoğu zaman bu işlemden haberdar olmamaları veya çerezlerin kullanımı konusunda yeterli şeffaflığın sağlanmamasıdır. Çerez politikaları ve gizlilik beyanları genellikle kullanıcıların kolayca erişebileceği ve anlayabileceği bir biçimde sunulmadığından, bu durum, kullanıcıların çevrimiçi gizliliklerini nasıl koruyacaklarını bilememelerine ve dolayısıyla verileri üzerinde yeterli kontrole sahip olamadıkları için onları yönetememe ve çevrimiçi izlenmelerini sınırlayamamalarına neden olmaktadır.

Çerezler ile ilgili uygulayıcılar arasında sıklıkla tartışma konusu olan gizlilik ve veri koruma endişeleri sonucunda, son yıllarda aralarında Türkiye'nin de olduğu birçok ülkede veri koruma otoriteleri kişisel verilerin çerezler yoluyla işlenmesi ile ilgili kural ve ilkeleri belirlemekte, kılavuzlar yayınlamakta ve veri sorumlularına cezalar uyguladığı kararlar yayınlamaktadır.

Kurul, çerezler yoluyla kişisel veri işleyen veri sorumlularına yönelik tavsiye niteliğinde ve yol gösterici mahiyette bir doküman oluşturulması amacıyla Çerez Uygulamaları Rehberi ("Rehber") hazırlayarak Haziran 2022'de Kurul'un internet sitesinde yayınlamıştır. Rehberde genel olarak çerezler ve çerezlerin türleri düzenlenmekte, ayrıca sürelerine, kullanım amaçlarına ve taraflarına göre çerez türleri sınıflandırılmaktadır.

Rehberde 5809 sayılı Elektronik Haberleşme Kanunu ("EHK") ile Kanun'un arasındaki ilişki de incelenmiştir. Çerezin sadece, iletişimin elektronik haberleşme şebekesi üzerinden sağlanması amacıyla kullanılması durumunda ve veri sorumlusunun da EHK kapsamında işletmeci sıfatını haiz olması halinde açık rıza alınmasına gerek kalmadan veri işlenmesi mümkün olmaktadır. Rehberde, çerez uygulamaları açısından yukarıda sayılan ve EHK'nın uygulama alanı bulacağı sınırlı haller dışında Kanun'un uygulama alanı bulacağı ve Kanun'da yer alan ilkeler ve veri işleme nedenlerinin çerezler yoluyla kişisel verilerin işlenmesi halinde de gözetilmesi gerekeceği belirtilmektedir.

Rehberde ayrıca açık rıza alınması gereken hallerde açık rıza ve aydınlatmaya ilişkin açıklayıcı detaylara yer verilmiştir. Buna göre

Rehber kapsamında açık rıza alınırken siteye girildiği anda ziyaretçiye bir çerez yönetim paneli gösterilmeli ve burada eşit renk, büyüklük ve puntoda "kabul et", "reddet", ve "tercihler" butonları sunulmalıdır. Ziyaretçiye, tercihler butonu üzerinden açık rıza olmaksızın kullanılamayacak çerezler açısından onay verme / vermeme imkanı tanınmalı ve açık rızaya dayalı çerez uygulamaları ilk etapta kapalı/pasif şekilde gelmelidir. Rehber'de bu durum, veri sorumluları tarafından ilgili kişilerden alınacak açık rıza beyanlarında olması gerekenin opt-in yani bireyin bilinçli eylemi ile kişisel verilerinin işlenmesine önceden onay vereceği bir sistem olduğu belirtilmektedir. Ayrıca, rıza yorgunluğunun önlenmesi bakımından ilgili kişinin siteye her girişinde açık rıza alınması yoluna gidilmemesi ve açık rızaya dayalı olarak kullanılacak çerezleri bir defa reddeden ziyaretçiye hatırlatmanın söz konusu çerezin ömrü ile orantılı olacak şekilde periyodik olarak yapılması gerektiği vurgulanmaktadır.

Ayrıca internet sitesine erişimi engelleyen ve ziyaretçinin çerez uygulamalarına onay vermeden internet sitesinden yararlanmasını önleyen "çerez duvarı" adı verilen sistemler Kanun'a uygun kabul edilmemektedir.
Belirtmek gerekir ki, Kanun'un aydınlatma yükümlülüğü açısından ortaya koyduğu ilkeler çerezler açısından da aynı şekilde uygulama alanı bulmaktadır, ziyaretçinin açık rızasına ya da başka bir veri işleme şartına dayalı olmasından bağımsız olarak her bir çerez aracılığıyla yapılan veri işleme faaliyeti için ziyaretçinin Kanun'a uygun biçimde aydınlatılması gerekmektedir.

Çerezlerin kullanımı, yasal dayanakları, rıza gerektiren durumlar, rızanın yasal şartları ve bilgilendirme süreçleri dahil olmak üzere çerez kullanımının tüm yönlerine ışık tutan Rehber'de veri sorumluları tarafından dikkat edilmesi gereken önemli noktalar da vurgulanmış, açık ve anlaşılır örneklerle konu daha somut bir hale getirilmiştir.

Veri sorumlularının çerezler ile ilgili olarak mevcut uygulamalarının Kurul tarafından yayınlanan Rehber ile uyumluluğunu gözden geçirmeleri ve çerezler yoluyla kişisel veri işleme faaliyetlerini hukuka uygun hale getirmeleri oldukça önemlidir. Nitekim çerezler ile ilgili uygulamalar incelendiğinde, bazılarında kullanıcılara "reddet" seçeneğinin sunulmadığı, bazılarında reddetme olanağının kabul etme olanağı kadar kolay sunulmadığı, bazılarında halen opt-out sisteminin kullanıldığı görülmektedir. Yanlış uygulamalar dışında Rehber'e uygun şekilde tasarlanan çerez uygulamaları bakımından da çerez kullanım şartlarında yeterli şeffaflığın sağlandığı, aydınlatma metinleri ile ilgili olarak da köprü bağlantılar ile kullanıcının doğru şekilde bilgilendirilmesini sağlayacak metinlere ulaşımının zorlaştırılması gibi uygulamaların açık rızanın geçerliliğini sakatlayabileceği unutulmamalıdır.

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 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.

Kurulun, bildirimde bulunurken veri sorumlularının doldurmaları gereken "Kişisel Veri İhlali Bildirim Formu" mevcuttur.

Yine Kurum'un internet sitesinde yayınlanan veri ihlal bildirimleri incelendiğinde ihlal bildirimlerinin çoğunlukla özel şirketler tarafından yapılmış olmasına karşın hastane ve üniversite gibi kuruluşlarca da ihlal bildirimleri yapıldığı görülmektedir. Diğer taraftan ihlallerden etkilenen kişi kategorilerinin ağırlıklı olarak ilgili veri sorumlularının çalışanları, hastaları, aboneleri, müşterileri, öğrencileri, klinik araştırma katılımcıları ve iş ortaklarından oluştuğu görülmektedir. Etkilenen veri kategorilerine baktığımızda ise, etkilenen veri kategorilerinin 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 verilerden oluştuğu görülmektedir. Söz konusu veri ihlali bildirimleri hem yurtiçinden hem de yurtdışından yapılmıştır.

İlaveten yayımlanan veri ihlallerinin önemli bir kısmının plastik sanayi ve bağlantılı sektörlerdeki veri sorumluları tarafından aynı gün maruz kalınan siber saldırı sonucunda gerçekleşen veri ihlallerinden oluştuğu görülmektedir. Diğer önemli kısmının ise bir hizmet sağlayıcı veri sorumlusunun maruz kaldığı yönetim paneline sızılması saldırısı sonucunda kendisinden hizmet alan veri sorumluları tarafından bildirilen veri ihlallerinden oluştuğu görülmektedir. Sonuç olarak 2024 yılına baktığımızda veri ihlali bildirimlerinin çok çeşitli tür ve sektördeki veri sorumluları tarafından yapılmış olduğu görülmektedir.

Veri ihlali ile ilgili 2024 yılı istatistiklerine baktığımızda, 81 veri ihlal bildirimi Kurul'a intikal etmiş, bu bildirimlerin 63'ü kamuoyuna ilan edilmiştir. Kurum'un internet sitesinde yayınlanan veri ihlal bildirimleri incelendiğinde, veri ihlallerinin genellikle fidye yazılım saldırısı, siber saldırı, kullanıcı hesaplarına yetkisiz erişim, bir dahili kullanıcının kimlik bilgilerinin ele geçirilmesi, veri sızıntısı, verilerin silinmesi, sunucuların kitlenmesi, yönetici paneline sızılması, verilerin çevrimiçi olarak herkese açık bir şekilde yayımlanması ve oltalama saldırıları sonucunda gerçekleştiği görülmektedir.

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

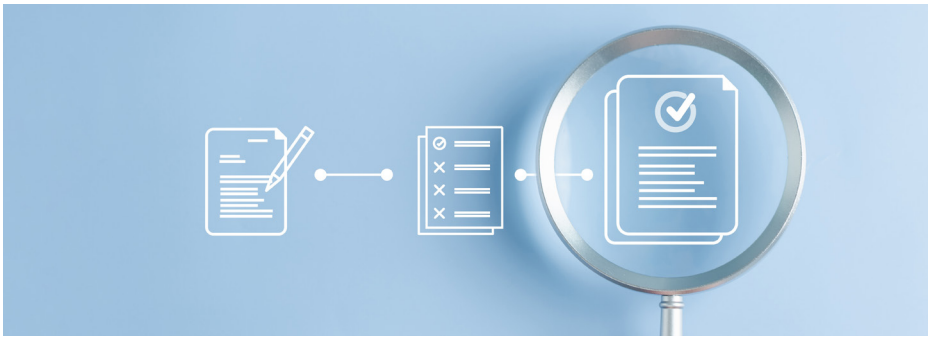
verilmesi veya ele geçirilmesine ilişkin yaptırımların yer aldığı ilgili hükümlerine atıfta bulunmaktadır.

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 68.083 – 13.620.402 TL'ye kadar (2025 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 karar 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 2025 yılında aşağıdaki şekilde uygulanacaktır:

Administrative Fines under the Law for 2025		
Legal Basis	**Breach Type**	**Current Administrative Fine**
Article 18/1/a of the Law	Failure to fulfil the disclosure obligation	TRY 68,083 – 1,362,02
Article 18/1/b of the Law	Failure to fulfil the data security obligations	TRY 204,285 – TRY13,620,402
Article 18/1/c of the Law	Failure to comply with the Board's decisions	TRY 340,476 – TRY 13,620,402
Article 18/1/ç of the Law	Failure to fulfil the obligations of register and notify the Data Controllers Registry	TRY 272,380 – TRY 13,620,402
Article 18/1/d of the Law	Failure to notify the Authority of Standard Contracts within 5 business days	TRY 71,965 – TRY 1,439,300

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 bir hayli 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.

Sulh Ceza Hakimlikleri tarafından verilen kararların yüzeysel ve hukuki gerekçeden yoksun olduğu gözlemlenmekle birlikte bu durumun bireyler açısından hak kaybı yarattığı yönünde görüşler ağırlıktaydı. Diğer bir yandan ise Sulh Ceza Hakimliklerinin kararlarına karşı yapılan itirazların bir diğer Sulh Ceza Hakimliği tarafından inceleniyor olması, bu kararların kesinleşmesine ve tesis edilen kararların yüksek mahkeme denetiminden geçmemesine sebep olmuş ve kişisel verilerin korunması hukuku alanında içtihat oluşturulmasına bir engel teşkil etmiştir.

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 olmaktadır. 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 bu kararı ile de ortaya konmuştur. Adalet Bakanlığı'nın yayımlamış olduğu İnsan Hakları Eylem Planı ile daha öncesinde, Kanun'un Avrupa Birliği standartları ile uyumlu hale getirileceği ve Kurul'un idari para cezası kararlarına karşı sulh ceza hakimlikleri yerine idari yargıya başvuru imkanı sağlanacağı ilan edilmiştir.

Değişiklik Kanunu 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;

- Fiilin Kanun değişikliğinden önce gerçekleşmiş ve bitmiş olduğu hallerde;
    - 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.

- Fiilin Kanun değişikliğinden önce başlamış ve devam ediyor olduğu hallerde (mütemadi hareketli – devam eden fiil hallerinde);
  - Fiilin Kanun değişikliğinden önce kesilmesi halinde lehe olan Kanun uygulanacaktır, ve
  - Fiil Kanun değişikliği sonrasında kesiliyor ise değişiklik sonrası yeni Kanun uygulanacaktır.
- Fiilin Kanun değişikliğinden sonra gerçekleşmiş olması halinde;
  - Bu hallerde zaman bakımından uygulama sorunu ortaya çıkmayacak ve yeni Kanun uygulanacaktır.

EKİBİMİZ

BEGÜM YAVUZDOĞAN OKUMUŞ
ORTAK AVUKAT

begum.yavuzdogan@gun.av.tr

DİCLE DOĞAN
YÖNETİCİ AVUKAT

dicle.dogan@gun.av.tr

DİRENÇ BADA
YÖNETİCİ AVUKAT

direnc.bada@gun.av.tr

YALÇIN UMUT TALAY
YÖNETİCİ AVUKAT

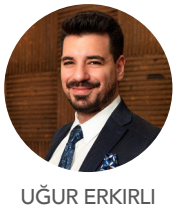
umut.talay@gun.av.tr

SEDA TAKMAZ
KIDEMLİ AVUKAT

seda.ozturk@gun.av.tr

GÜNCE GÜNEŞ CEYLAN
AVUKAT

gunes.ceylan@gun.av.tr



UĞUR ERKIRLI
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
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
Istanbul, Turkey

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

www.gun.av.tr