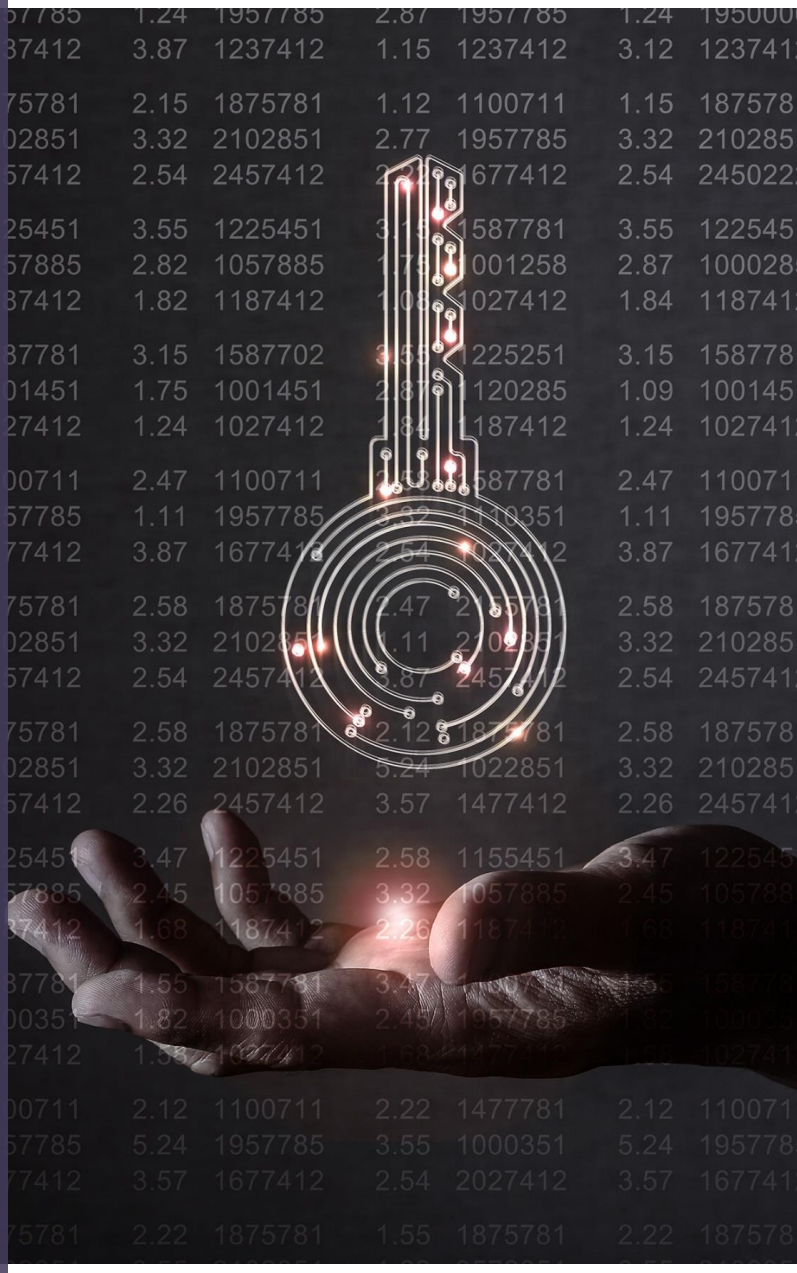
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR
BÜLTENİ

ARALIK 2020

AYIN KARAR ÖZETLERİ VE HABERLER

Bir Banka Tarafından Kurul Kararı ile Verilen Talimatın Gereğinin Yerine Getirilmemesi Hakkında Kurul Kararı

Karar No: 2020/765 **Karar Tarihi**: 08.10.2020
Konu Özeti: Bir banka tarafından Kurul kararı ile verilen talimatın gereğinin yerine getirilmemesi hakkında Kurul kararı

Karara göre Kurul, veri sorumlusu bankayı, ilgili kişinin;

- Kişisel Verilerin Korunması Kanunu kapsamında haklarını kullanmak üzere yaptığı başvuruya, 30 günlük yasal süre içinde cevap vermemesi;

- Bankanın internet sitesinde yayımlanan aydınlatma metninin Kurum tarafından yayımlanan tebliğe uygun olmaması; metinde kişisel verilerin işlenmesindeki sebeplerin belirtilmemesi ve kişisel verilerin işlenme amaçları için genel ifadeler kullanılması sebebiyle ilgili kişinin şikâyeti üzerine, internet sitesinde yer alan "Kişisel Verileriniz Koruma Altında!" başlıklı metnin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun hâle getirilmesi konusunda talimatlandırmıştır.

Talimatın veri sorumlusu bankaya tebliğ edilmesinden sonra banka aydınlatma metnine;

- *"Bankamızdan alacağınız ürün ve hizmetler nedeni ile kuracağınız ilişki çerçevesinde; Kişisel verileriniz aşağıda belirtilen hukuki sebeplere dayalı olarak işlenmektedir"* ifadesi ile birlikte 6698 sayılı Kanun'un 5. ve 6. maddesinde yer alan hükümlerin eklendiği;

- İşlenen kişisel verilere kategorik olarak yer verilmediği yalnızca yukarıda belirtildiği gibi kanun hükümlerinin sıralandığı;

- Veri işleme amaçlarına bazı eklemeler yapılmakla birlikte, genel itibariyle, talimatta yer verilen şekilde metni Tebliğe uygun hâle getirecek ilgili değişikliklerin yapılmadığı düzenlenmekle birlikte;

- Bankanın, yürüttüğü sosyal sorumluluk projeleri ve kurumsal marka çalışmaları ve reklam faaliyetleri gibi diğer faaliyetlerinde ilgili gerçek kişiler hakkında özel ve ayrı aydınlatma metinlerinin yer aldığı beyanında bulunmasına karşın Kurum'a bunu kanıtlayacak herhangi bir belge sunmadığı;

- Bunun yanında kredi kartı başvurusu veya ihtiyaç kredisi başvurusunda da ilgili kişilere "Kişisel Verilerin Korunması" başlıklı genel bir aydınlatma metninin sunulduğu ve bu kapsamda da Kurul'un talimatında yer alan *"aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerekliliği"* hükmüne uyulmadığı Kurul tarafından değerlendirilmiş olup;
- Veri sorumlusu tarafından yayımlanan aydınlatma metninin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak düzenlenmemesi ve Kurul Kararı ile verilen talimatın yerine getirilmemesi sebebiyle bankaya 120.000 TL idari para cezası uygulanmasına karar verilmiştir.

Bir Banka Tarafından Kurul Kararı ile Verilen Talimatın Gereğinin Yerine Getirilmemesi Hakkında Kurul Kararı

Karar No: 2020/766 **Karar Tarihi**: 08.10.2020
Konu Özeti: Bir banka tarafından Kurul kararı ile verilen talimatın gereğinin yerine getirilmemesi hakkında Kurul kararı

Karara göre Kurul, veri sorumlusu bankayı, ilgili kişinin;

- Kişisel Verilerin Korunması Kanunu kapsamında haklarını kullanmak üzere yaptığı başvuruya veri sorumlusu tarafından verilen cevabın yetersiz bulunması;
- Bankanın internet aydınlatma metni yerine, veri sorumlusu tarafından, 20 sayfalık Kişisel Verilerin İşlenmesi ve Korunması Politikasına link verilmesi, ve dokümanda ilgili kısımları bulabilmek için detaylı bir inceleme yapılması gerektiği, listelenen kişisel verilerin aktarım amaçlarının belirli bir konuya ilişkin olmaması sebepleriyle Kurul, gizlilik politikası metninin aydınlatma yerine geçmeyeceği, aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerektiği hususlarında gerekli düzenlemelerin yapılması ve metnin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e uygun hale getirilmesi konusunda talimatlandırmıştır.

Talimatın veri sorumlusu bankaya tebliğ edilmesinden sonra banka;

- Kurul'a internet sitesinde yer alan gizlilik politikasından farklı olarak ilettiği aydınlatma metninde kategorik bazda verilerin listelenerek, verilerin hangi ortamlarda ve hangi şekilde elde edildiği, neden işlendiği, aktarıldığı, hangi hukuki gerekçelerle hangi kurum ve kişilere aktarım yapıldığı ve verilerin ne kadar süre ile işlenip, saklandığına ilişkin net, anlaşılır ifadelere yer verilerek gerekli bu şartların sağlandığı
- Fakat işbu aydınlatma metninde işlenen kişisel verilerin hangi kişisel veri işleme şartına dayanılarak işlendiğine dair Tebliğ'e uygun bir aydınlatma yapılmadığı,

- "Kişisel Verilerinizi Hangi Hukuki Gerekçe ile İşliyoruz?" başlığı altında Kişisel Verilerin Korunması Kanunu'nun 5. maddesinde yer alan şartların listelendiği,

- Özel nitelikli kişisel veriler için ise yalnızca rızaya bağlı olarak işlendiği bilgisinin verildiği tespit edilmiştir.

Bu kapsamda veri sorumlusuna tebliğ edilen talimatta yer alan "*…veri sorumlusu tarafından işlenen kişisel verilerin hangi kişisel veri işleme şartlarına dayanarak işlediklerine ilişkin ayrıntılı şekilde yer verilmesi…"* gerekliliğine aykırı davranıldığı Kurul tarafından vurgulanmıştır.

- Bunun yanında veri sorumlusu bankanın cevabında Kurul'un talimatında yer alan *"aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi…"* hususuna yer vermediği ve bununla ilgili tevsik edici herhangi bir belge sunmadığı Kurul tarafından değerlendirilmiş olup; kredi kartı başvurusu ve konut kredisi başvurusu sırasında sunulan aydınlatma metinlerinin, bu başvurulara özgü olmadığı ve genel bir aydınlatma metni olduğu tespit edilmiştir.

- Veri sorumlusu tarafından talimatlandırma sonrasında hazırlanan aydınlatma metninin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak düzenlenmemesi ve Kurul Kararı ile verilen talimatın yerine getirilmemesi sebebiyle bankaya 120.000 TL idari para cezası uygulanmasına karar verilmiştir.

"Alenileştirme" Hakkında Kamuoyu Duyurusu

Kişisel Verileri Koruma Kurumu tarafından 16.12.2020 tarihinde yapılan duyuruda, Kişisel Verilerin Korunması Kanunu'nun 5. maddesinde yer alan işleme şartlarından birinin *"ilgili kişinin kendisi tarafından alenileştirilmiş olması"* olduğu belirtilmiş; alenileştirme kavramının ilgili kişinin kişisel verilerinin kendisi tarafından kamuoyuna açıklanması anlamına geldiği ifade edilmiştir. Bununla birlikte duyuruda, bu ifadenin dar yorumlanması gerektiği vurgulanmıştır.

Duyuruya göre bir verinin aleni kabul edilebilmesi için; ilgili kişinin verinin aleni olması yönünde bir iradesinin var olması ve ilgili kişinin ne amaç ile kişisel verilerini alenileştirdiğinin de tespit edilmesi gerekmektedir.

Kişinin iradesi dışında bir sebeple kişisel verinin kamuoyuna açıklandığı durumlarda Kanun kapsamında bir alenileştirmeden söz etmek mümkün olmayacaktır.

Ayrıca, verinin ilgili kişi tarafından alenileştirilmiş olması, veri sorumlularının, alenileştirme amacı dışında bu veriyi işlemelerini özgür kılmayacaktır.

Bu sebeple, Kanun'un 5. maddesinin 2. fıkrasının d bendine (alenileştirme) dayanılarak gerçekleştirilen kişisel veri işleme faaliyetlerinde yukarıdaki esasların ve Kanun'un genel ilkelerinin gözetilmesi önem arz etmektedir.

Konuya ilişkin, Kişisel Verileri Koruma Kurulu 07.11.2019 tarihli ve 2019/331 sayılı kararını yayımlamıştır. Karara buradan ulaşabilirsiniz.

Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş. - Veri İhlali Bildirimi

Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş. tarafından yapılan veri ihlali bildirimi ile;

- Veri sorumlusu bünyesinde çalışan satış sonrası hizmetler müdürünün yetkisini kötüye kullanarak verileri raporlar halinde aldığı, bu durumun müşteri şikayetiyle farkına varıldığı ve logların kontrol edilmesi sonucunda ihlalin tespit edildiği,
- Söz konusu ihlalin 16.12.2020 tarihinde başladığı, 19.12.2020 tarihinde sona erdiği ve 18.12.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişi sayısının 17.092 olduğu, ihlalden etkilenen kişisel verilerin kimlik, iletişim, müşteri işlem verileri ve müşteri kartında yer alan notlar olduğu Kurum'a iletilmiştir.

Söz konusu ihlal 22.12.2020 tarihinde Kurum'un internet sitesinde yayınlanmıştır.

Ficosa Otomotiv San. ve Tic. A.Ş. - Veri İhlali Bildirimi

Ficosa Otomotiv San. ve Tic. A.Ş. tarafından yapılan veri ihlali bildirimi ile,

- Veri sorumlusunun sunucularına 16.12.2020 tarihinde fidye saldırısının gerçekleştirildiği ve dosyaların şifrelendiği, ihlalin loglarda bir problem olduğunun fark edilmesiyle tespit edildiği,
- İhlalden etkilenen kişisel verilerin; ad, soyadı, e-posta ve/veya telefon numarası olduğu ancak bilişim incelemesinin devam ettiği,

- İhlalden çalışanların, müşterilerin, tedarikçiler ve hizmet sağlayıcıların etkilendiği,
- İhlalden tahmini 976 kişinin etkilendiği, incelemenin devam ettiği dolayısıyla kişi ve kayıt sayısının tam olarak bilinmediği,

Kurum'a bildirilmiştir.

Söz konusu ihlal Kişisel Verileri Koruma Kurulunun 22.12.2020 tarih ve 2020/987 sayılı Kararı ile Kurumun internet sayfasında ilan edilmiş ve konuyla ilgili incelemenin devam ettiği belirtilmiştir.

UiPath SRL - Veri İhlali Bildirimi

UiPath SRL tarafından yapılan veri ihlali bildirimi ile;

- Veri sorumlusunun, kullanıcıların UiPath yazılımını öğrenmelerini sağlayan UiPath Akademisi'nin ("*Akademi*") idaresi amacıyla, Akademi'ye katılan kullanıcıların kayıt bilgilerini içeren bir dosya tuttuğu, veri sorumlusu çalışanının söz konusu dosyayı kullanıcıların kaydını tutmak amacıyla bir tedarikçinin yazılım platformuna yüklediği, yetkisiz bir kullanıcının, dosya izin ayarlarında kazara gerçekleştirilen yanlış bir yapılandırma nedeniyle dosyaya eriştiği,
- Veri ihlalinin 01.12.2020 tarihinde, bir üçüncü tarafın veri sorumlusuna etkilenen dosyanın halka açık bir internet sitesinde ulaşılabilir durumda olduğunu bildirmesiyle tespit edildiği,
- İhlalden, kişilerin ad ve soyadı, kullanıcı adı, e-posta adresi, duruma göre kullanıcının işvereni olan şirketin ismi, kullanıcının ülkesi, veri sorumlusu tarafından verilen UiPath Akademi sertifikasyon düzeyi ve artık şirket tarafından kullanılmamakta olan UID kodu bilgilerinin etkilenmiş olabileceği,
- İhlalden etkilen kişi grubunun kullanıcılar olduğu, ihlalden Türkiye'yi kendi ülkesi olarak belirten 4,692 kişinin etkilendiği belirtilmiştir.

Söz konusu ihlal, Kişisel Verileri Koruma Kurulu'nun 22.12.2020 tarih ve 2020/984 sayılı Kararı ile Kurumun internet sayfasında ilan edilmiş ve incelemenin devam ettiği belirtilmiştir.

Ficosa International Otomotiv San. ve Tic. A.Ş. - Veri İhlali Bildirimi

Ficosa International Otomotiv San. ve Tic. AŞ tarafından yapılan veri ihlali bildiriminde,

- Veri Sorumlusunun sunucularına 16.12.2020 tarihinde fidye saldırısının gerçekleştirildiği ve dosyaların şifrelendiği,
- İhlalin loglarda bir problem olduğunun fark edilmesiyle tespit edildiği,
- İhlalden etkilenen kişisel verilerin; ad, soyad, e-posta ve/veya telefon numarası olduğu ancak bilişim incelemesinin devam ettiği,
- İhlalden çalışanlar, müşteriler, tedarikçiler ve hizmet sağlayıcılar olmak üzere tahmini 1084 kişinin etkilendiği, incelemenin devam ettiği dolayısıyla kişi ve kayıt sayısının tam olarak bilinmediği ifade edilmiştir.

Söz konusu ihlal Kurum'un internet sitesinde 29.12.2020 tarihinde yayımlanmış ve incelemenin devam ettiği bildirilmiştir.

Ayrıca bildirilen bu veri ihlali, Türkiye'de gerçekleşmiş olup; şirketin sunucuları yurt dışında olduğu için Ficosa International Otomotiv San. ve Tic. A.Ş. bu ihlalden etkilenmiştir.

Polonya Veri Koruma Kurumu Karantinaya Alınan Kişilerin Listesinin Açıklanması ile İlgili Kınama Cezası Verdi

Polonya Kişisel Verileri Koruma Kurumu, bir atık yönetimi şirketinin karantinaya alınan kişilerin adresleri de dahil olmak üzere bazı kişisel verilerinin yetkisiz alıcılara ifşa edilmesi ile ilgili re'sen soruşturma başlatarak; söz konusu şirkete kınama cezası verdi.

UODO durumu netleştirmek için detaylı bir araştırma yürüttü. UODO, COVID-19 tehdidi nedeniyle karantinaya alınan kimselerin elektronik ve basılı ortamlarda kişisel verilerini işlerken ve bu yönde prosedürleri belirlerken gizlilikle ilgili risk analizlerinin yapılıp yapılmadığına ilişkin şirketten bilgi talep etti.

Şirket yaptığı açıklamada, söz konusu veri işleme faaliyetleriyle ilgili olası kayıp veya yetkisiz ifşa durumu veya diğer muhtemel sonuçlarına ilişkin analizlerin yapıldığını; ayrıca bu listelerin yalnız kişilere ait mülki adreslerini içerdiği ancak kişilerin adı, soyadı veya diğer belirlenebilir bilgilerini içermediğini belirtti.

Kurum yaptığı inceleme neticesinde ilgili mahallin adı, cadde adı, bina numarası, kişinin karantinada bulunduğu bilgisinin GDPR kapsamında kişisel veri oluşturacağı; ayrıca kişinin karantinada olduğu bilgisinin özel nitelikli kişisel veri niteliğini haiz olduğu değerlendirmesini yaptı.

UODO aynı zamanda, bahsi geçen listeyi incelemekle yükümlü çalışanın söz konusu listeyi açık bir şekilde masasında bırakarak başka bir çalışanın listenin fotoğrafını çekmesine sebep olmasından dolayı veri gizliliğinin ihlal edildiği sonucuna vardı.

UODO, risk analizindeki hükümler ile ilgili beyan ve belgelerin çalışanlar tarafından imzalanmasının tek başına yetersiz bir önlem olduğunu vurguladı. Ayrıca, risk analizi yapan şirketin hem işlenen verilerin özel niteliğini hem de işleyen kimselerin insan olmasından kaynaklanacak doğal faktörleri (dikkatsizlik, ihmal, özen eksikliği vb.) dikkate alması gerektiğini belirtti. Buna karşılık Kurum, tek seferlik ve üstünkörü bir analizin yeterli olmadığını belirtti.

Şirketin ihlal bildirimini 72 saat içerisinde yapmadığı, ayrıca veri işleme faaliyeti özel nitelikli kişisel verilere temas ettiğinden ihlalin yüksek risk meydana getirdiğini buna rağmen şirketin kişilere de ihlalle ilgili bildirimde bulunmadığı tespit edildi.

Tüm bu bulgular kapsamında GDPR hükümlerinin ihlal edildiğini belirten UODO, şirkete kınama cezası verdi ve ilgili kişilere veri ihlalinin bildirilmesi yönünde şirketi talimatlandırdı.

İsveç Veri Koruma Kurumu Hukuka Aykırı Video Gözetimi İçin Ceza Verdi

İsveç Veri Koruma Kurumu, LSS konutlarında yasadışı video gözetimi yapılması nedeniyle Gnosjö Belediyesi'ne 200.000 SEK tutarında idari para cezası uyguladı.

Kurum, Gnosjö Belediyesi'nde engeli olan kişilerin kaldığı bakım evinde ("LSS konutları") ikamet eden bir kişinin akrabasından, ikamet eden kişinin yasadışı olarak izlendiğini iddia eden bir şikâyet aldı.

Kurum, LSS konutlarında yürütülen faaliyete ilişkin denetim başlattı. Söz konusu sakinin GDPR ve İsveç Video İzleme Yasası'na aykırı olarak kendi yatak odasında izlendiğini tespit etti.

Gnosjö'deki LSS konutlarında barınma işlerinden sorumlu Sosyal Refah Komitesi, ilgili kişinin hastalığının hem kendisi hem personel açısından büyük zorluklar yarattığını, bu kişi ile çalışanların zarar gördüğü durumlar olduğunu, bu çerçevede izlemenin kimsenin zarar görmemesi adına yapıldığını ifade etti.

Kurum değerlendirmesinde Sosyal Refah Komitesi tarafından güdülen amacın, LSS konutlarında barınan kişilerin mahremiyetine daha az müdahale edici araçlarla yapılabileceğini belirtti.

Kurum kararında, video gözetimi için herhangi bir yasal dayanak bulunmadığı, veri sorumlusu tarafından video gözetimi başlatılmadan önce bir etki değerlendirmesi yapılmadığı ve video gözetimi hakkında ilgili kişilerin bilgilendirilmediği sonucuna vardı. Bu nedenlerden Kurum, Sosyal Refah Komitesi'ne 200.000 SEK idari para cezası verdi.

Belçika Veri Koruma Kurumu Video Görüntülerinin Hukuka Aykırı Olarak İşlenmesi Sebebiyle Para Cezası Verdi

Belçika Veri Koruma Kurumu, bir video gözetim sistemi aracılığıyla kişisel verileri hukuka aykırı olarak işleyen kimselere 1.500 EUR para cezası verdi. Aynı zamanda bu video gözetim sistemi kameralarının konumlandırılışının da veri güvenliğinin ihlali teşkil ettiğine karar verdi.

İki şikayetçi, komşularının video gözetim sistemi ve sistem içerisinde depolanan görüntülerin kullanımıyla ilgili Kurum'a şikâyette bulundu. Şikâyetçiler tarafından, video gözetim sisteminin kaldırılması talep edildi.

Şikâyetçi olunan kişiler özel mülklerine 7/24 kayıt yapan beş güvenlik kamerası kurarak bir video gözetim sistemi oluşturmuştu. Kameraların konumlandırılış şekli şikâyetçileri, evlerine girerken, araba kullanırken veya özel mülklerinin çevresinde herhangi bir eylemde bulunurken mutlak suretle kayıt altına alacak şekilde konumlandırılmıştı. Görüntüler, şikâyet olunanlar ve şikâyetçiler arasında çıkan bir çevresel planlama anlaşmazlığında şikâyet olunan kişiler tarafından kullanıldı.

Kurum verdiği kararda görüntülerin GDPR kapsamında yasal bir şekilde işlenmediğini ve meşru menfaat kapsamında olmadığını tespit etti. Zira güdülen amaç özel mülkün korunması olsa da kamuya açık alanların görüntülenmesinin meşru menfaat sınırını aştığı ve ilgili kişilerin hak ve özgürlüklerini zedelediği sonucuna vardı.

Ayrıca, veriler hukuka aykırı elde edildiğinden sonradan ortaya çıkan anlaşmazlığın çözümü için görüntülerin kullanılması amacıyla veri işleme faaliyetinin de aykırı olduğuna karar verdi.

Kurum, sayılan nedenlerden dolayı ilgili kişilere 1.500 EUR para cezası ve kınama cezası verdi.

İsviçre Veri Koruma Kurumu Sağlık Hizmeti Sağlayıcılarının Personeli Tarafından Hasta Verilerine Erişimde Var Olan Eksikleri Açıkladı

İsveç Veri Koruma Kurumu, elektronik ortamda tutulan sağlık kayıtları için personelin erişim yetkilerinin yönetimi ve kısıtlaması hususunda sekiz adet sağlık hizmeti sağlayıcısını denetledi.

Kurum öncelikle elektronik sağlık kayıtlarında yer alan kişisel verilere erişim yetkisinin gerekli ihtiyaç ve risk analizi doğrultusunda yetkili kişilere tanınıp tanınmadığını araştırdı.

Sağlık hizmeti sağlayıcıları, sağlık kayıtlarındaki bilgilere erişmek için personelin ihtiyaç duyduğu ve erişimin içerdiği risklerin detaylı bir analizini ve değerlendirmesini yapmalıydı. Ancak Kurum, sağlık hizmeti sağlayıcılarından yedi tanesinin herhangi bir risk değerlendirmesi yapmadığını, yalnızca birinin eksiklikler içeren bir analiz formu çıkardığını belirtti.

Kurum sağlık hizmeti sağlayıcılarının yedi tanesinin, kullanıcıların hasta bilgilerine erişimini gerekli olanla sınırlı tutmadığı sonucuna vardı. Bunun da sağlayıcıların, elektronik kayıt sistemlerindeki kişisel veriler için yeterli düzeyde önlem almadığının göstergesi olduğunu belirtti. Bu nedenler ile Kurum, sekiz sağlayıcının yedisine 30 milyon SEK'e varan idari para cezası verdi.

Ayrıca Kurum ihtiyaçlar ve risk analizi yapma zorunluluğu ile ilgili olarak mevcut denetimlerinden çıkan sonuçları özetleyen bir kılavuz hazırladı.

Kurum kılavuz çerçevesinde, sağlık hizmeti sağlayıcılarının ihtiyaç ve risk analizlerini yapmasının önemine işaret etti. Kurum kılavuzun amacının, sağlık kayıt sisteminde erişim yetkisi verilmeden önce yapılması gereken analizler hakkında hizmet sağlayıcılara yardımcı olmak olduğunu açıkladı. Bu çerçevede amacın, ülkedeki tüm sağlık hizmeti sağlayıcıları tarafından yapılan yetkilendirmenin doğru bir şekilde yapılmasını sağlamak ve hastaların hakkı olan gizlilik korumasını garanti altına almak olduğunu belirtti.

Estonya Veri Koruma Müfettişliği, E-eczanelerde 3. Kişilerin Reçete Bilgilerine Olan Erişimini Derhal Sonlandırmasına Karar Verdi

Estonya Veri Koruma Müfettişliği, üç eczane zincirine e-eczane ortamında başka bir kişinin reçetesini, kişinin rızası olmadan görüntüledikleri için 100.000 EUR para cezası uyguladı.

Müfettişlik, "Kimlik numaraları kullanılarak, e-eczane ortamında bireylerin reçetelerinin görüntülenmesinin herhangi bir yasal dayanağı bulunmadığı için acilen durdurulması gerektiğine karar verdik." açıklamasında bulundu.

Müfettişlik bir başkası için ilaç satın almanın hayatın olağan koşulları içerisinde mümkün olabileceği, ancak böyle durumlarda eczacının ilgili kişinin rızasının olduğundan emin olması gerektiğini vurguladı.

Müfettişlik e-eczane portalını incelediğinde, erişim gerçekleştiren kullanıcıların sohbet penceresini kullanarak diğer kişilerin reçete bilgilerine hızlıca erişebildiğini fark etti. Siteye giriş aşamasında kullanıcıların, kendi reçete bilgilerini mi bir başkasının reçete bilgilerini mi görmek istediğini seçtiği ve başka bir kişinin kimlik numarasını girdiğinde bilgilerin erişilebilir olduğunu tespit etti. Bu faaliyetin GDPR'a uygun olmadığına karar verdi.

Estonya Veri Koruma Müfettişliği, Apotheka, Südameapteek ve Azeta.ee e-eczanelerini kapsayan bir uyarı yayınladı.

İrlanda Veri Koruma Kurumu, Twitter Soruşturmasındaki Kararını Açıkladı

İrlanda Veri Koruma Kurumu ("DPC"), Twitter International Company'e karşı yürüttüğü soruşturmanın sonucunu açıkladı.

DPC, Twitter'ın ihlali gereken zamanda bildirmemesi ve belgelememesi sebebiyle GDPR m. 33 (1) ve 33 (5)'e aykırı hareket ettiğini belirtti. DPC Twitter'a, etkili, orantılı ve caydırıcı olduğunu açıkladığı 450.000 EUR tutarında idari para cezası uyguladı.

Soruşturma çerçevesindeki taslak karar, Mayıs 2020'de GDPR'ın 60. maddesi uyarınca diğer İlgili Denetleme Makamlarına sunulmuş olup, GDPR yürürlüğe girdiğinden bu yana 65. maddenin ("Anlaşmazlıkların Çözümü") uygulandığı ve tüm AB Denetim Makamları ile iş birliği içerisinde yürütülen ilk "büyük teknoloji" vakası oldu.

Avrupa Veri Koruma Kurulu 65. madde kararını resmî sitesinde yayımladı.

İsveç Veri Koruma Kurumu Bir Konut Şirketine 300.000 SEK Para Cezası Uyguladı

İsveç Veri Koruma Kurumu, bir apartmanda yapılan yasadışı video gözetimi nedeniyle Uppsalahem adlı konut şirketine 300.000 SEK idari para cezası uyguladı.

Kurum, konut şirketi Uppsalahem'e ait bir apartmanda video gözetimi yapıldığına ilişkin bir şikâyet aldı. Şikayetçi, apartmanda müştekinin ön kapısına doğru konumlandırılmış bir güvenlik kamerası olduğunu iddia etmekteydi.

Kurum, konut şirketinin şikayetçinin yaşadığı katı izleyen bir gözetleme kamerası kurduğunu tespit etti. Kameranın izleme alanı biri şikayetçiye, diğeri de rahatsızlık ve tacize maruz kaldığını iddia eden bir diğer konut sakinine ait iki apartman kapısını açıkça kapsamaktaydı.

Konut şirketi ise, video gözetiminin amacının merdiven boşluğunda zaman içinde meydana gelebilecek rahatsızlıkları önlemek olduğunu belirtti.

Kurum verdiği kararda, söz konusu video gözetiminin, kişilerin ev ortamında izlenmesi hususunun mahremiyeti ihlal ettiğini bildirdi. Bu nedenle Kurum konut şirketine 300.000 SEK para cezası uyguladı. Konut şirketi karardan sonra söz konusu video gözetimini durdurduğunu açıkladı.

BİLGİLENDİRME REHBERİ

Mobil Cihazlar Şirketler Tarafından Kişisel Verilerin Korunması Kapsamında Nasıl Değerlendirilmelidir?

Bilindiği üzere, şirket cihazlarında yer alan verilerin, kişisel verilerin korunması ve bilgi güvenliği kapsamında gerekli idari ve teknik önlemlerin alınarak korunması veri sorumlusu şirketin yükümlülüklerindendir. Bu konuya KVKK kapsamında, teknik tedbirler arasında yer verilerek "Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması" başlığı ile Kurum tarafından açıklansa da konuyu yalnızca teknik açıdan değil, idari açıdan da incelemek gerekmektedir.

Öncelikle açıklamak gerekir ki, kişisel veri içeren ortamların güvenliğinin sağlanması, şirketlerin yalnızca şirket bilgisayarlarını veya serverlarını korumaları anlamına gelmemektedir. Bu kapsamda mobil cihazlar genellikle gözden kaçırılan ve uygulamada çokça ihlal doğuran önemli bir unsurdur.

İhlal doğurabilecek hususlar, teknik ve idari olarak ayrılarak aşağıdaki şekilde incelenmiştir:

<u>İdari Tedbir Eksikliğinden Kaynaklanan İhlaller:</u>

Çalışanın Şahsi Mobil Cihazını Şirket İşleri İçin Kullanması

Genellikle karşılaşılan tedbirsizliklerin başında çalışana şirket tarafından mobil cihaz sağlanmaması sebebiyle, çalışanın şahsi mobil cihazını işleri için kullanması gelmektedir. Şahsi mobil cihazın kullanılması, çalışan ve veri sorumlusu şirketin iş ilişkisinin sona ermesi durumunda, çalışanın bu verilere erişmeye devam etmesi tehlikesini doğuracaktır. Her ne kadar çalışanın e-postalara veya şirket dokümanlarına erişmesi mobil cihaz yönetim sistemleriyle ve şirket hesaplarının kapatılmasıyla engellenebilse de çalışanın müşteri, tedarikçi veya şirketin ilişkili olduğu kişilerin iletişim bilgilerinin bu mobil cihazda kalması yahut iş ilişkisinin sona ermesinden sonra bu ilgili kişilerin çalışana ulaşması engellenemeyecektir.

Böyle bir durumda çalışanlardan, işten ayrılması veya görevinde değişiklik olması hâlinde iş amacıyla kullanılan şahsi cihazlarda şirkete ait veri bulundurulmamasına ve ilgili verilerin farklı amaçlar ile kullanılmamasına ilişkin bir taahhüt alınması riski, minimum seviyeye indirecek idari tedbirlerden biri olacaktır.

Bununla birlikte, şirket nezdinde ihlal doğuracak diğer bir tehlike, mobil cihazlar için takip sistemlerinin kullanılması ve bu sistemlerin çalışanın şahsi cihazına kurulması durumunda, çalışanın kişisel verilerinin şirket nezdinde tutulması olacaktır. Bunun da ölçüsüz bir veri işleme faaliyeti olduğu aşikardır.

Yukarıda açıklanan sebeplerle, çalışana, şirketin işlerini yürütmek üzere ayrı bir mobil cihaz ve telefon hattı sağlanması veya katı bir politika ile şirketin sabit hatlarının ilgili kişiler ile iletişime geçmede kullanılmasının çalışana bildirilmesi yerinde uygulamalar olacaktır.

Çalışanın Şirkete Ait Mobil Cihazı, Şahsi İşleri İçin Kullanması

Çalışanın, şirket mobil cihazını şahsi işleri için kullanması, şirket cihazına kendi kişisel verilerini yüklemesi, şirket nezdinde tutulmaması gereken verilerden sorumlu olması ve amaçla bağdaşmayan verileri nezdinde tutması sonucunu doğuracaktır. Örneğin, çalışanın şahsi olarak üçüncü kişilerin iletişim bilgilerini cihazın rehberine eklemesi, bu cihaz ile görsel ve işitsel kayıtlar alması bu amaçla bağdaşmayan faaliyetlerden olacaktır.

Bununla birlikte, çalışanın, diğer cihazlarda olduğu gibi, şirketin kontrolünde olmayan WhatsApp, Zoom gibi güvenlik açığı tespit edilmiş uygulamaları cihaza yüklemesi de ayrıca ihlal sebebi olacaktır.

Bu sebeple, çalışanın şirket cihazını veya şirket telefon hattını şahsi işleri için kullanmamasını temin etmek üzere, yukarıdaki tüm hususları düzenleyen katı bir politika hazırlanarak çalışanlara bunun duyurulması ve çalışanların cihaz kullanımı konusunda farkındalığının sağlanması yerinde bir uygulama olacaktır. Ayrıca bu durumda, çalışanın aydınlatılması sağlanarak güvenli mobil cihaz yönetim sistemlerinin kullanılması ölçülü bir veri işleme faaliyeti olacak ve mobil cihazlar üzerinden yaşanabilecek ihlallerin önüne geçecektir.

Mobil Cihaz Güvenliğinin Sağlanması

Cihazların kurulumu kadar yönetilmesi de oldukça önemlidir. Kullanılan cihazlarda hangi özellikler açık ya da cihazların dışardan erişim için açığı var mı gibi bilgilerin bilinmesi ve yönetilmesi gerekmektedir. Güvenli Mobil Cihaz Yönetimi için aşağıdaki teknik hususlara dikkat edilmelidir.

1. Varlık yönetimi gerçekleştirilmeli, cihazlara ilişkin çeşit, işletim sistemi sürüm bilgileri takip edilmelidir.

2. Mobil cihazlarda güncel anti-virüs uygulamaları kullanılmalı ve bu uygulamanın devre dışı bırakılması engellenmelidir.

3. Çalışanların mobil cihazlara şirket tarafından onaylanmayan uygulamaları yüklemeleri ve kullanmaları engellenmeli ve uygulamalar için uzaktan sürüm güncelleme ve yama güvenliği tedbirleri alınmalıdır.

4. Herhangi bir saldırı veya veri ihlali hâlinde cihaz içerisinde bulunan verilerin tespit edilebilmesi ve veri kaybı yaşanmaması için cihaz yedekleme politikaları belirlenmeli ve yedeklerin güvenliği sağlanmalıdır.

5. Mobil cihazların bakım, onarım vb. işlemler için yetkisiz kişilere teslim edilmesi hâlinde veriler ulaşılamaz durumda olmalı, bakım sırasında cihaza herhangi bir kötü amaçlı yazılımın kurulmadığından emin olunmalıdır.

Mobil Cihaz Yönetim (MDM) Çözümlerinin kullanılması veri güvenliğinin sağlanması hususunda şirketlere büyük fayda sağlamakla birlikte yukarıda sayılan tedbirlere ek koruma yöntemleri kurgulanmasını da sağlamaktadır.

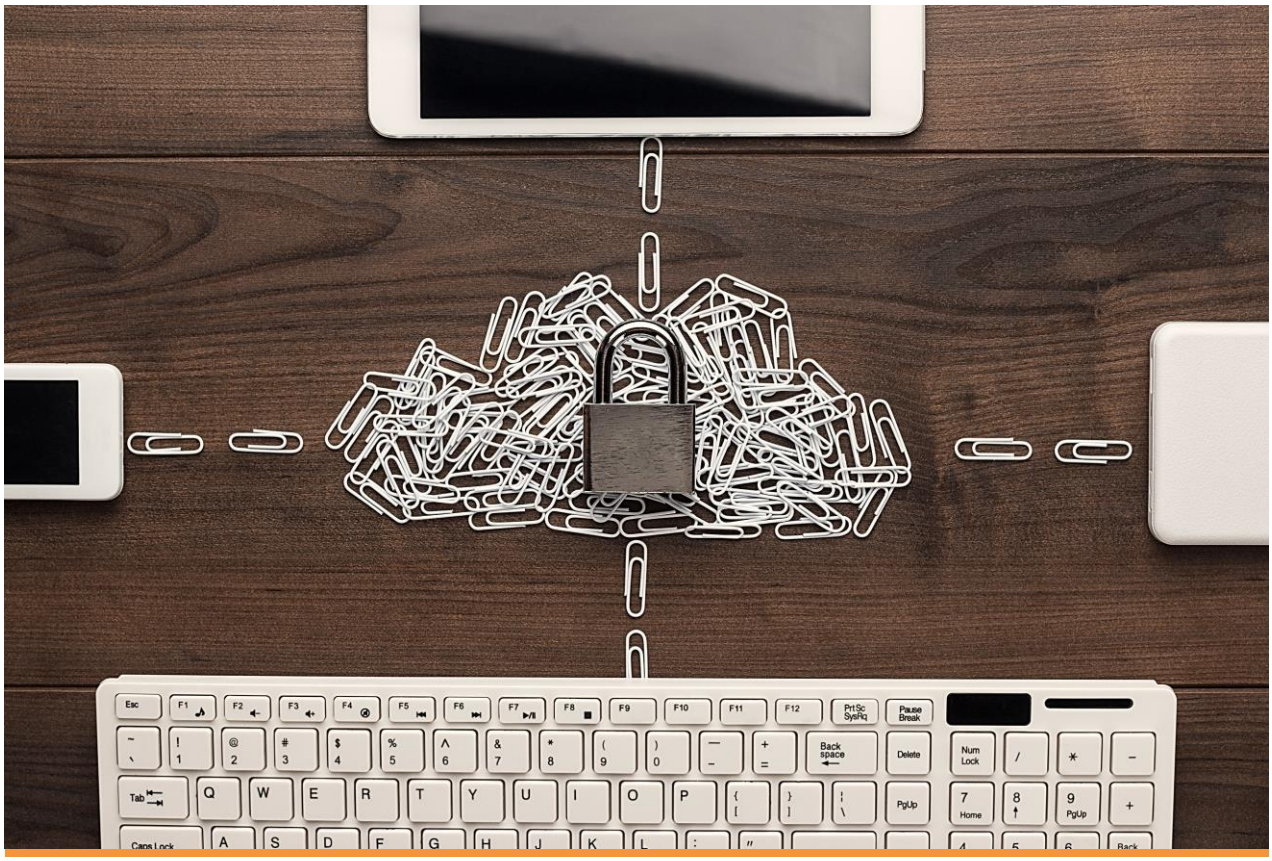
MDM Çözümleri ile şirket verileri, yazışmaları, e-postaları, hassas dokümanlar korunabilir ve paylaşımı sınırlandırılabilir. Cihazlardaki parola yönetimini sağlamak, veri kopyalamayı ve ekran görüntüsü almayı engellemek Mobil Cihaz Yönetim Sistemleri ile mümkündür.

Ayrıca mobil cihazların kaybolması veya çalınması hâlinde; cihazlar uzaktan kilitlenerek içerisinde bulunan verilerin güvenliği de sağlanabilir ve hatta SIM kartların başka bir cihaza takılması hâlinde erişimi engellenebilir.

Yukarıda mobil cihazlara ilişkin açıklanan tüm ihlal tehlikeleri, alınması gereken idari ve teknik tedbirler, şirketin kontrolünde olan bilgisayar, tablet ve benzeri akıllı iletişim araçları için geçerlidir. Burada dikkat edilmesi gereken husus, kişisel veri içeren ortamların güvenliğinin sağlanması konusunda geniş düşünmek ve risk analizini doğru şekilde yapmaktır.

Kübra Özkahraman | Kalite Güvence ve Eğitim Sorumlusu

Şeyma Kaplan | Hukuk Danışmanı | Avukat



Hazırlayanlar

Ece Melis Erkoçak

Hazal Özçelik

Kerem Akdağ

Kübra Özkahraman

Livanur Sever

Onur İzli

Rabia Dağcı

Şeyma Kaplan

Şule Özcan

Bizi Sosyal Medyadan Takip Edebilirsiniz...