MOROĞLU ARSEVEN

KVKK KURUL KARARLARI

Karar Özetleri Bülteni

10 Ağustos 2026

47 karar özeti **39** sektör **27** idari para cezası

Kişisel Verileri Koruma Kurulu tarafından yayımlanan karar özetlerinin derlemesidir.
Bilgilendirme amaçlı olup hukuki mütalaa niteliği taşımaz.

Abdi İpekçi Caddesi 19 -1, Nişantaşı, 34367 İstanbul
T: + 90 212 377 47 00 **F:** + 90 212 377 47 99
www.morogluarseven.com

İçindekiler

#	SEKTÖR	KARAR BAŞLIĞI / İHLAL KONUSU	YAPTIRIM
13	Telekomünikasyon / Teknoloji	Telekomünikasyon teknolojileri geliştirme alanında faaliyet gösteren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme	—
14	Sivil Toplum / Bilimsel Araştırma	Bilimin ilerlemesini destekleyen kâr amacı gütmeyen bir kuruluş olarak faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	—
15	Otelcilik / Konaklama	Otelcilik ve konaklama yönetimi alanında faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	—
16	Tüketici Ürünleri / Küçük Ev Aletleri	Küçük ev aletleri üretimi ve satışı yapan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	—
17	Gıda / Restoran	Restoran zinciri ve hızlı servis gıda şirketi olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**1.000.000 TL**
18	Üretim / Plastik ve Temizlik Ürünleri	Plastik ev gereçleri ve temizlik ürünleri üretimi yapan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**250.000 TL**
19	Kurumsal Hizmetler	Avrupa'da bulunan grup şirketlerine kurumsal destek hizmetleri sağlayan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**700.000 TL**
20	İlaç / Sağlık Ürünleri	İlaç ve sağlık ürünleri alanında faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**350.000 TL**
21	Kozmetik / Kişisel Bakım	Konu Özeti Kozmetik ve kişisel bakım şirketi olan veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme	**500.000 TL**
22	Turizm / Otelcilik	Turizm, otelcilik ve konaklama işletmeciliği yapan veri sorumlusu tarafından Kuruma intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**500.000 TL**
23	Dijital Oyun / Eğlence	Dijital oyun ve eğlence platformları sunan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**1.500.000 TL**
24	Yazılım / Teknoloji	Yazılım ve teknoloji odaklı girişim yatırımları ve geliştirme faaliyetleri yürüten veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**350.000 TL**
25	Medya / Basın	Yerel bir basın organının seçim anketi sonuçlarına ilişkin verileri internet sitesinde paylaşmasına ilişkin ihbar	**40.179 TL**
26	Perakende / Hazır Giyim	Hazır giyim ve tekstil ürünlerinin perakende satışı gerçekleştiren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme	—

#	SEKTÖR	KARAR BAŞLIĞI / İHLAL KONUSU	YAPTIRIM
27	Eğitim	Bir Üniversite tarafından parmak izi verilerinin işlenmesi suretiyle devamsızlık takibi uygulamasına ilişkin şikayet üzerine ve resen yürütülen inceleme	—
28	Medya / Basın	İlgili kişiler hakkında bir gazetede yayımlanan ve halen söz konusu gazetenin arşiv kayıtlarında yer alan bir habere ilişkin şikâyet	—
29	Finans / Muhasebe	Finans ve muhasebe alanında faaliyet gösteren uluslararası bir meslek kuruluşu olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**1.000.000 TL**
30	Otomotiv	Otomotiv sektöründe faaliyet gösteren bir yan sanayi üretim firması olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**430.000 TL**
31	Tarım Makineleri / Üretim	Tarım makineleri, traktör ve tarımsal ekipman üretimi ile ticareti alanında faaliyet gösteren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme	**150.000 TL**
32	Online Yemek / Teslimat	Online yemek siparişi, restoran entegrasyonu ve teslimat/kurye hizmetleri veren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme	**250.000 TL**
33	Endüstriyel Üretim / Mutfak Ekipmanları	Endüstriyel mutfak ekipmanları üretimi yapan veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme	—
34	Bilişim / Hosting Hizmetleri	Bir hosting firması tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**350.000 TL**
35	Moda / Tekstil	Moda tekstil faaliyeti yürüten Veri Sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme	—
36	Üretim / Sanayi	Bir sanayi şirketi olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**1.000.000 TL**
37	Teknoloji	Bir Teknoloji Şirketi olan veri sorumlusu tarafından Kurula iletilen veri ihlal bildirimine istinaden yürütülen inceleme	—
38	Tarım / Emtia Ticareti	Tarımsal emtia ticareti alanında faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**200.000 TL**
39	Otomotiv / Elektronik Sistemler	Otomotiv güvenlik ve elektronik sistemleri üretimi yapan veri sorumlusu tarafından Kurula intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	**500.000 TL**
40	Perakende / Mağazacılık	Mağazacılık hizmeti veren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme	—
41	İşveren / Özel Sektör	İşveren tarafından işyerinde kamera vasıtasıyla görüntü ve ses kaydı alınması	**125.000 TL**

#	SEKTÖR	KARAR BAŞLIĞI / İHLAL KONUSU	YAPTIRIM
42	Belediye / Kütüphane Hizmetleri	Bir Belediyenin kütüphane üyelik uygulamasına ilişkin şikâyet	—
43	Güvenlik Hizmetleri / Alarm Sistemleri	Alarm ve görüntüleme sistemi hizmeti sunan veri sorumlusu tarafından ilgili kişinin telefon görüşmelerinin kaydedilmesi	**15.000 TL**
44	Perakende / Hazır Giyim	İlgili Kişinin kişisel verilerinin veri sorumlusu giyim mağazasına ait internet sitesinde üçüncü kişilerin erişimine açılması	**200.000 TL**
45	Sağlık Hizmetleri	İlgili kişinin Covid-19 test sonucunun tarafından veri kayıt sisteminde bulunan eski cep telefonu numarasına gönderilmesine ilişkin şikâyet	**30.000 TL**
46	Çevrimiçi Spor ve Şans Oyunları	Bir çevrimiçi yasal spor ve şans oyunları platformu tarafından canlı maç yayını faaliyeti sunumunun ticari nitelikli ileti göndermek suretiyle açık rıza alınması şartına bağlanması	**250.000 TL**
47	Kamu / Ceza İnfaz	İlgili kişinin erişim hakkı talebinin reddedilmesine ilişkin şikâyeti	—

KARAR 01

FINANS

Bir tasarruf finansman şirketi tarafından reklam ve pazarlama amaçlı izinsiz SMS gönderilmesi ve arama yapılması suretiyle işlenen kişisel verilere ilişkin şikâyet hakkında

Karar No **2026/1183** Tarih **10.06.2026**

YAPTIRIM

1.000.000 TL idari para cezası

KARARIN ÖZETİ

Marka elçiliği programı kapsamında, müşteriler tarafından üçüncü kişilere ait telefon numaralarının veri sorumlusuna iletilmesi ve bu kişilere SMS ve telefon araması yoluyla reklam ve pazarlama yapılması incelenmiştir. Program kapsamında, üçüncü kişilere ait iletişim bilgilerini veri sorumlusuna aktaran müşterilere prim ödemesi yapıldığı belirtilmiştir. Veri sorumlusu; marka elçisi olan müşterilerinin, tasarruf finansman sistemi hakkında bilgi almak isteyen tanıdıklarının telefon numarasını uygulama üzerinden tavsiye niteliğinde eklediğini, bu tavsiye üzerine çağrı merkezi tarafından ilgili kişinin arandığını ve ilgili kişinin görüşme sırasında şirket ve tasarruf finansman sistemi hakkında bilgi almaya devam etmesini açık rıza olarak değerlendirmiş, ayrıca SMS'lerde ileti gönderimini sonlandırmaya imkân sağlayan bir iptal seçeneği bulunduğunu savunmuştur.

Kurul; ilgili kişinin telefon numarasının doğrudan kendisinden değil, üçüncü bir kişi aracılığıyla elde edildiğini ve söz konusu verinin ilgili kişiyle iletişim kurulması amacıyla kullanılacak olması nedeniyle, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ madde 6 uyarınca en geç ilk iletişim sırasında aydınlatma yükümlülüğünün yerine getirilmesi gerektiğini değerlendirmiştir. Buna karşılık, ilk görüşmede usulüne uygun bir aydınlatma yapılmadığı veya ilgili kişinin bir aydınlatma kanalına yönlendirilmediği; aksine kampanya tanıtımında ısrarcı olunarak tanıtım üzerinden konuşmaya devam edildiği ve görüşmenin kayda alındığı hususunda da aydınlatmada bulunulmadığı tespit edilmiştir. Kurul, KVKK madde 3 kapsamında açık rızanın bir irade beyanı olduğunu ve açık rızaya dayalı veri işleme hâlinde kişisel veri işlemeye başlamadan önce aydınlatma yükümlülüğünün de yerine getirilmesi gerektiğini belirtmiştir. Bu çerçevede, ilgili kişinin konuşmaya devam etmesi ve kampanya tanıtımına ilgi göstermesi suretiyle ortaya çıkan zımni rızanın, KVKK anlamında "belirli bir konuya ilişkin olma", "bilgilendirmeye dayanma" ve "özgür iradeyle açıklanma" unsurlarını taşıyan geçerli bir açık rıza olarak kabul edilemeyeceği sonucuna ulaşmıştır.

Bu kapsamda Kurul, yalnızca ilgili kişi bakımından değil, marka elçiliği programı kapsamında kişisel verileri aynı yöntemle işlenen diğer kişiler bakımından da geçerli bir veri işleme şartı bulunmadığını değerlendirmiştir. Bu nedenle KVKK madde 5'e uygun bir açık rıza veya başka bir işleme şartı bulunmaksızın gerçekleştirilen veri işleme faaliyetlerinin KVKK madde 12/1'deki kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğüne aykırı olduğu sonucuna varılarak veri sorumlusu hakkında KVKK madde 18/1-(b) uyarınca 1.000.000 TL idari para cezası uygulanmıştır. Veri işleme faaliyetinin herhangi bir hukuki sebebe dayanmadığının tespit edilmiş olması nedeniyle aydınlatma yükümlülüğü yönünden ayrıca bir işlem tesis edilmesine gerek görülmemiş; ilgili kişinin veri sorumlusuna yaptığı başvurunun cevaplandırıldığı tespit edildiğinden bu iddia bakımından da ayrıca işlem yapılmamıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 02

KAMU / CEZA İNFAZ

İlgili kişinin erişim hakkı talebinin reddedilmesine ilişkin şikâyeti

Karar No **2024/2158** Tarih **19.12.2024**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Kapalı ceza infaz kurumunda bulunan ilgili kişi; iş yurdu müdürlüğü tarafından düzenlenen fişlerde ad ve soyadının buzlandığını, ancak tahsilat ve reddiyat makbuzlarında ad-soyad, T.C. kimlik numarası, cezaevi kayıt numarası, cezaevindeki durumu, cezaevine giriş tarihi ve kaldığı blok/oda numarası gibi kendisine ait bilgilerin yanı sıra, adına para yatıran üçüncü kişilerin ad-soyad, T.C. kimlik numarası ve yakınlık durumuna ilişkin kişisel verilerinin herhangi bir maskeleme yapılmaksızın yer aldığını belirtmiştir. Bu belgelerin kendisine ulaştırılması sürecinde belirli bir memurun görevli olmaması nedeniyle söz konusu verilerin birden fazla memur ve idareci tarafından görülebildiğini ileri sürmüş; veri sorumlusuna yaptığı başvuruya talebinin değerlendirileceği yönünde yanıt verilmesine rağmen uygulamada herhangi bir değişiklik yapılmadığını ifade etmiştir.

Ceza infaz kurumu ise makbuzlardaki hükümlü ve tutuklu bilgilerinin UYAP kayıtlarından otomatik olarak aktarıldığını, tahsilat ve reddiyat makbuzlarının yalnızca ilgili birimde görev yapan personel tarafından görüldüğünü ve ilgili kişiye teslim edildiğini belirtmiştir. Söz konusu kişisel verilerin, 5275 sayılı Kanun madde 121 uyarınca hazırlanan Ceza İnfaz Kurumlarının Yönetimi ile Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Yönetmelik madde 60 ve 61, Hükümlü ve Tutukluların Emanete Alınan Kişisel Paralarının Kullanımına Dair Yönetmelik madde 5, 6 ve 8 ile Ceza İnfaz Kurumlarında Kullanılacak Defter ve Belgeler ile Bunların Düzenlenmesine Dair Yönerge madde 62 ve 63'de yer alan esaslara göre işlendiği açıklanmıştır.

Kurulca başlatılan resen inceleme çerçevesinde; ilgili kişiye ait kişisel verileri içeren tahsilat ve reddiyat makbuzlarının düzenlenmesi ve ilgili kişiye ulaştırılması süreçlerinde gerçekleştirilen kişisel veri işleme faaliyetlerinin infaz işlemleri kapsamında ve bir infaz mercii tarafından gerçekleştirildiği değerlendirilmiştir. Bu nedenle söz konusu veri işleme faaliyetlerinin KVKK madde 28/1-(d)'de düzenlenen, kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesine yönelik istisna kapsamında bulunduğu ve KVKK hükümlerinin uygulanmayacağı sonucuna ulaşılmıştır. Bu çerçevede şikâyet konusu veri işleme faaliyetleri bakımından yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 03

ELEKTRONIK HABERLEŞME

Uçak Yolculuğu esnasında sunulan internet hizmetinin veri sorumlusu olduğu tespit edilen internet servis sağlayıcı tarafından açık rıza şartına bağlanmasına ilişkin şikâyet

Karar No **2024/1393** Tarih **15.08.2024**

YAPTIRIM

90.000 TL idari para cezası

KARARIN ÖZETİ

İlgili kişi, uçuş sırasında sunulan internet hizmetinden yararlanabilmek için kişisel verilerinin işlenmesine ve paylaşılmasına ilişkin onay vermek zorunda bırakıldığını ileri sürmüştür. İnternet servis sağlayıcısına ait portalda, "Havayolu şirketine bildirmiş olduğum bilgilerimin, internet kullanıcı bilgilerimin doğrulanması amacıyla ilgili makamlar ve Şirket ile paylaşılmasını kabul ediyorum." şeklinde bir onay kutucuğunun yer aldığı ve bu kutucuk onaylanmadan hizmetten yararlanılamadığı tespit edilmiştir. Kurul, internet hizmetinin sunulması sürecinde havayolu şirketi ile internet servis sağlayıcısının iki ayrı veri sorumlusu olduğunu; havayolu şirketinin internet hizmeti sunumunda doğrudan yetkisinin bulunmadığını, hizmet sözleşmesinin ilgili kişi ile internet servis sağlayıcı arasında kurulduğunu ve havayolu şirketinin yalnızca 5651 sayılı Kanun kapsamında kullanıcı doğrulaması amacıyla ilgili kişinin soyadı ve koltuk/bilet numarası bilgilerini sistem üzerinden internet servis sağlayıcıya bildirdiğini değerlendirmiştir.

Kurul, söz konusu bilgilerin internet hizmetinin sunulabilmesi için işlenmesinin KVKK madde 5/2-(c), (ç) ve (e) kapsamındaki veri işleme şartlarına dayanabildiğini ve bu nedenle ayrıca açık rıza alınmasına ihtiyaç bulunmadığını tespit etmiştir. Buna rağmen internet servis sağlayıcısına ait portalda ilgili kişiden kişisel verilerinin paylaşılmasına ilişkin ayrıca açık rıza talep edilmesini, veri işlemenin hukuki dayanağı konusunda ilgili kişiyi yanıltıcı ve yanlış yönlendirici nitelikte bulmuş; bu uygulamanın KVKK madde 4/2-(a)'da düzenlenen hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırı olduğu sonucuna ulaşmıştır. İnceleme sürecinde internet servis sağlayıcının Kurum'a sunduğu güncel ekran görüntüsünde şikâyete konu onay kutucuğunun kaldırılmış olduğu tespit edilmiştir.

Bu nedenle veri sorumlusu internet servis sağlayıcı hakkında KVKK madde 12/1'deki kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğüne aykırı olduğu sonucuna varılarak veri sorumlusu hakkında KVKK madde 18/1-(b) uyarınca 90.000 TL idari para cezası uygulanmıştır. Ayrıca aydınlatma yükümlülüğünün yerine getirilmediğine ilişkin iddia, ilgili kişinin daha önce veri sorumlusuna yaptığı başvuruda ileri sürülmediğinden inceleme kapsamına alınmamış; yurt dışına veri aktarımına ilişkin talep bakımından ise havayolu şirketinin gerekli ve yeterli açıklamayı yaptığı değerlendirilerek ayrıca işlem tesis edilmemiştir

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 04

EĞITIM

Veri sorumlusu tarafından güvenlik kamerasıyla ses ve görüntü kaydı alınması, aydınlatma yükümlülüğünün yerine getirilmemesi, internet sitesinde çerezler vasıtasıyla kişisel verilerin işlenmesi ve hizmetin ön şartı olarak reklam ve pazarlama amaçlı açık rıza alınmasına ilişkin şikâyet

Karar No **2024/1361** Tarih **08.08.2024**

YAPTIRIM

Toplam 265.000 TL idari para cezası 250.000 TL: Açık rıza gerektiren çerezler ve reklam/pazarlama amaçlı veri işleme süreçleri bakımından gerekli tedbirlerin alınmaması 15.000 TL: Aydınlatma yükümlülüğünün gereği gibi yerine getirilmemesi

KARARIN ÖZETİ

Özel öğretim kurumunda deneme dersine katılan ilgili kişi; kurumda güvenlik kameraları aracılığıyla ses ve görüntü kaydı yapıldığını, sabit hat üzerinden gerçekleştirilen telefon görüşmelerinin kaydedildiğini, bu veri işleme faaliyetleri hakkında usulüne uygun şekilde aydınlatılmadığını, internet sitesinde gizlilik politikası, aydınlatma metni, başvuru formu gibi herhangi bir metnin ve çerez yönetim panelinin bulunmadığını ve iletişim formunda kişisel verilerin reklam, promosyon ve kampanya amacıyla kullanılmasına ilişkin rızanın zorunlu tutulduğunu ileri sürmüştür.

Kurul; güvenlik kameraları aracılığıyla ses kaydı alındığının tevsik edilemediğini, görüntü kaydının ise Millî Eğitim Bakanlığı Özel Öğretim Kurumları Yönetmeliği madde 11/4'ten kaynaklanan yükümlülük kapsamında KVKK madde 5/2-(ç) uyarınca hukuka uygun olduğunu değerlendirmiştir. Kamera ve telefon görüşmelerine ilişkin ön bilgilendirmelerin katmanlı aydınlatma niteliğinde olmakla birlikte, KVKK madde 10'da öngörülen asgari unsurları içeren bir aydınlatmaya yönlendirme yapılmadığı; internet sitesinde yer alan "Yasal Uyarı" bilgilendirmesinin ise açık rıza beyanı niteliğinde olduğu ve KVKK madde 10'daki asgari unsurların yer aldığı bir aydınlatmanın mevcut olmadığı tespit edilerek aydınlatma yükümlülüğünün yerine getirilmediği sonucuna ulaşılmıştır.

İnternet sitesinde zorunlu çerezlerin yanı sıra kalıcı bir analitik çerez kullanıldığı, ancak siteye ilk girişte bu çerez bakımından açık rıza alınmasını sağlayacak bir mekanizmanın bulunmadığı belirlenmiştir. Kurul, kesinlikle gerekli olmayan çerezler bakımından başka bir veri işleme şartı bulunmadığı takdirde, kişisel veriler işlenmeye başlamadan önce kullanıcının aktif hareketiyle rıza vermesine imkân sağlayan "opt-in" mekanizmasının bulunması gerektiğini; somut olayda analitik çerez aracılığıyla gerçekleştirilen veri işleme faaliyetinin KVKK madde 5'teki herhangi bir işleme şartına dayanmadığını değerlendirmiştir. Ayrıca iletişim formunda, kurumdan bilgi almak isteyen kişiye ulaşılmasına ilişkin rıza ile kişisel verilerin reklam, promosyon ve kampanya amaçlarıyla kullanılmasına ilişkin rızanın tek bir seçenek altında birleştirildiği tespit edilmiştir. Kurul, farklı amaçlara yönelik veri işleme faaliyetlerinin tek bir açık rıza altında birleştirilmesinin açık rızanın "belirli bir konuya ilişkin olma", bilgi alma hizmetinin reklam ve pazarlama amaçlı veri işlemeye ilişkin rızaya bağlanmasının ise "özgür iradeyle açıklanma" unsurunu sakatladığı ve bu uygulamanın KVKK madde 4'teki hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırı olduğu sonucuna ulaşmıştır.

Bu kapsamda, hukuka aykırı veri işlemeyi önlemeye yönelik gerekli tedbirlerin alınmaması nedeniyle 250.000 TL, aydınlatma yükümlülüğünün gereği gibi yerine getirilmemesi nedeniyle 15.000 TL olmak üzere toplam 265.000

TL idari para cezası uygulanmıştır. Veri sorumlusu ayrıca aydınlatma süreçlerinin mevzuata uygun hâle getirilmesi, açık rıza gerektiren çerezler bakımından veri işleme başlamadan önce rıza alınmasını sağlayacak mekanizmanın kurulması ve reklam/pazarlama amaçlı açık rızanın bilgi alma hizmetinden ayrıştırılarak hizmetin ön şartı olmaktan çıkarılması hususlarında talimatlandırılmıştır.

Kurul ayrıca, ilgili kişinin veri sorumlusuna yaptığı başvurunun yazılı veya elektronik ortamda cevaplandırılması gerekirken sözlü olarak cevaplandırılmasının ilgili mevzuata uygun olmadığını belirterek, ilgili kişi başvurularının usulüne uygun ve gerekçeli şekilde sonuçlandırılması gerektiğini veri sorumlusuna hatırlatmıştır. Şikâyete konu ses kaydının ise güvenlik kameraları aracılığıyla değil, veri sorumlusunun bir çalışanı tarafından alındığının anlaşılması üzerine, söz konusu fiilin Türk Ceza Kanunu kapsamında suç teşkil edebileceği değerlendirilerek ilgili kişiye çalışan hakkında suç duyurusunda bulunabileceği yönünde bilgi verilmesine karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 05

SIGORTA

İlgili kişinin banka hesap bilgilerine bilgisi olmaksızın ve gerekli aydınlatma ve açık rıza alma yükümlülükleri yerine getirilmeksizin veri sorumlusu sigorta şirketi tarafından elde edildiği ve işlendiği iddiası

Karar No **2024/1359** Tarih **08.08.2024**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

İlgili kişi, sigortalı bir araçla karıştığı kaza sonrasında araç değer kaybı için sigorta şirketine başvurmuş; değer kaybı ödemesinin banka hesabına yapılması üzerine, IBAN bilgisini şirkete kendisinin vermediğini, sigorta şirketinin müşterisi de olmadığını ve banka hesap bilgisinin bilgisi ve açık rızası dışında elde edilerek işlendiğini ileri sürmüştür. Sigorta şirketi ise IBAN bilgisinin, kaza sonrasında sigortalısı tarafından yapılan hasar bildirimi sırasında şirkete iletildiğini ve KKB'nin IBAN Doğrulama Hizmeti aracılığıyla T.C. kimlik numarası ile IBAN eşleşmesinin teyit edildiğini belirtmiştir.

Kurul, zorunlu mali sorumluluk sigortası mevzuatı kapsamında tazminat başvurusunda zarar gören üçüncü kişiye ait banka hesap bilgilerinin sunulmasının öngörüldüğünü ve somut olayda IBAN bilgisinin poliçe sahibi üçüncü kişi tarafından hasar bildirimi sırasında sigorta şirketine iletildiğini dikkate alarak, söz konusu verinin elde edilmesini hukuka uygun bulmuştur. Aynı kazaya ilişkin daha sonraki değer kaybı başvurusunda avukatın IBAN bilgisinin bulunmaması üzerine, daha önce hukuka uygun şekilde elde edilen IBAN'ın değer kaybı ödemesinde kullanılmasının da KVKK madde 5/2-(e)'deki "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" şartına dayandığı sonucuna varılmıştır. Bu nedenle söz konusu veri işleme faaliyeti bakımından KVKK kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

Bununla birlikte, ilgili kişinin KVKK madde 11 kapsamındaki başvurusunun şirket içindeki bir aksaklık nedeniyle ilgili birimine iletilmediği ve süresinde cevaplandırılmadığı tespit edilmiştir. Kurul, başvuruların KVKK madde 13 ve ilgili Tebliğ uyarınca etkin, hukuka ve dürüstlük kuralına uygun ve gerekçeli şekilde sonuçlandırılması gerektiğini veri sorumlusuna hatırlatmıştır. Ayrıca veri sorumlusunun şikâyetin süre yönünden reddi talebi kabul edilmemiş; ilgili kişinin Kurum'a yaptığı ilk şikâyet tarihi esas alınarak başvurunun süresinde olduğu değerlendirilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 06

ELEKTRONIK HABERLEŞME

İlgili kişinin kişisel verisi niteliğindeki cep telefonu numarasının elektronik haberleşme işletmecisi veri sorumlusu tarafından SMS gönderilmek suretiyle işlenmesi

Karar No **2024/1350** Tarih **08.08.2024**

YAPTIRIM

100.000 TL idari para cezası

KARARIN ÖZETİ

İlgili kişiye, elektronik haberleşme işletmecisi tarafından kampanyasının sona ereceğine ve sunulan hizmetlere ilişkin aynı veya benzer içerikte çok sayıda SMS gönderilmiştir. İlgili kişi, mesajlarla sunulan teklifleri çağrı merkezi görüşmelerinde reddetmesine rağmen iletilerin devam ettiğini ve ticari ileti izninin aktif bir onayla değil, sözleşmede yer alan "pazarlama yapılmasına izin vermiyorum" seçeneğinin işaretlenmemesi üzerinden kurgulandığını ileri sürmüştür. Veri sorumlusu ise elektronik haberleşme mevzuatı uyarınca abonelere kampanya bitişi hakkında bilgilendirme yapılmasının zorunlu olduğunu ve ilgili kişiye pazarlama içerikli ileti gönderimini reddetme imkânı tanındığını savunmuştur.

Kurul, kampanya bitişine ilişkin bilgilendirme yapılmasının veri sorumlusunun hukuki yükümlülüğü kapsamında olduğunu ve bu amaçla ilgili kişinin cep telefonu numarasının KVKK madde 5/2-(ç) uyarınca işlenebileceğini kabul etmiştir. Bununla birlikte, 2 Eylül 2023 tarihinde sona erecek sözleşme bakımından 8 Mayıs 2023–26 Temmuz 2023 tarihleri arasında 20'den fazla ve sık aralıklarla SMS gönderilmesini, ilgili kişinin makul beklentisini aşan ve veri sorumlusunun sahip olduğu hakkı kötüye kullanması sonucunu doğuran bir veri işleme faaliyeti olarak değerlendirmiştir. Bu nedenle söz konusu uygulamanın KVKK madde 4/2-(a)'daki hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırı olduğu sonucuna ulaşılmıştır.

Bu kapsamda veri sorumlusu hakkında KVKK madde 12/1'deki kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğüne aykırı olduğu sonucuna varılarak veri sorumlusu hakkında KVKK madde 18/1-(b) uyarınca 100.000 TL idari para cezası uygulanmıştır. Kurul ayrıca, kişisel verilerin işlenmesine ilişkin açık rıza hükümlerinin abonelik sözleşmesinin içinde yer almasının ilgili kişiler bakımından yanıltıcı olabileceğini ve açık rızanın unsurlarını sakatlayabileceğini değerlendirerek, açık rıza metninin sözleşmeden ayrı şekilde sunulmasının uygun olacağını veri sorumlusuna hatırlatmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 07

BANKACILIK

Veri sorumlusu banka çalışanı İlgili Kişi ile bir müşteri arasında gerçekleştirilen telefon görüşmelerine ilişkin kayıtlara erişim talebinin veri sorumlusu tarafından reddedilmesi

Karar No **2024/592** Tarih **18.04.2024**

YAPTIRIM

Görüşme kayıtlarının ilgili kişiye sağlanması yönünde talimat verilmiştir.

KARARIN ÖZETİ

Bir banka çalışanı, banka müşterisiyle kayıt altına alınan telefon görüşmesinde kendisine hakaret edildiğini belirterek yasal yollara başvurabilmek amacıyla görüşme kaydının kendisine verilmesini talep etmiştir. Banka ise kaydın müşteriye ait kredi ve gecikme bilgileri gibi müşteri sırrı niteliğindeki verileri de içerdiğini, bu nedenle kaydın paylaşılmasının bankacılık mevzuatına aykırı olacağını ileri sürerek talebi reddetmiştir. Banka, müşteri bilgilerinin maskelenmesinin dahi müşterinin kredi durumuna ilişkin bilgi açığa çıkarabileceğini savunmuştur.

Kurul, Anayasa madde 20/3 ve KVKK madde 11 kapsamında kişisel verilere erişim hakkının, kişinin kendisiyle ilgili işlenen verilere ulaşabilmesini de içerdiğini değerlendirmiştir. Çalışanın talebinin müşterinin bankacılık bilgilerini öğrenmeye değil, tarafı olduğu görüşmede gerçekleştiğini iddia ettiği hakareti ispatlamaya yönelik olduğu ve yasal yollara başvurabilmesi bakımından kayda erişmekte meşru menfaatinin bulunduğu kabul edilmiştir. Bu nedenle somut olayda Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik'in uygulanamayacağı ve KVKK hükümlerinin uygulanacağı sonucuna ulaşılmıştır.

Kurul, üçüncü kişiye ait müşteri sırrı niteliğindeki bankacılık işlem verilerinin maskelenmesi suretiyle görüşme kaydının yazılı döküm veya dijital ortamda ilgili kişiye verilmesi ve sonucundan Kurula bilgi verilmesi yönünde bankayı talimatlandırmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 08

ÜRETIM / SANAYI

Veri sorumlusu tarafından iş yerinin kamera ile izlenmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyeti

Karar No **2024/540** Tarih **28.03.2024**

YAPTIRIM

Veri sorumlusuna aydınlatma ve açık rıza metinlerinin düzeltilmesi yönünde talimat verilmiş; ayrıca KVKK başvurularında özel yetkili vekâletname aranmaması konusunda uyarıda bulunulmuştur.

KARARIN ÖZETİ

İlgili kişi, veri sorumlusu bünyesinde üretim görevlisi olarak çalışmakta iken iş akdini noter ihtarnamesiyle feshetmiş ve fesih gerekçelerinden biri olarak, çalışanların soyunma/giyinme odası olarak kullandığını belirttiği alanın güvenlik kameralarıyla izlenmesini göstermiştir. İlgili kişi, bu kapsamda gerçekleştirilen kişisel veri işleme faaliyetinin hukuka aykırı olduğunu ileri sürmüştür. Veri sorumlusu ise söz konusu alanın soyunma odası olmadığını, çalışanların kişisel eşyalarını ve iş yeleklerini muhafaza ettikleri kilitli dolapların bulunduğu bir alan olduğunu; daha önce yaşanan hırsızlık olayları nedeniyle kameraların çalışanların talebi üzerine yerleştirildiğini belirtmiştir. Kurul, kamera yerleştirilmesine ve sonrasında yaygınlaştırılmasına ilişkin çalışan taleplerinin bulunduğunu ve ilgili kişinin de bu talep yazılarını imzaladığını dikkate almıştır

Kurul, kameraların çalışanların kişisel eşyalarının korunması ile iş yerinde asayiş ve güvenliğin sağlanması amacıyla kullanılmasını KVKK madde 5/2-(f) kapsamındaki veri sorumlusunun meşru menfaati çerçevesinde değerlendirmiştir. Kameraların çalışanların talebi üzerine kurulması, kurulum sonrasında yeni bir hırsızlık vakası yaşanmaması, kapalı devre kayıt sistemi kullanılması ve görüntülerin 60 gün süreyle yurt içindeki yerel sunucularda saklandıktan sonra imha edilmesi birlikte dikkate alınarak, söz konusu veri işleme faaliyetinin KVKK madde 4'teki genel ilkelere aykırılık teşkil etmediği ve bu hususta işlem yapılmasına gerek bulunmadığı sonucuna ulaşılmıştır. Görüntü kayıtlarının 60 gün sonunda imha edildiğinin ayrıca belgelendirildiği dikkate alınarak bu hususta da işlem yapılmamıştır.

Bununla birlikte Kurul, ilgili kişiye sunulan aydınlatma metninde kişisel verilerin hangi işleme şartına dayanılarak işlendiğinin somut biçimde açıklanmadığını, yalnızca KVKK madde 5, 6, 8 ve 9'a genel nitelikte atıflar yapıldığını tespit etmiştir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ madde 5/1-(g), (ğ) ve (h) bentleri uyarınca aydınlatma kapsamında işleme amacının belirli, açık ve meşru olması, anlaşılır ve sade bir dil kullanılması ve hukuki sebebin açıkça belirtilmesi gerektiği dikkate alınarak söz konusu aydınlatma metninin yeniden düzenlenmesi yönünde veri sorumlusu talimatlandırılmıştır. Ayrıca aydınlatma ile açık rıza alma süreçlerinin birlikte yürütülmesinin Tebliğ madde 5/1-(f) bendine aykırı olduğu, bu süreçlerin ayrıştırılması ve açık rıza metninde diğer hukuki sebeplere dayanılarak işlenen kişisel verilere yer verilmemesi gerektiği belirtilmiştir. Veri sorumlusunun, ilgili kişinin vekili tarafından yapılan başvuruyu vekâletnamede özel yetki bulunmadığı gerekçesiyle cevaplamaması da uygun bulunmamış; kişisel verilerin korunması mevzuatında vekil aracılığıyla yapılan başvurular için özel yetkili vekâletname şartı bulunmadığı belirtilerek veri sorumlusu bu hususta uyarılmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 09

FİNANS

İlgili kişinin, kapatmış olduğu borcuna ilişkin bilgilerin risk raporundan silinmesi talebinin Kredi Kayıt Bürosu AŞ tarafından reddedilmesi hakkında

Karar No **2024/444** Tarih **14.03.2024**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

İlgili kişi, daha önce bir bankaya olan ve 2017 yılında tamamen ödediği borcuna ilişkin kayıtların Findeks Risk Raporu'nda hâlen görünmesi üzerine Kredi Kayıt Bürosu AŞ'ye ("KKB") başvurarak söz konusu verilerin silinmesini talep etmiştir. KKB ise Findeks Risk Raporlarının Türkiye Bankalar Birliği Risk Merkezi ("Risk Merkezi") nezdindeki bilgiler esas alınarak oluşturulduğunu, ilgili borcun ödendiği bilgisinin kayıtlara işlendiğini ve raporda gerçeğe aykırı herhangi bir bilgi bulunmadığını belirtmiştir.

Kurul, KKB'nin Risk Merkezi adına yürüttüğü operasyonel faaliyetlerde veri işleyen sıfatıyla hareket etmekle birlikte, Findeks platformu kapsamında banka ve finansal kuruluşlardan aktarılan bilgileri derleyerek risk raporu oluşturması ve bu kapsamda müşterilerin finansal verilerini kullanması bakımından veri sorumlusu olduğunu değerlendirmiştir. İncelemede, ilgili kişinin borcunun 20.01.2017 tarihinde tamamen ödendiği ve varlık yönetim şirketi tarafından aynı tarihte Risk Merkezi'ne "kapalı" olarak bildirildiği tespit edilmiştir. Risk Merkezi'nin ise kişisel verileri KVKK madde 5/2'deki "kanunlarda açıkça öngörülme" işleme şartına dayanarak açık rıza aranmaksızın işlediği değerlendirilmiştir.

Kurul, borcun kapanmış olmasının borca ilişkin geçmiş finansal verilerin derhâl silinmesini gerektirmediğini; Risk Merkezi tarafından belirlenen sistem kapsamında kapanmış borçlara ilişkin verilerin, son durumun bildirilmesinden itibaren 10 yıl boyunca işlenmeye ve Risk Merkezi üyeleri ile ilgili kişinin kendisiyle paylaşılmaya devam edildiğini dikkate almıştır. Somut olayda borcun 2017 yılında kapanması nedeniyle bu veriye ilişkin işleme amacının 2027 yılına kadar devam ettiği ve dolayısıyla verinin bu tarihe kadar Risk Merkezi nezdinde işlenmesinin hukuka uygun olduğu değerlendirilerek, ilgili kişinin iddiaları hakkında KVKK kapsamında yapılacak herhangi bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 10

FINANS

İlgili kişinin kişisel verilerinin Kredi Kayıt Bürosu AŞ tarafından hukuka aykırı şekilde işlendiğine yönelik şikâyet

Karar No **2024/292** Tarih **22.02.2024**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

İlgili kişi, Kredi Kayıt Bürosu AŞ ("KKB") tarafından kişisel verilerinin işlendiğini, saklandığını, üçüncü kişilerle paylaşıldığını ve ticari amaçlarla kullanıldığını öğrendiğini; bu nedenle KKB'ye başvurarak kişisel verilerinin silinmesini talep ettiğini, ancak verilerinin silinmeyeceği ve kullanılmaya devam edileceği yönünde cevap aldığını ileri sürerek Kurula başvurmuştur.

KKB; 5411 sayılı Bankacılık Kanunu ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu uyarınca bankalar ve finansal kuruluşlar arasındaki veri paylaşımına aracılık ettiğini ve bu kapsamda gerçekleştirilen veri işleme faaliyetleri bakımından ilgili kişinin açık rızasının aranmadığını belirtmiştir. Ayrıca ilgili kişinin 2013 yılında Findeks platformuna üye olduğu ve üyeliğinin hâlen aktif bulunduğu, Findeks üzerinden sağlanan kişisel verilerin ise üyeliğin iptal edildiği tarihten itibaren 10 yıl süreyle saklanacağı ve bu sürenin sonunda mevzuata uygun şekilde imha edileceği açıklanmıştır.

Kurul, KKB'nin ilgili kişinin başvurusuna verdiği cevapta bankacılık mevzuatından kaynaklanan veri işleme faaliyetlerini, açık rıza gerekmemesinin hukuki dayanağını ve Findeks üyeliği kapsamında uygulanan saklama süresini yeterli şekilde açıkladığını değerlendirmiştir. Bu nedenle KKB tarafından verilen cevabın açık ve yeterli olduğu sonucuna ulaşılmış ve şikâyet hakkında KVKK kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 11

KAMU İŞTIRAKI / İSTIHDAM

Bir kamu kuruluşunun iştiraki hakkındaki kişisel verilerin hukuka aykırı işlenmesi, amacına aykırı kullanılması ve üçüncü taraflara aktarılması ile aydınlatma metninin hukuka aykırılığı konulu şikâyet

Karar No **2024/284** Tarih **22.02.2024**

YAPTIRIM

Veri sorumlusuna aydınlatma metninin mevzuata uygun hâle getirilmesi ve ilgili kişinin kişisel verilerine erişim talebinin karşılanması yönünde talimat verilmiş; sağlık verilerine erişim yetkilerinin yalnızca görevleri gereği bu verilere erişmesi gereken kişilerle sınırlandırılması gerektiği hatırlatılmıştır.

KARARIN ÖZETİ

İlgili kişi, iş ilişkisinin sona ermesinden sonra da kişisel verilerinin işlendiğini; kurumsal e-posta hesabına erişildiğini, istirahat ve sağlık raporlarının Personel Yönetim Sistemi ("PYS") üzerinden işlendiğini ve aktarıldığını, işyerinde ateş ölçümü yapıldığını, sağlık verilerine gereğinden geniş erişim bulunduğunu ve kişisel verilerine erişim talebinin karşılanmadığını ileri sürmüştür.

Kurul, işten ayrılma sonrasında kurumsal e-posta hesabına fiilen erişildiğinin ve ateşi yüksek kişilerin fotoğraflarının yetkili personele gönderildiğinin ispatlanamadığını; anlık ateş ölçümünün ise herhangi bir veri kayıt sisteminin parçası olmaması nedeniyle KVKK kapsamında kişisel veri işleme faaliyeti oluşturmadığını değerlendirmiştir. İstirahat raporlarının işverenin hukuki yükümlülükleri kapsamında PYS üzerinden işlenmesini hukuka uygun bulmuş; PYS altyapısını sağlayan kamu kurumunun bu süreçte veri işleyen konumunda olduğunu kabul etmiştir.

Bununla birlikte Kurul, sağlık verilerine görevleri gereği erişmesi gerekmeyen kişilerin erişiminin sınırlandırılması gerektiğini belirtmiştir. Eski çalışana ait e-posta içeriklerinin olası uyuşmazlıklarda savunma ve ispat amacıyla muhafaza edilmesini KVKK madde 5/2-(e) kapsamında hukuka uygun bulmuş; ancak bu işleme faaliyetlerinin aydınlatma metninde yeterince açıklanmadığını tespit etmiştir. Ayrıca PYS hesabının pasife alınmasının kişisel verilerin silindiği anlamına gelmediğini ve muhafazanın da kişisel veri işleme faaliyeti olduğunu belirterek, ilgili kişinin erişim talebinin karşılanması ve aydınlatma metninin güncellenmesi yönünde veri sorumlusunu talimatlandırmıştır. İlgili kişinin talebi üzerine sağlık bilgileri ile sunum ve raporlarda yer alan kişisel verilerin 30 gün içinde imha edildiği de tespit edilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 12

TELEKOMÜNIKASYON / ELEKTRONIK HABERLEŞME

İlgili kişinin abonelik sözleşmesinin bir telekomünikasyon şirketi tarafından kimlik belgesi eksikliği sebebiyle feshedilmesi kapsamında yürütülen kişisel veri işleme faaliyetlerine ilişkin şikâyet ile Kurul tarafından başlatılan resen inceleme

Karar No **2024/282** Tarih **22.02.2024**

YAPTIRIM

350.000 TL idari para cezası Ayrıca abonelik sözleşmesinin ve açık rıza süreçlerinin mevzuata uygun hâle getirilmesi ile ilgili kişiye talep ettiği bilgi ve belgelerin sağlanması yönünde veri sorumlusu talimatlandırılmıştır.

KARARIN ÖZETİ

İlgili kişinin telekomünikasyon aboneliği, altyapı değişikliği nedeniyle yeni bir abonelik sözleşmesi kurulması sürecinde gerekli kimlik belgesinin sunulmaması üzerine feshedilmiş; ilgili kişi kimlik belgesinin talep edilmesini ve kişisel verilerinin işlenmeye devam edilmesini hukuka aykırı bulmuştur. Kurul, yeni abonelik sözleşmesinin kurulması sırasında kimlik belgesinin ibraz edilmesinin elektronik haberleşme mevzuatından kaynaklanan bir yükümlülük olduğunu ve bu kapsamda kimlik bilgilerinin işlenmesinin KVKK madde 5/2-(c) ve (ç) kapsamında hukuki dayanağa sahip olduğunu değerlendirmiştir. Ayrıca kimlik bilgilerinin olası hukuki uyuşmazlıklarda savunma hakkının kullanılması ve yetkili mercilerden gelebilecek talepler bakımından muhafaza edilmesinin KVKK madde 5/2-(e) kapsamında da mümkün olduğu; bu nedenle işleme sebepleri devam ettiği sürece verilerin imha edilemeyeceği, ancak amaçla bağlantılı ve asgari süreyle sınırlı olarak saklanması gerektiği belirtilmiştir.

Kurul ayrıca, açık rıza dışında geçerli veri işleme şartları mevcut olmasına rağmen abonelik sözleşmesinde kişisel verilerin işlenmesi ve aktarılmasına açık rıza verildiği izlenimi uyandıran hükümlere yer verilmesini, ilgili kişinin yanıltılması ve yanlış yönlendirilmesi sonucunu doğurabilecek nitelikte değerlendirmiştir. Bu uygulamanın KVKK madde 4/2-(a)'daki hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırı olduğu ve veri sorumlusunun KVKK madde 12/1 kapsamındaki yükümlülüğünü ihlal ettiği sonucuna ulaşılmıştır.

Bu nedenlerle, veri sorumlusu hakkında 350.000 TL idari para cezası uygulanmış; ilgili kimlik verilerinin amaçla bağlantılı ve asgari süreyle saklanması gerektiği hatırlatılmış, abonelik sözleşmesinin bir örneğinin ilgili kişiye verilmesi, kişisel verilerin aktarıldığı grup şirketlerinin listesinin paylaşılması ve sözleşmenin "Gizlilik" bölümündeki açık rıza izlenimi veren hükümlerin çıkarılarak açık rıza gerektiren veri işleme faaliyetlerinin sözleşme ve aydınlatma metninden ayrı şekilde düzenlenmesi yönünde veri sorumlusu talimatlandırılmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 13

TELEKOMÜNIKASYON / TEKNOLOJI

Telekomünikasyon teknolojileri geliştirme alanında faaliyet gösteren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2025/881** Tarih **22.05.2025**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Veri sorumlusunun çalışanlarının iş seyahatleri ve buna bağlı harcamalarının yönetildiği uygulamada, uygulamayı yöneten bir çalışanın sehven başka bir uygulama ile entegrasyonu etkinleştirmesi sonucunda bazı çalışanlara ait kişisel veriler üçüncü bir şirketle paylaşılmıştır. İhlal, çalışanların iş e-posta adreslerine gelen otomatik bildirimleri fark ederek durumu ilgili birimlere iletmesi üzerine tespit edilmiş; bunun ardından senkronizasyon derhal durdurulmuş ve verilerin aktarıldığı şirketten ilgili verilerin silinmesi talep edilmiştir.

İhlalden 488 çalışan etkilenmiş; etkilenen veriler ad-soyad, iş e-posta adresi ve iş telefon numarası ile sınırlı kalmıştır. Kurul ayrıca ihlalle bağlantılı çalışanlara son bir yıl içinde kişisel verilerin korunması eğitimi verilmiş olmasını ve ihlalin ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının düşük olduğunu dikkate almıştır.

Bu hususlar birlikte değerlendirilerek, kişisel veri ihlali hakkında yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 14

SIVIL TOPLUM / BILIMSEL ARAŞTIRMA

Bilimin ilerlemesini destekleyen kâr amacı gütmeyen bir kuruluş olarak faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2025/833** Tarih **02.05.2025**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Bilimin ilerlemesini destekleyen ve kâr amacı gütmeyen bir kuruluşun kullandığı haber bülteni dağıtım platformuna yetkisiz erişim sağlanması sonucunda kişisel veri ihlali meydana gelmiştir. Olay, platformu işleten veri işleyenin bildirimi üzerine veri sorumlusu tarafından öğrenilmiş ve inceleme süresince ilgili platform geçici olarak devre dışı bırakılmıştır. İhlalden Türkiye'de ikamet eden 15 kişi etkilenmiş; erişime konu veriler ad, soyad ve e-posta adresleriyle sınırlı kalmıştır.

Kurul; etkilenen kişi sayısının ve veri kapsamının sınırlı olmasını, verilerin dolandırıcılık veya kimlik hırsızlığı gibi kötüye kullanım faaliyetlerinde kullanıldığına ilişkin herhangi bir bulgu bulunmamasını ve ilgili kişiler bakımından riskin son derece düşük olmasını dikkate almıştır. İlgili kişilere bildirim yapılması ile veri sorumlusunun benzer ihlallerin önlenmesine yönelik ek tedbirleri değerlendirmeye ve uygulamaya başlaması da değerlendirmede göz önünde bulundurulmuştur.

Veri sorumlusu, sistem ve veri güvenliğini güçlendirmeye yönelik önlemler kapsamında çok faktörlü kimlik doğrulamanın (MFA) etkinleştirilmesini de değerlendirmiştir. Bu hususlar birlikte dikkate alınarak yapılacak bir işlem bulunmadığına karar verilmiştir. Bununla birlikte, gelecekte Kurul'a yapılacak veri ihlal bildirimlerinde 24.01.2019 tarihli ve 2019/10 sayılı Kurul Kararı'na uygun Kişisel Veri İhlal Bildirim Formunun kullanılması gerektiği veri sorumlusuna hatırlatılmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 15

OTELCILIK / KONAKLAMA

Otelcilik ve konaklama yönetimi alanında faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2025/601** Tarih **28.03.2025**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Hong Kong merkezli ve Türkiye'de herhangi bir tüzel kişiliği, kuruluşu, grup şirketi, iştiraki, çalışanı veya teknoloji altyapısı bulunmayan otelcilik şirketinin sistemlerine yetkisiz erişim sağlanmış; bazı dosyaların şifrelendiği ve fidye talebi içeren bir mesaj gönderildiği tespit edilmiştir. İhlalden Türkiye'de yerleşik 909 kişi etkilenmiş; etkilenen veriler arasında ad, doğum tarihi, pasaport veya kimlik numarası, adres, telefon, e-posta ile bazı kişiler bakımından ödeme kartı numarası ve son kullanma tarihi yer almıştır.

Kurul, değerlendirmesini esas olarak KVKK'nin yer bakımından uygulanabilirliği üzerinden yapmıştır. KVKK'de yer bakımından uygulama alanının açıkça düzenlenmediğini; bununla birlikte 24.01.2019 tarihli ve 2019/10 sayılı Kurul Kararı uyarınca, yurt dışında yerleşik veri sorumlusu nezdinde gerçekleşen bir ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve bu kişilerin sunulan ürün veya hizmetlerden Türkiye'de faydalanması hâlinde "etki ilkesi" doğrultusunda Kurul'a bildirim yükümlülüğünün doğabileceğini belirtmiştir.

Somut olayda ise ilgili kişilerin şirketin ürün ve hizmetlerinden Türkiye'de faydalanmadıkları; şirketin tüm veri işleme faaliyetlerinin, otel varlıklarının ve teknoloji altyapısının Hong Kong'da bulunduğu dikkate alınmıştır. Bu nedenle şirketin somut olay bakımından KVKK kapsamında veri ihlali bildirim yükümlülüğünün bulunmadığı ve ilgili veri işleme faaliyetinin KVKK'de yer bakımından uygulama alanına girmediği sonucuna ulaşılmış; KVKK kapsamında bu aşamada yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 16

TÜKETICI ÜRÜNLERI / KÜÇÜK EV ALETLERI

Küçük ev aletleri üretimi ve satışı yapan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2025/536** Tarih **12.03.2025**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Veri sorumlusu tarafından müşterilere gönderilen bazı bilgilendirme e-postalarında alıcıların e-posta adreslerinin gizlenmeden iletilmesi nedeniyle müşterilerin birbirlerinin e-posta adreslerini görmesi şeklinde bir kişisel veri ihlali meydana gelmiştir. Olay, gönderim sonrasında ilgili çalışan tarafından fark edilmiş ve e-postaların geri çekilmesi için aksiyon alınmıştır. İhlalin tahmini olarak 500 müşteriyi etkilediği, ihlale konu kişisel verinin ise e-posta adresiyle sınırlı olduğu bildirilmiştir.

Kurul, ihlalin toplam 14 e-posta üzerinden gerçekleştiğini, geri çekme işlemi nedeniyle bazı alıcılara iletilerin ulaşmamış olabileceğini ve ihlalin ilgili kişiler üzerinde olumsuz sonuç doğurma ihtimalinin düşük olduğunu dikkate almıştır. Ayrıca ilgili kişilere e-posta ve çağrı merkezi aracılığıyla ihlal bildirimi yapılacağının belirtildiği görülmüştür. Bu hususlar birlikte değerlendirilerek, kişisel veri ihlali hakkında yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 17

GIDA / RESTORAN

Restoran zinciri ve hızlı servis gıda şirketi olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2025/88** Tarih **09.01.2025**

YAPTIRIM

Toplam 1.000.000 TL idari para cezası 800.000 TL: gerekli teknik ve idari tedbirlerin alınmaması 200.000 TL: veri ihlalinin ilgili kişilere en kısa sürede bildirilmemesi

KARARIN ÖZETİ

Restoran zinciri ve hızlı servis alanında faaliyet gösteren şirketin bir bilgi işlem çalışanının bilgisayarına, tarayıcı üzerinden çalışan zararlı yazılım aracılığıyla yetkisiz erişim sağlanmış; tarayıcıda kayıtlı kullanıcı adı ve şifrelerin ele geçirilmesi sonucunda şirket sistemlerinden birine de erişilmiştir. İhlal kapsamında 505.337 müşterinin ad-soyad, cinsiyet, e-posta adresi, telefon numarası ve yaşadığı şehir bilgileri etkilenmiştir.

Kurul; saldırganın sisteme girişini tespit edecek alarm ve izleme mekanizmalarının bulunmamasını, kullanıcı adı ve şifrelerin tarayıcıda kayıtlı tutulmasını, iki faktörlü kimlik doğrulama ile SIEM ve güvenlik duvarı gibi takip ve kontrol mekanizmalarının ihlal sonrasında devreye alınmasını ve ihlal öncesinde çalışanlara kişisel veri güvenliği eğitimi verildiğinin tevsik edilememesini önemli güvenlik eksiklikleri olarak değerlendirmiştir. Bu hususlar, veri sorumlusunun risk ve tehditleri önceden belirleyerek gerekli teknik ve idari tedbirleri almakta yetersiz kaldığını göstermiştir.

Kurul, ihlalin kapsamını ve ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının yüksek olmasını da dikkate alarak, KVKK madde 12/1 kapsamındaki veri güvenliği yükümlülüklerinin ihlali nedeniyle 800.000 TL idari para cezası uygulamıştır. Ayrıca ilgili kişilere ihlalin en kısa sürede ve Kurul'un belirlediği usule uygun şekilde bildirilmemesi nedeniyle KVKK madde 12/5 kapsamında 200.000 TL daha idari para cezasına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 18

ÜRETIM / PLASTIK VE TEMIZLIK ÜRÜNLERI

Plastik ev gereçleri ve temizlik ürünleri üretimi yapan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/2196** Tarih **26.12.2024**

YAPTIRIM

250.000 TL idari para cezası

KARARIN ÖZETİ

Plastik ev gereçleri ve temizlik ürünleri üreten veri sorumlusunun sistemleri fidye yazılımı saldırısına uğramış; sistemlerdeki veriler şifrelenmiş ve saldırganlar tarafından fidye talep edilmiştir. Veri sorumlusu başlangıçta kişisel verilerin ele geçirildiğine ilişkin bir tespit bulunmadığını belirtmesine rağmen, saldırganların verileri kopyaladıklarını ileri sürmesi ve veri sorumlusunun adli mercilere sunduğu belgelerde verilerin saldırganlarca elde edildiğine ilişkin ifadelere yer verilmesi dikkate alınmıştır. Kurul ayrıca veri sorumlusunun ihlalin kapsamı, etkilenen kişiler, veri kategorileri ve ihlalin tespit tarihi konusunda birbiriyle çelişen beyanlarda bulunduğunu tespit etmiştir.

İncelemede çalışanlara ait belgelerde çok sayıda kişisel veri ile özel nitelikli kişisel verilerin bulunduğu görülmüş; müşteri bilgilerinin yalnızca ticari veri olduğu yönündeki açıklama ise, tüzel kişilere ilişkin belgelerin gerçek kişileri belirli veya belirlenebilir kılan bilgiler içerebileceği dikkate alınarak yeterli bulunmamıştır. Veri sorumlusunun talep edilmesine rağmen ilgili belge örneklerini ve Kişisel Veri İşleme Envanteri'ni Kurul'a sunamaması da değerlendirmede dikkate alınmıştır.

Kurul; güvenli şifreleme/kriptografik anahtar kullanımına yönelik tedbirler ile işletme dışından erişimler için iki faktörlü kimlik doğrulamanın ancak ihlal sonrasında uygulanmasını, saldırıya neden olan güvenlik açığının belirlenememesini, gerekli log kayıtlarına ulaşılamamasını ve ihlal öncesinde yapılan güvenlik testlerinin saldırganların sisteme erişmesini ve veri çıkarmasını engelleyecek yeterlilikte olmamasını önemli eksiklikler olarak değerlendirmiştir. Ayrıca saldırının veri sorumlusu dahil dokuz şirketi etkilemesi, ağ segmentasyonunun uygun şekilde yapılmadığının göstergesi olarak kabul edilmiştir. Bu nedenlerle KVKK madde 12/1 kapsamında gerekli teknik ve idari tedbirlerin alınmadığı sonucuna varılarak 250.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 19

KURUMSAL HIZMETLER

Avrupa'da bulunan grup şirketlerine kurumsal destek hizmetleri sağlayan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/1899** Tarih **07.11.2024**

YAPTIRIM

700.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusunun pazarlama faaliyetlerinde kullanılan bir kullanıcı hesabının kullanıcı adı ve parola bilgilerinin ele geçirilmesi üzerine, saldırganlar bu hesap aracılığıyla FTP sunucusunda bulunan ve bazıları "herkese açık" olarak ayarlanmış klasörlere yetkisiz erişim sağlamıştır. İhlalden yaklaşık 70.000 kişinin ad-soyad, e-posta, iletişim ve adres bilgileri etkilenmiş; kredi kartı veya özel nitelikli kişisel verilere erişildiğine ilişkin bir bulguya rastlanmamıştır.

Kurul, ihlalin ne zaman başladığının belirlenememesini, sisteme birden fazla kez yetkisiz erişim sağlanmasını ve olayın uzun süre sonra fark edilmesini, veri sorumlusunun sistem erişimlerini yeterli şekilde takip ve kontrol edemediğinin göstergesi olarak değerlendirmiştir. Kişisel veri içeren klasörlerin erişime açık bırakılması ve güçlü parola politikasının ancak ihlal sonrasında uygulanmaya başlanması da erişim güvenliği bakımından önemli eksiklikler olarak kabul edilmiştir.

Bu değerlendirmeler doğrultusunda veri sorumlusunun KVKK madde 12 kapsamında gerekli teknik ve idari tedbirleri almadığı sonucuna varılarak 700.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 20

İLAÇ / SAĞLIK ÜRÜNLERİ

İlaç ve sağlık ürünleri alanında faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/1898** Tarih **07.11.2024**

YAPTIRIM

350.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusunun sipariş yönetim sistemine bağlı sunucusu ransomware saldırısıyla şifrelenmiş ve saldırgan tarafından fidye talep edilmiştir. İhlalden 196 mevcut çalışan, 303 eski çalışan ve 17 müşteri/iş ortağı olmak üzere toplam 520 kişi etkilenmiş; ad-soyad, doğum tarihi, iş e-posta adresi, işe giriş tarihi, portal şifresi ve sipariş bilgileri ihlale konu olmuştur. Veri sorumlusu, verilerin dışarı aktarıldığına ilişkin kanıt bulunmadığını belirtmiş olsa da Kurul değerlendirmesini yetkisiz erişimin gerçekleşmesi ve alınan güvenlik tedbirlerinin yeterliliği üzerinden yapmıştır.

Kurul; saldırganın sunucuda zararlı yazılım ve dosyalar indirip çalıştırabilmesini, farklı kodlar çalıştırarak sistemi şifreleyebilmesini, ilk erişim yönteminin kesin olarak belirlenememesini, sınırlı log kayıtlarında yoğun uzak bağlantı denemelerinin bulunmasını ve saldırganın yetkisini yükselterek sistemde kalıcılık sağlayabilmesini, kişisel veri güvenliğinin yeterince izlenmediğinin göstergeleri olarak değerlendirmiştir.

Ayrıca ihlal sonrasında hazırlanan teknik raporda ağ ve sunucu güvenliğinin sıkılaştırılması, merkezi loglama, uç nokta güvenliği, en az yetki prensibi ve düzenli zafiyet/sızma testleri gibi çok sayıda iyileştirme önerilmesi, mevcut tedbirlerin yetersiz kaldığını göstermiştir. Bu nedenle veri sorumlusunun KVKK madde 12/1 kapsamındaki gerekli teknik ve idari tedbirleri almadığı sonucuna varılarak 350.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 21

KOZMETIK / KIŞISEL BAKIM

Konu Özeti Kozmetik ve kişisel bakım şirketi olan veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/1718** Tarih **09.10.2024**

YAPTIRIM

500.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusunun ağ sunucularından birine Trojan türü zararlı yazılım bulaştırılması sonucunda sistemlere yetkisiz erişim sağlanmış; saldırganlar tarafından fidye talep edilerek ele geçirilen verilerin yayımlanacağı veya satılacağı yönünde tehditte bulunulmuştur. İhlalden Türkiye bakımından yaklaşık 432 kişi etkilenmiş; 325 kişiye ait kimlik belgesi veya ikamet izin belgesi ile 107 marka elçisine ait kimlik ve iletişim bilgileri ihlale konu olmuştur.

Kurul, özellikle EDR çözümünün ancak ihlal sonrasında devreye alınmasını, zararlı yazılımlara karşı yeterli tespit ve izleme mekanizmalarının önceden kurulmadığının göstergesi olarak değerlendirmiştir. Çalışanlara veri koruma eğitimleri verilmiş olmasına rağmen, mevcut risklerin belirlenmesi ve bu risklere karşı alınacak önlemlerin planlanması bakımından risk analizinin yeterli olmadığı sonucuna ulaşılmıştır.

Ayrıca veri sorumlusunun ihlal öncesinde sızma testi yaptırmadığı ve sistemlerin düzenli güvenlik taramalarına tabi tutulduğunu gösteren yeterli belge sunamadığı dikkate alınarak, zararlı yazılımlara karşı koruma, risk analizi ve sistemlerin etkin şekilde izlenmesi bakımından gerekli teknik ve idari tedbirlerin alınmadığı değerlendirilmiş; veri sorumlusu hakkında 500.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 22

TURIZM / OTELCILIK

Turizm, otelcilik ve konaklama işletmeciliği yapan veri sorumlusu tarafından Kuruma intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/1523** Tarih **10.09.2024**

YAPTIRIM

500.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusu otel işletmesinde çalışan bir personelin phishing içerikli e-postadaki bağlantıya tıklaması üzerine bilgisayarın kontrolü yetkisiz kişilerce ele geçirilmiştir. Olay fark edildiğinde ilgili bilgisayar ağdan ayrılarak erişim sonlandırılmıştır. İhlal yalnızca bu cihazla sınırlı kalmış ve olağandışı veri aktarımı tespit edilmemiş olmakla birlikte, bilgisayarda bulunan vardiya çizelgesi nedeniyle 450 çalışanın ad-soyad bilgisi yetkisiz erişime maruz kalmıştır.

Kurul, olayın gerçekleşme biçiminin yanı sıra veri sorumlusunun genel bilgi güvenliği altyapısını da değerlendirmiş; güncel olmayan sanal sunucu ve veri tabanı sistemleri, yetersiz konfigürasyon ve alan adı politikaları, zayıf parola kullanımı, web uygulaması zafiyetleri ve spam e-postalarına karşı ciddi koruma eksikliği bulunduğunu tespit etmiştir. Çalışanın phishing saldırısına maruz kalması ve zayıf parola kullanımı da çalışan farkındalığı ve erişim güvenliği bakımından yetersizlik göstergesi olarak değerlendirilmiştir.

Ayrıca sunucu odalarına girişlerde kimlik doğrulama mekanizmasının bulunmaması, fiziksel veri güvenliği bakımından ayrı bir eksiklik olarak görülmüştür. Bu hususlar birlikte değerlendirilerek veri sorumlusunun KVKK madde 12 kapsamında gerekli teknik ve idari tedbirleri almadığı sonucuna varılmış ve 500.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 23

DIJITAL OYUN / EĞLENCE

Dijital oyun ve eğlence platformları sunan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2023/1017** Tarih **08.06.2023**

YAPTIRIM

1.500.000 TL idari para cezası

KARARIN ÖZETİ

Dijital oyun ve eğlence platformunun kullandığı bir uygulamadaki güvenlik açığı saldırgan tarafından iki ayrı kez kullanılmış; ilk saldırıda platformun veri tabanına yetkisiz erişim sağlanmış, ikinci saldırıda ise veri tabanındaki veriler sistem dışına aktarılmıştır. Saldırganın bir forum sitesinde yaklaşık 69 milyon mevcut ve eski kullanıcıya ait verileri ve platformun kaynak kodlarını satışa çıkarması üzerine veri sorumlusu ihlalden haberdar olmuştur. Türkiye'de ikamet eden 90.182 kişiye ait kullanıcı adı, isim, e-posta adresi, doğum tarihi, cinsiyet, ülke, IP adresi ve platforma ilişkin bilgiler ihlalden etkilenmiştir. İlk aşamada şifrelerin de etkilenmiş olabileceği değerlendirilmişse de adli bilişim incelemesi ve elde edilen örnekler sonucunda şifre verilerinin ele geçirilmediği sonucuna ulaşılmıştır. Etkilenen kişiler arasında çocukların da bulunması ve verilerin satışa çıkarılması nedeniyle Kurul, ihlalin ilgili kişiler bakımından yüksek risk taşıdığını değerlendirmiştir.

Kurul, ihlalin veri sorumlusunun kendi sistem ve bilgi güvenliği ekipleri tarafından tespit edilememesini, kullanıcı işlem hareketlerinin düzenli olarak izlenmesi ve kişisel veri güvenliğinin takibi bakımından eksiklik bulunduğunun göstergesi olarak değerlendirmiştir. Veri sorumlusunun ihlal öncesinde ve sonrasında kişisel veri içeren sistemlerine yönelik sızma testi yaptırmadığını beyan etmesi nedeniyle güvenlik açığının zamanında tespit edilip giderilemediği; ayrıca aynı açığın farklı tarihlerde ikinci kez kullanılabilmesinin, kişisel veri güvenliğinin uygun aralıklarla izlenmediğini ve güvenlik açıklarının mümkün olduğunca hızlı şekilde raporlanmasına yönelik düzenin yeterli olmadığını gösterdiği sonucuna ulaşılmıştır.

Kurul ayrıca yama yönetimi politikasının ancak ihlal sonrasında uygulanmaya başlanmasını önemli bir güvenlik eksikliği olarak değerlendirmiştir. Düzenli zafiyet taraması ve sızma testlerinin yapılmaması, sistem ve kullanıcı hareketlerinin yeterince izlenmemesi, aynı güvenlik açığının ikinci kez kullanılmasının engellenememesi ve yama yönetiminin zamanında uygulanmaması birlikte değerlendirilerek veri sorumlusunun KVKK madde 12/1 kapsamındaki gerekli teknik ve idari tedbirleri almadığı sonucuna varılmış; KVKK madde 18/1-(b) uyarınca 1.500.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 24

YAZILIM / TEKNOLOJI

Yazılım ve teknoloji odaklı girişim yatırımları ve geliştirme faaliyetleri yürüten veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/790** Tarih **16.05.2024**

YAPTIRIM

Toplam 350.000 TL idari para cezası 250.000 TL: gerekli teknik ve idari tedbirlerin alınmaması 100.000 TL: veri ihlalinin ilgili kişilere bildirilmemesi

KARARIN ÖZETİ

Veri sorumlusunun, farklı lokasyonlarda kişiye özel çalışma alanı sunan mobil uygulamasına ve bu uygulamanın veri tabanına yetkisiz erişim sağlanmıştır. İhlal tarihinde uygulamada 7.823 kullanıcı kaydı bulunduğu; erişime konu verilerin ad-soyad, e-posta adresi ve telefon numarası olduğu belirlenmiştir. Yetkisiz kişiler veri tabanı şifresine ulaşmış, ancak bu şifreye hangi yöntemle erişildiği kesin olarak tespit edilememiştir. Uygulamadaki bazı lokasyon ve görsel bilgiler değiştirilmiş olmakla birlikte kişisel verilerin bütünlüğünün bozulduğuna veya verilerin kaybedildiğine ilişkin bir tespit yapılmamıştır.

Kurul, ihlal sonrasında parola politikasının değiştirilmiş olmasını ve tüm veri tabanı alanlarında yeterli loglama altyapısının bulunmaması nedeniyle saldırının kaynağının belirlenememesini, parola güvenliği ile erişim kayıtlarının tutulması ve kişisel veri güvenliğinin takibi bakımından önemli eksiklikler olarak değerlendirmiştir. Veri sorumlusunun da ihlalin, güvenlik tedbirleri henüz yeterli seviyeye ulaşmadan gerçekleştiğini belirtmesi dikkate alınarak KVKK madde 12/1 kapsamındaki yükümlülüklerin yerine getirilmediği sonucuna varılmış ve 250.000 TL idari para cezası uygulanmıştır.

Veri sorumlusu, kişisel verilerde değişiklik veya kayıp meydana gelmediği ve veri kopyalandığına ilişkin bulgu bulunmadığı gerekçesiyle ilgili kişilere ihlal bildirimi yapmamıştır. Kurul ise veri ihlalinin yalnızca verilerin bütünlüğünün bozulmasıyla sınırlı olmadığını, gizlilik ve erişilebilirliğin ihlal edilmesinin de veri ihlali oluşturabileceğini vurgulamış; bu nedenle ilgili kişilere bildirim yapılmamasını KVKK madde 12/5'e aykırı bularak ayrıca 100.000 TL idari para cezası uygulanmasına karar vermiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 25

MEDYA / BASIN

Yerel bir basın organının seçim anketi sonuçlarına ilişkin verileri internet sitesinde paylaşmasına ilişkin ihbar

Karar No **2024/275** Tarih **22.02.2024**

YAPTIRIM

40.179 TL idari para cezası Ayrıca, veri sorumlusuna, aydınlatma ve açık rıza süreçlerinin mevzuata uygun hâle getirilmesi ve hukuka aykırı veri işlemeyi önlemeye yönelik gerekli tedbirlerin alınması gerektiği hatırlatılmıştır.

KARARIN ÖZETİ

Yerel bir basın organı tarafından gerçekleştirilen seçim anketinin sonuçları internet sitesinde yayımlanmıştır. Veri sorumlusu; katılımcıların ad-soyad ve telefon bilgilerinin açık şekilde tutulmadığını, bu bilgilerin maskelendiğini ve bu nedenle kişilerin kimliğinin belirlenemeyeceğini savunmuştur. Ancak yayımlanan tabloda isimlerin ilk harflerine, telefon numaralarının bir bölümüne ve bazı kayıtlar bakımından mahalle bilgisine yer verilmesi nedeniyle, bu verilerin başka bilgilerle birlikte değerlendirildiğinde ilgili kişilerin kimliğinin belirlenmesine imkân verebileceği değerlendirilmiştir.

Kurul, uygulanan maskelemenin anonimleştirme için yeterli olmadığını vurgulamıştır. Bir verinin anonim sayılabilmesi için başka verilerle eşleştirilse dahi belirli veya belirlenebilir bir kişiyle ilişkilendirilememesi gerekir. Somut olayda telefon numarasının yalnızca bir bölümünün gizlenmesi ve buna isim baş harfleri ile mahalle bilgisinin eklenmesi, özellikle ankete katıldığı bilinen kişiler bakımından yeniden kimliklendirme riskini ortadan kaldırmamıştır. Bu nedenle yayımlanan bilgilerin kişisel veri niteliğini koruduğu sonucuna varılmıştır.

Anketin kişilerin oy tercihleri ve siyasi yönelimleri hakkında bilgi içermesi nedeniyle ayrıca özel nitelikli kişisel veri işlendiği kabul edilmiştir. Kurul, bu verilerin işlenmesi için geçerli bir hukuki sebep bulunmadığını ve katılımcılara gönderilen metnin de belirli bir konuya ilişkin, bilgilendirmeye dayalı ve özgür iradeyle açıklanmış geçerli bir açık rıza niteliği taşımadığını değerlendirmiştir. Bu nedenle siyasi görüş verilerinin herkese açık biçimde yayımlanması hukuka aykırı bulunmuş ve gerekli teknik ve idari tedbirlerin alınmaması sebebiyle 40.179 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 26

PERAKENDE / HAZIR GIYIM

Hazır giyim ve tekstil ürünlerinin perakende satışı gerçekleştiren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/756** Tarih **09.05.2024**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Hazır giyim ve tekstil ürünlerinin perakende satışını gerçekleştiren veri sorumlusunun deposunda, paketleme personelinin sehven yaptığı hata sonucunda bir müşteriye ait kargo ve sevkiyat faturası başka bir müşterinin siparişiyle eşleştirilmiş ve üçüncü kişiye teslim edilmiştir. Böylece ilgili kişinin ad-soyad, adres, cep telefonu numarası, e-posta adresi ve sipariş bilgileri üçüncü kişinin erişimine açılmıştır. İhlalin sistemsel bir güvenlik açığından değil, paketleme sürecindeki tekil bir insan hatasından kaynaklandığı ve yalnızca bir müşteriyi etkilediği tespit edilmiştir.

Olay, yanlış kargonun ulaştığı müşterinin siparişinin kendisine ulaşmadığını bildirmesi üzerine başlatılan iç inceleme sonucunda ortaya çıkarılmış; paketleme alanı ve kamera kayıtları incelenerek ihlalin nedeni belirlenmiştir. Veri sorumlusu, ihlalin tespit edilmesinin ardından ilgili kişiyle gecikmeksizin iletişime geçmiş ve hem telefon hem de e-posta yoluyla bilgilendirme yapmıştır. İlgili kişi de olay nedeniyle herhangi bir sipariş veya hak kaybına uğramadığını bildirmiştir.

Kurul; ihlalin yalnızca bir kişiyi etkilemesini, veri kategorilerinin sınırlı olmasını, olayın sistemsel bir zafiyetten değil insan hatasından kaynaklanmasını, ilgili kişiye bildirim yapılmasını ve ihlalin ilgili kişi üzerinde olumsuz sonuç doğurma riskinin düşük olmasını birlikte değerlendirmiştir. Bu nedenle veri sorumlusu hakkında KVKK m. 12 kapsamında ayrıca bir yaptırım veya işlem uygulanmasını gerektiren bir durum bulunmadığı sonucuna varmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz:

KARAR 27

EĞITIM

Bir Üniversite tarafından parmak izi verilerinin işlenmesi suretiyle devamsızlık takibi uygulamasına ilişkin şikayet üzerine ve resen yürütülen inceleme

Karar No **2024/197** Tarih **08.02.2024**

YAPTIRIM

Üniversite bünyesinde sorumlu kişi/kişiler hakkında disiplin hükümleri çerçevesinde işlem yapılması ve sonucunun Kurula bildirilmesi talimatlandırılmıştır. Ayrıca parmak iziyle yoklama uygulamasının derhâl durdurulması, mevcut biyometrik verilerin ivedilikle imha edilmesi, varsa üçüncü kişilere aktarılan verilerin de imhasının sağlanması ve ilgili kişi başvurularının süresinde ve gerekçeli biçimde cevaplandırılması yönünde talimat ve hatırlatmalarda bulunulmuştur.

KARARIN ÖZETİ

Üniversitede ders devamlılığının takibi amacıyla öğrencilerin parmak izi verileri kullanılmaya başlanmış; bazı fakültelerde bu sistemin yanında klasik imza yöntemi de uygulanmaya devam etmiştir. Üniversite, parmak iziyle yoklama sisteminin devamsızlığın daha sağlıklı takip edilmesi ve öğrencilerin birbirleri yerine imza atmasının önlenmesi amacıyla kurulduğunu, açık rıza vermek istemeyen öğrenciler için manuel yoklama seçeneğinin bulunduğunu savunmuştur. Buna karşılık Kurul, parmak izi verisinin biyometrik ve dolayısıyla özel nitelikli kişisel veri olduğunu ve bu tür bir verinin işlenmesinde yalnızca açık rızanın varlığının yeterli olmadığını değerlendirmiştir.

Kurul'un esas değerlendirmesi ölçülülük ilkesi üzerinde yoğunlaşmıştır. İlgili kişiden açık rıza alınmış olsa dahi, ders devamlılığının takibi gibi bir amaç için daha az müdahaleci alternatif yöntemler mevcutken biyometrik veri işlenmesinin gerekli ve ölçülü kabul edilemeyeceği belirtilmiştir. Kurul ayrıca açık rızanın, gereğinden fazla veri toplanmasını meşrulaştırmayacağını; kişisel verilerin yalnızca amaç için gerekli olduğu ölçüde işlenmesi gerektiğini vurgulamıştır. Bu nedenle parmak iziyle yoklama uygulamasının hem özel nitelikli kişisel verilerin işlenme şartları hem de "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi bakımından hukuka aykırı olduğu sonucuna ulaşılmıştır.

Kurul, biyometrik verilerin işlenmesine dayalı yoklama sisteminin ivedilikle sona erdirilmesine, yoklamanın biyometrik veri kullanmayan alternatif yöntemlerle yapılmasına ve bugüne kadar toplanan parmak izi verilerinin mevzuata uygun şekilde silinmesi/yok edilmesine karar vermiştir. Verilerin üçüncü kişilerle paylaşılmış olması hâlinde imha işlemlerinin bu kişilere de bildirilmesi gerektiği belirtilmiştir. Ayrıca öğrencinin başvurusuna süresinde cevap verildiğinin kanıtlanamaması nedeniyle, KVKK kapsamındaki başvuruların etkin, hukuka ve dürüstlük kuralına uygun, gerekçeli ve süresi içinde sonuçlandırılması gerektiği üniversiteye hatırlatılmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 28

MEDYA / BASIN

İlgili kişiler hakkında bir gazetede yayımlanan ve halen söz konusu gazetenin arşiv kayıtlarında yer alan bir habere ilişkin şikâyet

Karar No **2023/2185** Tarih **28.12.2023**

YAPTIRIM

Gazete arşivinden haberin kaldırılması yönünden yapılacak işlem bulunmadığına karar verilmiş; ilgili kişilerin unutulma hakkı taleplerini öncelikle arama motorları nezdinde ileri sürmeleri gerektiği belirtilmiştir. Ayrıca veri sorumlusuna, KVKK kapsamındaki başvuruların süresinde ve gerekçeli şekilde cevaplandırılması gerektiği hatırlatılmıştır.

KARARIN ÖZETİ

İlgili kişiler, 2001 yılında yayımlanan bir haberin gazetenin internet arşivinde hâlen erişilebilir olduğunu ve ad-soyadlarıyla arama yapıldığında haberin üst sıralarda çıktığını belirterek, aradan uzun süre geçmiş olması ve konunun artık kamu yararı taşımadığı gerekçesiyle haberin kaldırılmasını talep etmiştir. Gazete ise söz konusu içeriğin basın ve ifade özgürlüğü kapsamında yayımlandığını, haberin görünür gerçekliğe uygun olduğunu ve arşivden tamamen kaldırılmasının basın özgürlüğüne müdahale oluşturacağını savunmuştur.

Kurul, somut olayda basın özgürlüğü ile kişisel verilerin korunmasını isteme hakkının karşı karşıya geldiğini ve bu iki menfaat arasında denge kurulması gerektiğini vurgulamıştır. Bu dengelemede özellikle kamu yararı, haberin gerçekliği ve güncelliği ile haberin içeriği ve sunuluş biçimi arasındaki denge gibi ölçütlerin dikkate alınması gerektiğini belirtmiştir. Somut olayda, haber kapsamında gerçekleştirilen veri işleme faaliyetinin ifade özgürlüğünün bir görünümü olan basın hürriyeti kapsamında KVKK m. 28/1-(c) istisnasına girdiği değerlendirilmiş ve haberin gazete arşivinden kaldırılması yönünden KVKK kapsamında işlem yapılmasına gerek olmadığı sonucuna ulaşılmıştır.

Kurul ayrıca, ilgili kişilerin asıl talebinin ad-soyadlarıyla yapılan internet aramalarında söz konusu içeriğin görünürlüğünün sona erdirilmesi olduğunu dikkate alarak, bu talebin unutulma hakkı kapsamında arama motorları tarafından değerlendirilmesi gerektiğini belirtmiştir. Bu nedenle ilgili kişilerin öncelikle arama motorlarına başvurması ve KVKK madde 13 ve 14 kapsamındaki başvuru yollarını tüketmesi gerektiği ifade edilmiştir. Öte yandan, ilgili kişilerin gazeteye yaptığı KVKK başvurusunun süresi içinde cevaplandırılmamış olması nedeniyle, veri sorumlusuna başvuruların etkin, hukuka ve dürüstlük kuralına uygun, gerekçeli ve süresi içinde sonuçlandırılması gerektiği hatırlatılmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 29

FINANS / MUHASEBE

Finans ve muhasebe alanında faaliyet gösteren uluslararası bir meslek kuruluşu olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/728** Tarih **09.05.2024**

YAPTIRIM

Toplam 1.000.000 TL idari para cezası 750.000 TL: gerekli teknik ve idari tedbirlerin alınmaması 250.000 TL: veri ihlalinin Kurul'a 72 saat içinde bildirilmemesi

KARARIN ÖZETİ

Uluslararası bir meslek kuruluşunda görev yapan çalışan, kurumun Başkanı ve CEO'sundan gelmiş izlenimi veren bir phishing e-postasına yanıt vererek Avrupa'daki üyelere ait listeyi saldırganın harici e-posta adresine göndermiştir. İhlal kapsamında 217 Türk üyeye ait ad-soyad, üyelik numarası ve bazı kişiler bakımından iş veya kişisel e-posta adresleri üçüncü kişinin eline geçmiştir. Yapılan teknik incelemede kurumun e-posta veya bilgi sistemlerinin doğrudan ele geçirildiğine ilişkin bir bulguya rastlanmamış; olayın çalışan üzerinden gerçekleştirilen sosyal mühendislik saldırısından kaynaklandığı anlaşılmıştır. Kurul, ihlal edilen verilerin niteliği ve saldırının gerçekleşme biçimi nedeniyle ilgili kişiler bakımından olumsuz sonuç doğurma riskini yüksek değerlendirmiştir.

Kurul, veri sorumlusunun ihlal sonrasında ağ ve güvenlik duvarı kontrollerini sıklaştırması, Office 365 üzerindeki şüpheli e-posta incelemelerini artırması, posta kutusu erişim yetkilerini gözden geçirmesi, günlük ve canlı e-posta/oturum açma incelemeleri yapması ve çok faktörlü doğrulama kontrollerini artırması gibi tedbirleri devreye aldığını dikkate almıştır. Ancak bu önlemlerin önemli bir kısmının ihlalden sonra uygulanmaya başlanması, veri sorumlusunun phishing ve e-posta güvenliği risklerini önceden yeterince öngörmediği ve azaltmadığı yönünde değerlendirilmiştir. Bu nedenle mevcut risklerin belirlenmesi ve e-posta güvenlik sistemlerinin daha sıkı yapılandırılması bakımından eksiklik bulunduğu sonucuna varılmıştır.

Ayrıca çalışanlara kişisel veri güvenliği ve siber tehditler konusunda eğitimler verilmiş olmasına rağmen, çalışanın gönderen adresindeki ve mesaj içeriğindeki farklılıkları sorgulamadan ve ek bir doğrulama yapmadan üye listesini dışarıya göndermesi, Kurul tarafından eğitim ve farkındalık çalışmalarının uygulamada yeterince içselleştirilmediğinin göstergesi olarak değerlendirilmiştir. Bu kapsamda veri sorumlusunun çalışan farkındalığı, sosyal mühendislik riskleri ve veri paylaşım süreçlerindeki teyit mekanizmaları bakımından yeterli idari tedbirleri almadığı sonucuna varılarak 750.000 TL idari para cezası uygulanmıştır. Buna ek olarak, veri sorumlusunun ihlali öğrendikten sonra Kurul'un 2019/10 sayılı Kararı ile belirlenen 72 saatlik süre içerisinde bildirim yapmadığı tespit edilmiştir. Bu nedenle KVKK madde 12/5 kapsamındaki bildirim yükümlülüğünün de ihlal edildiği değerlendirilmiş ve ayrıca 250.000 TL idari para cezası verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 30

OTOMOTİV

Otomotiv sektöründe faaliyet gösteren bir yan sanayi üretim firması olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/415** Tarih **06.03.2024**

YAPTIRIM

430.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusunun Fransa'da bulunan sunucularına yönelik LockBit fidye yazılımı saldırısı, Fransa ve Türkiye sistemleri arasındaki bağlantı üzerinden Türkiye'de bulunan 8 sunucuya da yayılmıştır. İhlalden çalışanlar, müşteriler ve kullanıcılar olmak üzere toplam 43 kişi etkilenmiş; işlem güvenliği, finans ve pazarlama verileri ihlale konu olmuştur. Kayıt sayısının 100.000'i aşabileceği belirtilmiş, olay sonrasında veriler yedeklerden geri yüklenmiş ve ilgili kişilere bildirim yapılmıştır.

Kurul, saldırının Türkiye'deki sistemlere kadar yayılmasını özellikle ağ bileşenleri arasındaki erişimin yeterince sınırlandırılmaması ve ağın uygun biçimde segmentlere ayrılmaması ile ilişkilendirmiştir. Fransa'daki zararlı yazılımın network üzerinden Türkiye sistemlerine ulaşabilmesi, veri sorumlusunun ağ mimarisi üzerinde yeterli kontrol sağlamadığının göstergesi olarak değerlendirilmiştir. Bu kapsamda, kişisel veri içeren sistemlerin diğer ağ kaynaklarından ayrıştırılması ve erişimlerin yalnızca gerekli alanlarla sınırlandırılması gerektiği vurgulanmıştır.

Kurul ayrıca veri sorumlusunun ihlal öncesinde sızma testi yaptırmadığını ve sistemlerin düzenli güvenlik taramalarına tabi tutulduğunu gösteren yeterli rapor sunamadığını dikkate almıştır. Sistemlerin yapılandırmasının düzenli olarak gözden geçirilmesi, zafiyet taraması ve sızma testleriyle olası açıkların tespit edilmesi ve EDR gibi uç nokta tehdit algılama ve müdahale çözümlerinin kullanılması gerektiği belirtilmiştir. Ağ segmentasyonu, sistem takibi, zafiyet yönetimi ve saldırı tespit tedbirlerindeki eksiklikler birlikte değerlendirilerek KVKK madde 12 kapsamında gerekli teknik ve idari önlemlerin alınmadığı sonucuna varılmış ve 430.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 31

TARIM MAKINELERI / ÜRETIM

Tarım makineleri, traktör ve tarımsal ekipman üretimi ile ticareti alanında faaliyet gösteren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/413** Tarih **06.03.2024**

YAPTIRIM

150.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusunun bağlı bulunduğu yurt dışındaki şirketin sistemlerine yönelik fidye yazılımı saldırısı, ortak sunucu altyapısı nedeniyle Türkiye'deki veri sorumlusunun sistemlerini de etkilemiştir. Saldırganların bazı verileri dışarı aktardığı ve dark web üzerinde örneklerini paylaştığı anlaşılmıştır. İhlalden 56 çalışan etkilenmiş; kimlik, iletişim ve özlük verilerinin yanı sıra bazı çalışanlara ait kaza raporları ve sağlık bilgileri de ihlale konu olmuştur. Kurul, kişisel verilerin hem gizliliğinin hem de erişilebilirliğinin etkilendiğini dikkate almıştır.

Kurul, saldırının çok faktörlü kimlik doğrulama kullanılması hâlinde engellenebilecek nitelikte olduğunu, ancak MFA'nın ihlal sonrasında etkinleştirilmesinin öngörüldüğünü tespit etmiştir. Benzer şekilde, sunuculardaki bilinen açıkları gidermeye yönelik yama ve güncellemelerin ihlal sonrasında yapılması ile verilerin dışarı sızdırılması, yama yönetimi ve kişisel veri güvenliğinin takibi bakımından önemli eksiklikler olarak değerlendirilmiştir.

Ayrıca farklı veri sorumlularının ortak sunucu sistemi kullanması nedeniyle ihlalin birden fazla veri sorumlusuna yayılabilmesi, ağ bileşenleri arasında yeterli ayrıştırma ve erişim sınırlandırması yapılmadığını göstermiştir. Kurul, bu yapının hem teknik hem de idari eksiklik oluşturduğunu değerlendirerek KVKK madde 12 kapsamında gerekli tedbirlerin alınmadığı sonucuna varmış ve 150.000 TL idari para cezası uygulamıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 32

ONLINE YEMEK / TESLIMAT

Online yemek siparişi, restoran entegrasyonu ve teslimat/kurye hizmetleri veren veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2024/133** Tarih **25.01.2024**

YAPTIRIM

250.000 TL idari para cezası

KARARIN ÖZETİ

Online yemek siparişi, restoran entegrasyonu ve kurye hizmetleri sunan veri sorumlusunun veri tabanına gerçekleştirilen siber saldırı sonucunda sistemdeki veriler silinmiş ve saldırganlar tarafından ele geçirilmiş, ardından veri sorumlusundan fidye talep edilmiştir. İhlalden 1.362 kullanıcıya ait ad-soyad, telefon numarası, adres ve e-posta bilgileri etkilenmiştir. Veri sorumlusu saldırının kesin kaynağını belirleyememekle birlikte, USOM'a yaptığı bildirimde olayın DoS/DDoS saldırısı niteliğinde olduğunu; yetkisiz erişime yönetim paneli şifresinin tarayıcıda kayıtlı tutulmasının veya phpMyAdmin üzerinden veri tabanına erişimin belirli IP adresleriyle sınırlandırılmamış olmasının yol açmış olabileceğini değerlendirmiştir.

Kurul, yönetim paneli şifresinin tarayıcıda saklanmasını parola güvenliği bakımından gereken dikkat ve özenin gösterilmediğinin göstergesi olarak değerlendirmiştir. Ayrıca veri tabanı yönetim yazılımına erişimin belirli IP adresleriyle sınırlandırılmamış olmasının yetkisiz erişime imkân verdiğini ve bu konuda gerekli tedbirlerin alınmadığını tespit etmiştir.

Kurul, Kişisel Veri Güvenliği Rehberi'nde veri güvenliği tedbirlerinin her zaman yüksek maliyet gerektirmeyebileceğine; bazı önlemlerin masrafsız, düşük maliyetli veya mevcut sistemler üzerinden uygulanabilir olabileceğine dikkat çekmiştir. Bu kapsamda söz konusu iki güvenlik eksikliği nedeniyle KVKK madde 12/1 kapsamında gerekli teknik ve idari tedbirlerin alınmadığı sonucuna varılarak 250.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 33

ENDÜSTRIYEL ÜRETIM / MUTFAK EKIPMANLARI

Endüstriyel mutfak ekipmanları üretimi yapan veri sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2023/1675** Tarih **28.09.2023**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

İnsan Kaynakları Departmanı tarafından kullanılan uygulamada adres güncelleme bildirimi yapılırken, personelin bireysel gönderim menüsü yerine sehven toplu gönderim menüsünü kullanması sonucu 1.522 çalışana ait ad-soyad, T.C. kimlik numarası ve adres bilgileri 1.589 çalışana gönderilmiştir. İhlal, çalışanlardan gelen geri bildirim üzerine aynı gün tespit edilmiş; etkilenen çalışanlara bildirim yapılmıştır.

Kurul, insan hatasının bilgi güvenliği bakımından önemli bir risk olduğunu ve sistem tasarımlarında bu riski azaltacak tedbirlerin dikkate alınması gerektiğini belirtmiştir. Bununla birlikte, somut olayda bireysel ve toplu gönderim menülerinin aynı sekme altında ve benzer tasarlanmış olması nedeniyle hatanın anlaşılabilir nitelikte olduğu; ayrıca bu riskin yazılım geliştirme aşamasında kolaylıkla öngörülemeyebileceği değerlendirilmiştir. İhlal sonrasında iki gönderim türünün farklı sekmelere ayrılması için yazılım geliştiricisine talepte bulunulması da olumlu karşılanmıştır.

Kurul ayrıca, İK çalışanlarına KVKK ve bilgi güvenliği eğitimleri verilmiş olmasını, gizlilik taahhütnameleri ve disiplin düzenlemelerinin mevcut bulunmasını, erişim kontrolü ve ağ güvenliği bakımından çeşitli teknik tedbirlerin uygulanmasını ve bunların belgelenmesini dikkate almıştır. İhlalin çalışan geri bildirimi üzerine aynı gün tespit edilmesi de kişisel veri güvenliğinin takip edildiğinin göstergesi olarak değerlendirilmiştir.

Bu unsurlar birlikte dikkate alınarak, olayın tekil bir insan hatasından kaynaklandığı ve veri sorumlusunun uygun düzeyde teknik ve idari tedbirler aldığı sonucuna ulaşılmış; KVKK madde 12/1 kapsamında bu aşamada yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 34

BILIŞIM / HOSTING HIZMETLERI

Bir hosting firması tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2023/412** Tarih **21.03.2023**

YAPTIRIM

350.000 TL idari para cezası

KARARIN ÖZETİ

Hosting hizmeti sunan veri sorumlusunun satış ve muhasebe yazılımındaki müşteri yönetim panelinde bulunan güvenlik açığından yararlanılarak ana sunucuya yetkisiz erişim sağlanmış ve veriler toplu şekilde Almanya merkezli bir IP adresine aktarılmıştır. İhlalden çalışan, müşteri ve kullanıcı olmak üzere 31.179 kişi etkilenmiş; kimlik, iletişim, müşteri işlem ve finans verilerinin yanı sıra hizmet detayları, bazı şifreleri içeren e-posta içerikleri, ".tr" alan adı kayıtlarına ilişkin belgeler ve kredi kartı bilgileri ihlale konu olmuştur. Verilerin dark web üzerinde yayımlanması ve veri kapsamının genişliği nedeniyle Kurul, ihlalin ilgili kişiler üzerinde olumsuz etki doğurabileceğini değerlendirmiştir.

Kurul, veri sızıntısının yaklaşık altı ay sonra ve bir müşterinin bildirimi üzerine fark edilmesini, sistemlerin yeterince izlenmediğinin göstergesi olarak değerlendirmiştir. Ayrıca ihlal öncesinde saldırı tespit sistemlerinin bulunmaması, toplu veri indirmeyi engelleyen bir mekanizmanın olmaması ve loglarda 3.027 kredi kartı bilgisinin açık şekilde tutulması, veri güvenliği, maskeleme ve veri minimizasyonu bakımından önemli eksiklikler olarak görülmüştür.

İhlal sonrasında iki faktörlü doğrulama, tek kullanımlık SMS ile giriş ve daha güçlü parola politikası uygulanmaya başlanması da bu tedbirlerin ihlal öncesinde yeterli düzeyde bulunmadığını göstermiştir. Kurul, bu eksiklikleri birlikte değerlendirerek veri sorumlusunun KVKK madde 12/1 kapsamındaki yükümlülüklerini yerine getirmediği sonucuna varmış ve 350.000 TL idari para cezası uygulamıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 35

MODA / TEKSTİL

Moda tekstil faaliyeti yürüten Veri Sorumlusunun veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2022/1407** Tarih **28.12.2022**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Veri sorumlusunun bir müşterisi, kimliği belirsiz kişiler tarafından aranarak teslim alınmayan bir kargo nedeniyle ücret ve zarar doğduğu, ödeme yapılmaması hâlinde icra takibi başlatılacağı söylenmek suretiyle dolandırılmaya çalışılmıştır. Olay müşterinin aynı gün veri sorumlusuna bildirimde bulunması üzerine öğrenilmiş; veri sorumlusu ihlal müdahale planını devreye almış, internet sitesi ve sosyal medya hesapları üzerinden müşterilerini uyarmış ve Cumhuriyet Başsavcılığı'na suç duyurusunda bulunmuştur. İlk bildirimde yalnızca bir müşterinin etkilendiği belirtilmişse de Kurul, savcılığa sunulan bilgilerden daha fazla müşterinin benzer şekilde aranmış olabileceğini değerlendirmiştir.

Kurul, dolandırıcılık girişiminin gerçekleştirilebilmesi için müşterilerin telefon numarası ile veri sorumlusundan alışveriş yaptığı bilgisinin ele geçirilmesinin yeterli olduğunu; ancak bu verilerin mutlaka veri sorumlusunun sistemlerinden sızdığının ortaya konulamadığını dikkate almıştır. Verilerin e-ticaret platformları, kargo şirketleri veya finans kuruluşları gibi başka veri sorumlularının sistemlerinden de elde edilmiş olabileceği; ayrıca veri sorumlusunun mali büyüklüğü ve faaliyet alanı dikkate alındığında ihlalin kapsamının genişleme ihtimalinin düşük olduğu değerlendirilmiştir. Olay sonrasında yapılan genel uyarılar ve müşteriler bakımından somut bir zarar bildiriminin bulunmaması da dikkate alınmıştır.

Kurul ayrıca, veri sorumlusunun ihlal öncesinde sızma testleri yaptırmış olmasını, ERP sistemine üç katmanlı kimlik doğrulama ile erişim sağlamasını, kişisel veri ihlali müdahale planının bulunmasını, veri paylaşılan taraflarla veri güvenliği hükümleri içeren sözleşmeler akdetmesini ve çalışanlarla gizlilik taahhütnameleri imzalamasını makul teknik ve idari tedbirler olarak değerlendirmiştir.

Bu hususlar birlikte dikkate alınarak, veri sızıntısının doğrudan veri sorumlusundan kaynaklandığının ortaya konulamaması ve alınan teknik ve idari tedbirlerin yeterli bulunması nedeniyle KVKK madde 12/1 kapsamında bu aşamada yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 36

ÜRETIM / SANAYI

Bir sanayi şirketi olan veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2022/1375** Tarih **23.12.2022**

YAPTIRIM

Toplam 1.000.000 TL idari para cezası 800.000 TL: gerekli teknik ve idari tedbirlerin alınmaması 200.000 TL: veri ihlalinin Kurul'a geç bildirilmesi

KARARIN ÖZETİ

Veri sorumlusunun ABD'deki kuruluşunda bir çalışanın internetten indirdiği programı çalıştırması üzerine fidye yazılımı küresel altyapıya yayılmış ve 797 sunucudaki bazı dosyalar şifrelenmiştir. Türkiye bakımından 4.885 çalışan, müşteri ve tedarikçi ihlalden etkilenmiş; kimlik, iletişim ve finans bilgilerinin yanı sıra kimlik fotoğrafları, pasaport bilgileri ve 600 kişiye ait kan grubu bilgileri de ihlale konu olmuştur.

Kurul, ihlal öncesinde yapılan penetrasyon testinde acil, kritik ve yüksek seviyeli güvenlik açıkları tespit edilmiş olmasına rağmen bunların giderildiğinin belgelendirilememesini temel bir eksiklik olarak değerlendirmiştir. Buna ek olarak zayıf parola politikası, kullanıcı adı ve şifrelerin açık şekilde saklanması, gereğinden geniş erişim yetkileri, güncel olmayan sistemlerin kullanılması ve brute-force saldırılarına karşı yeterli koruma bulunmaması veri güvenliği bakımından önemli zafiyetler olarak görülmüştür. İhlalin bir çalışanın indirdiği uygulamayla başlaması ve fidye yazılımının tek bir cihazdan 797 sunucuya yayılabilmesi ise çalışan farkındalığı ile ağ segmentasyonu bakımından tedbirlerin yetersiz olduğunu göstermiştir.

Bu eksiklikler birlikte değerlendirilerek veri sorumlusunun KVKK madde 12/1 kapsamındaki gerekli teknik ve idari tedbirleri almadığı sonucuna varılmış ve 800.000 TL idari para cezası uygulanmıştır. Ayrıca veri ihlalinin tespitinden 23 gün sonra Kurul'a bildirilmesi, KVKK madde 12/5'teki "en kısa sürede bildirim" yükümlülüğüne aykırı bulunarak 200.000 TL daha idari para cezası verilmiş; toplam ceza 1.000.000 TL olmuştur.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 37

TEKNOLOJI

Bir Teknoloji Şirketi olan veri sorumlusu tarafından Kurula iletilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2022/1087** Tarih **07.10.2022**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Büyük miktarda kişisel veri işleyen teknoloji şirketine, kimliği belirsiz kişi veya kişiler tarafından şirket sistemlerindeki kişisel verilere erişildiği iddiasını içeren bir tehdit e-postası gönderilmiştir. Bunun üzerine veri sorumlusu iki bağımsız siber güvenlik firmasından destek alarak eş zamanlı analiz, sızma testi ve adli bilişim incelemeleri başlatmıştır. Yapılan incelemelerde, tehdit e-postasında örnek olarak sunulan verilerin şirket sistemlerindeki kişisel verilerle eşleşmediği ve fiilen bir kişisel veri sızıntısı yaşandığını gösteren herhangi bir bulguya ulaşılamadığı tespit edilmiştir.

Kurul, gerçekleştirilen testlerde yüksek seviyeli bazı güvenlik zafiyetleri bulunduğunu da dikkate almıştır. Bunlar arasında güvensiz veri tabanı kullanımı, hassas bilgilerin erişilebilir olması ve belirli bir DDoS açığı yer almakla birlikte, bu zafiyetlerin somut olayda kişisel verilerin yetkisiz kişilerce ele geçirildiğini gösteren bir ihlale yol açtığı ortaya konulamamıştır.

Veri sorumlusunun tehdidi öğrendikten sonra ivedilikle teknik inceleme başlatması, bağımsız uzman kuruluşlardan destek alması ve adli bilişim raporlarında kişisel veri ihlaline ilişkin herhangi bir bulguya rastlanmaması dikkate alınarak KVKK madde 12/1 kapsamında bu aşamada yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 38

TARIM / EMTIA TICARETI

Tarımsal emtia ticareti alanında faaliyet gösteren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2022/714** Tarih **21.07.2022**

YAPTIRIM

200.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusunun üst düzey yöneticisine ait e-posta hesabı oltalama, sosyal mühendislik veya benzeri bir yöntemle ele geçirilmiş; saldırganlar bu hesap üzerinden yaklaşık 1.000 kişiye yanıltıcı içerikli e-posta göndermeye çalışmıştır. E-postalarda borç/fatura izlenimi veren içerikler kullanılmış ve alıcılar zararlı yazılım barındıran bir siteye yönlendirilmiştir. İhlalden müşteriler, tedarikçiler, müşteri adayları ve çalışanlar etkilenmiş; ad-soyad, e-posta adresi ve unvan bilgilerinin yanı sıra, e-posta yazışmaları ve imza alanlarında bulunabilecek telefon ve adres gibi diğer kişisel verilerin de yetkisiz erişime maruz kalmış olabileceği değerlendirilmiştir.

Kurul, veri sorumlusunun ihlalden etkilenen kişi sayısını kesin olarak belirleyememesini, kişisel veriler üzerindeki kontrolün yeterince sağlanamadığının göstergesi olarak değerlendirmiştir. Ayrıca DLP çözümleri, gelişmiş/çok faktörlü kimlik doğrulama ile saldırı ve anomali tespit sistemlerinin ancak ihlal sonrasında devreye alınması, ihlal öncesinde uygun güvenlik seviyesinin sağlanmadığını göstermiştir. Şifre/Parola Yönetim Politikası'nda aynı parolanın farklı platformlarda kullanılmaması gerektiğine ilişkin yeterli düzenlemenin bulunmaması da parola güvenliği bakımından eksiklik olarak kabul edilmiştir.

İhlalin şirketin kendi güvenlik mekanizmalarıyla değil, bir müşterinin telefonla bildirimde bulunması üzerine fark edilmesi ve saldırganların ilgili e-posta hesabında 2–3 gün boyunca işlem yapabilmesi, erişim ve log kayıtlarının düzenli şekilde kontrol edilmediğini ve olağan dışı hareketlerin etkin biçimde izlenmediğini ortaya koymuştur. Bu hususlar birlikte değerlendirilerek veri sorumlusunun KVKK madde 12/1 kapsamındaki teknik ve idari tedbirleri yeterli düzeyde almadığı sonucuna varılmış ve 200.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 39

OTOMOTIV / ELEKTRONIK SISTEMLER

Otomotiv güvenlik ve elektronik sistemleri üretimi yapan veri sorumlusu tarafından Kurula intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2022/711** Tarih **21.07.2022**

YAPTIRIM

500.000 TL idari para cezası

KARARIN ÖZETİ

Veri sorumlusunun sistemlerine yönelik fidye yazılımı saldırısının, insan kaynakları yazılımına hizmet veren üçüncü taraf sağlayıcı için oluşturulmuş 2003 yılından beri kullanılan eski bir kullanıcı hesabının saldırganlarca ele geçirilmesiyle başladığı değerlendirilmiştir. Saldırganlar bu hesap üzerinden sisteme sızmış, ağ içerisinde ilerleyerek yönetici erişim bilgilerini ele geçirmiş ve son aşamada fidye yazılımını devreye alarak dosyaları şifrelemiş; bazı verileri de yayımlamıştır. İhlalden 660 kişi etkilenmiş; müşteri ve tedarikçi temsilcileri ile eski ve mevcut çalışanlara ait kimlik, iletişim ve özlük verilerinin yanı sıra bazı çalışanların kan grubu, Covid-19 bilgileri ve doktor raporları da ihlale konu olmuştur.

Kurul, saldırının hizmet sağlayıcıya tahsis edilmiş eski bir kullanıcı hesabı üzerinden başlamasını özellikle değerlendirmiş; veri sorumlusunun, hizmet aldığı veri işleyenin de kendisiyle en az aynı düzeyde veri güvenliği sağlamasını temin etmekle yükümlü olduğunu ve KVKK madde 12/2 uyarınca veri işleyenle birlikte sorumluluğunun devam ettiğini belirtmiştir.

Ayrıca saldırganların sisteme sızdıktan sonra ağ keşfi yapabilmesi, erişim bilgilerini ele geçirebilmesi ve diğer sunuculara yanal hareket edebilmesine rağmen bu faaliyetlerin veriler şifrelenene kadar tespit edilememesi, kişisel veri güvenliğinin takibi ve bilişim ağlarının düzenli izlenmesi bakımından önemli bir eksiklik olarak değerlendirilmiştir. Bu nedenlerle gerekli teknik ve idari tedbirlerin alınmadığı sonucuna varılarak veri sorumlusu hakkında 500.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 40

PERAKENDE / MAĞAZACILIK

Mağazacılık hizmeti veren veri sorumlusu tarafından Kurul'a intikal ettirilen veri ihlal bildirimine istinaden yürütülen inceleme

Karar No **2022/707** Tarih **21.07.2022**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

Veri sorumlusunun mobil e-ticaret sisteminde, yaklaşan kampanya öncesinde yapılan uygulama güncellemelerinde yaşanan bir hata nedeniyle, bazı müşterilerin kendi hesaplarına giriş yaptıklarında en son önbelleğe alınan (tedarikçi tarafından önbelleğe alınabilir olarak sunulmaması gereken) profil bilgilerini görüntülemesi sonucu başka kullanıcılara ait kişisel verilerin görüntülenmesi şeklinde veri ihlali meydana gelmiştir. İhlal kapsamında ad-soyad, telefon, e-posta ve bazı durumlarda maskelenmiş kart bilgileri etkilenmiş; kesin olarak 17 kişinin, teknik simülasyona göre ise en fazla 136 kişinin etkilenmiş olabileceği değerlendirilmiştir. Verilerin kamuya açık biçimde yayılmadığı ve ihlalin kapsamının sınırlı kaldığı tespit edilmiştir.

Kurul, ihlalin bir müşteri bildirimiyle kesinleşmiş olmasına rağmen, veri sorumlusunun teknik ekiplerinin bu bildirimden önce de sistemdeki performans ve kesinti problemini incelemekte olduğunu dikkate almıştır; bu husus Kişisel Veri Güvenliği Rehberi'nin "Veri İşleyenler ile İlişkilerin Yönetimi" başlığı kapsamında olumlu değerlendirilmiştir. Sorunun veri ihlaliyle bağlantısının anlaşılması üzerine sistemin kapatılması, tedarikçi nezdindeki hatalı konfigürasyonun düzeltilmesi ve etkilenen kişilere bildirim yapılması, Rehber'in "Kişisel Veri Güvenliğinin Takibi" başlığında vurgulanan ihlale gecikmeksizin müdahale edilmesi ilkesiyle uyumlu bulunmuştur. Ayrıca tedarikçinin kayıtlarında farklı kullanıcıları kesin olarak ayırt etmeye yarayan ayrıntıların uluslararası bilgi güvenliği standartları nedeniyle bulunmaması, Rehber'in "Mevcut Risk ve Tehditlerin Belirlenmesi" başlığında öngörülen ilkelere uygun şekilde işlenen verilerin bilgi güvenliği standartlarına uygun biçimde sınırlandırıldığını gösteren bir unsur olarak kabul edilmiştir.

Kurul; ihlalin kısa sürede giderilmesi, etkilenen kişi ve veri miktarının sınırlı olması, verilerin kamuoyuna ifşa edilmemesi, kötüye kullanım riskinin düşük bulunması ve veri sorumlusunun sistemleri denetleyerek hızlı aksiyon alması hususlarını birlikte değerlendirerek, KVKK madde 12/1 kapsamında bu aşamada yapılacak bir işlem bulunmadığına karar vermiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 41

İŞVEREN / ÖZEL SEKTÖR

İşveren tarafından işyerinde kamera vasıtasıyla görüntü ve ses kaydı alınması

Karar No **2023/2007** Tarih **30.11.2023**

YAPTIRIM

125.000 TL idari para cezası Ayrıca veri sorumlusuna, hukuka aykırı şekilde işlenen ses kayıtlarının imha edilmesi ve sonucun Kurul'a bildirilmesi yönünde talimat verilmiştir.

KARARIN ÖZETİ

Veri sorumlusu bünyesinde şoför olarak çalışan ilgili kişi, işyerindeki güvenlik kulübesinde kamera aracılığıyla görüntü ve ses kaydı alındığını, bu konuda kendisine bilgilendirme yapılmadığını ve kayıtların tarafı olduğu dava dosyasına sunulması üzerine kayıtların varlığından haberdar olduğunu ileri sürmüştür. Veri sorumlusu ise kameranın eski yönetim döneminde fiziksel güvenliği sağlamak ve çalışanlar ile ziyaretçiler arasında çıkabilecek olayları önlemek amacıyla kurulduğunu; ilgili kaydın, ilgili kişinin güvenlik kulübesinde yönetime ve çalışma arkadaşlarına küfür etmesi üzerine bir hakkın tesisi ve korunması amacıyla saklanarak adli mercilerle paylaşıldığını savunmuştur. Veri sorumlusu ayrıca, yönetim kurulunun değişmesinin ardından ses kaydı alan kameranın ses kaydı almayan bir kamerayla değiştirildiğini belirtmiştir.

Kurul, KVKK madde 5/2-(f) kapsamında meşru menfaat değerlendirmesi yaparken "söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi" ve "kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması" kriterlerini esas almıştır. Bu çerçevede görüntü kaydının güvenlik amacıyla bağdaşabileceğini ve bu amacı gerçekleştirmeye yeterli olduğunu; ancak aynı amaca ulaşmak için ayrıca ses kaydı alınmasının zorunlu olmadığını değerlendirmiştir. Görüntü kaydı güvenliği sağlamak bakımından yeterli olduğundan, ses verilerinin işlenmesi için KVKK madde 5 kapsamında geçerli bir hukuki sebep bulunmadığı sonucuna ulaşılmıştır.

Kurul ayrıca, hukuki dayanağı bulunmayan bir veri işleme faaliyeti bakımından aydınlatma yükümlülüğünün yerine getirilip getirilmediğinin ayrıca incelenmesine gerek görmemiştir. Veri sorumlusunun aydınlatma metinleri hazırladığı, tesis girişlerine astığı, kamera uyarı levhaları yerleştirdiği ve web sitesinde bilgilendirme yayımladığı belirtilmiş olmakla birlikte, Kurul bu KVK uyum tedbirlerini ses kaydı bakımından ayrıca değerlendirmemiştir. Ses kayıtlarının imha edildiği beyan edilmekle birlikte bu husus belgelendirilemediğinden veri sorumlusu, söz konusu verilerin imha edilmesi ve sonucundan Kurula bilgi verilmesi yönünde talimatlandırılmış; KVKK madde 12/1 kapsamındaki yükümlülüğün ihlali nedeniyle 125.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz

KARAR 42

BELEDİYE / KÜTÜPHANE HİZMETLERİ

Bir Belediyenin kütüphane üyelik uygulamasına ilişkin şikâyet

Karar No **2023/1863** Tarih **02.11.2023**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

İlgili kişi, belediyeye ait kütüphaneden yararlanabilmek için üyelik oluşturmasının zorunlu tutulduğunu, üyelik sırasında T.C. kimlik numarası, ad-soyadı, meslek/okul, e-posta adresi, cep telefonu ve doğum tarihi gibi kişisel verilerinin talep edildiğini ve yeterli aydınlatma yapılmadığını ileri sürmüştür. Belediye ise söz konusu verilerin kimlik doğrulama, rezervasyon sisteminin işletilmesi, öğrencilerin tespiti, kullanıcılarla iletişim kurulması ve kişinin 18 yaşından büyük olduğunun belirlenmesi gibi amaçlarla işlendiğini açıklamıştır.

Kurul, kütüphane hizmetinden yararlanmanın açık rıza verilmesi şartına bağlanmadığını; kişisel verilerin KVKK madde 5/2-(c)'deki sözleşmenin kurulması veya ifasıyla doğrudan ilgili olma ve madde 5/2-(e)'deki bir hakkın tesisi, kullanılması veya korunması için zorunlu olma şartlarına dayanılarak işlendiğini değerlendirmiştir. Kurul ayrıca, açık rızanın üyeliğin ve hizmetin bir koşulu olarak dayatılmasının açık rızayı sakatlayacağı ilkesini belirtmekle birlikte, somut olayda diğer işleme şartlarına dayanıldığından açık rızanın hizmet koşulu hâline getirildiği yönündeki iddia yerinde bulunmamıştır.

Aydınlatma yükümlülüğü bakımından ise bilgilendirmenin yalnızca yazılı değil, sözlü veya elektronik yollarla da yapılabileceği belirtilmiştir. Belediye, geçmişte görevli personel aracılığıyla sözlü bilgilendirme yaptığını, ancak bu uygulamaya son verilerek mevcut sistemde internet sitesi ve e-Devlet üzerinden üyelik kaydı ekranında aydınlatma metnine erişim sağlandığını tevsik etmiştir. İlgili kişinin kişisel verilerinin de imha tutanağıyla silindiği dikkate alınarak KVKK kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 43

GÜVENLIK HIZMETLERI / ALARM SISTEMLERI

Alarm ve görüntüleme sistemi hizmeti sunan veri sorumlusu tarafından ilgili kişinin telefon görüşmelerinin kaydedilmesi

Karar No **2023/1818** Tarih **26.10.2023**

YAPTIRIM

15.000 TL idari para cezası Ayrıca veri sorumlusuna, KVKK ve asgari unsurları içeren aydınlatmanın yapılması; katmanlı aydınlatma tercih edilmesi hâlinde ise ilgili kişilerin bu bilgilerin tamamına erişebileceği bir mecraya yönlendirilmesi ve 30 gün içinde Kurul'a bilgi verilmesi yönünde talimat verilmiştir.

KARARIN ÖZETİ

İlgili kişi, alarm ve görüntüleme hizmeti sunan veri sorumlusu ile yaptığı telefon görüşmelerinin bilgisi ve rızası dışında kaydedildiğini ileri sürmüştür. Veri sorumlusu ise taraflar arasındaki abonelik ilişkisinin yıllar içinde telefon görüşmeleriyle yenilendiğini ve değiştirildiğini; bu nedenle kayıtların sözleşme ilişkisinin içeriğinin, yapılan değişikliklerin ve tarafların haklarının ispatı bakımından gerekli olduğunu savunmuştur.

Kurul, hizmet sözleşmesinin özel bir şekle tabi olmadığını ve telefon görüşmesi kayıtlarının sözlü olarak gerçekleştirilen sözleşme değişikliklerinin ve sözleşmenin gereği gibi ifa edilip edilmediğinin ispatı bakımından önem taşıdığını değerlendirmiştir. Bu nedenle görüşme kayıtlarının KVKK madde 5/2-(e) ve (f) kapsamında, bir hakkın tesisi, kullanılması veya korunması ile veri sorumlusunun meşru menfaati hukuki sebeplerine dayanılarak işlenebileceği sonucuna ulaşılmış ve kayıtların alınması bakımından hukuka aykırılık tespit edilmemiştir.

Buna karşılık Kurul, ilgili kişiye yalnızca görüşmelerin kayıt altına alındığının bildirilmesini KVKK madde 10 kapsamında yeterli bir aydınlatma olarak görmemiştir. Aydınlatmanın KVKK ve ilgili Tebliğ'de öngörülen asgari unsurları içermesi veya katmanlı aydınlatma kullanılıyorsa ilgili kişinin bu bilgilere ulaşabileceği bir mecraya yönlendirilmesi gerektiği; geçmiş görüşmeler bakımından da usulüne uygun aydınlatma yapıldığının veri sorumlusu tarafından tevsik edilemediği değerlendirilmiştir.

Bu nedenle görüşmelerin kaydedilmesi bakımından işlem yapılmamış; aydınlatma yükümlülüğünün ihlali nedeniyle 15.000 TL idari para cezası uygulanmıştır. Ayrıca mevzuata uygun aydınlatma yapılması ve sonucundan 30 gün içinde Kurul'a bilgi verilmesi yönünde veri sorumlusu talimatlandırılmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 44

PERAKENDE / HAZIR GIYIM

İlgili Kişinin kişisel verilerinin veri sorumlusu giyim mağazasına ait internet sitesinde üçüncü kişilerin erişimine açılması

Karar No **2023/1796** Tarih **19.10.2023**

YAPTIRIM

200.000 TL idari para cezası

KARARIN ÖZETİ

İlgili kişi, giyim mağazasının internet sitesindeki hesabında yer alan ad-soyad, telefon, adres, üyelik ve sipariş bilgilerinin üçüncü kişiler tarafından görüntülenebildiğini, hatta başka bir kişinin hesabına girerek adres bilgisini değiştirip kendi adına sipariş verebildiğini tespit etmiştir. Veri sorumlusu, olayın kampanya dönemi öncesindeki teknik çalışmalar kapsamında kullanılan CDN/cache hizmetindeki bir konfigürasyon sorunundan kaynaklandığını ve bu hizmetin üçüncü taraf bir veri işleyen tarafından sağlandığını belirtmiştir. Yapılan incelemede sorunun, cache konfigürasyonunun gerçekleştirildiği cihazlardan yalnızca birinde meydana gelen teknik bir durumdan kaynaklandığı tespit edilmiştir. Veri sorumlusu, düzenli olarak her yıl sızma testi yaptırdığını ve ortaya çıkan bulguların titizlikle giderildiğini belirtmiş; olayın tespitinin ardından ilgili kişinin şifresini sıfırlayarak hesabını geçici olarak pasif duruma getirmiştir.

Kurul, veri işleyenden hizmet alınmasının veri sorumlusunun sorumluluğunu ortadan kaldırmadığını; KVKK madde 12/2 uyarınca veri sorumlusu ile veri işleyenin veri güvenliğinin sağlanmasından müştereken sorumlu olduğunu ve teknik/idari tedbirleri alma yükümlülüğünün sözleşmeyle tamamen veri işleyene devredilemeyeceğini vurgulamıştır. Kişisel Veri Güvenliği Rehberi'nin 3.5 "Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı" başlığında belirtildiği üzere, yeni sistemlerin tedariği veya mevcut sistemlerin iyileştirilmesinde güvenlik gereksinimlerinin göz önüne alınması ve uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılması gerekmektedir. Bu çerçevede veri sorumlusunun, veri işleyen eliyle yürütülen süreçleri denetlemek ve sistem değişiklikleri canlıya alınmadan önce yeterli testleri yapmak veya yaptırmakla yükümlü olduğu; somut olayda bu kontrollerin yeterli olmadığı değerlendirilmiştir.

İlgili kişinin kişisel verilerinin internet sitesi üzerinden sınırsız bir kitlenin erişimine açık hâle gelmesi, herhangi bir veri işleme şartına dayanmadığından veri sorumlusunun kişisel verilere hukuka aykırı erişimi önleme yükümlülüğünü ihlal ettiği sonucuna varılmıştır. Bu nedenle 200.000 TL idari para cezası uygulanmıştır. Veri sorumlusu, ilgili kişinin Başvuru Tebliği'nde belirtilen usule riayet etmediğini ve şirket sistemlerinde kayıtlı olmayan bir e-posta adresi kullandığını ileri sürerek başvurunun usulsüz olduğunu savunmuştur. Ancak Kurul, veri sorumlusunun başvurunun esasına ilişkin cevap vermiş olmasını dikkate alarak bu itirazı kabul etmemiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 45

SAĞLIK HIZMETLERI

İlgili kişinin Covid-19 test sonucunun tarafından veri kayıt sisteminde bulunan eski cep telefonu numarasına gönderilmesine ilişkin şikâyet

Karar No **2023/1787** Tarih **19.10.2023**

YAPTIRIM

30.000 TL idari para cezası Ayrıca ilgili kişinin güncel telefon numarasının veri kayıt sistemine işlenmesi, eski numaranın kayıtlardan çıkarılarak imha edilmesi ve sonucunun Kurula bildirilmesi yönünde veri sorumlusu talimatlandırılmıştır.

KARARIN ÖZETİ

İlgili kişi, üniversite kampüsünde yaptırdığı Covid-19 testinin sonucunun kendisine iletilmesi için güncel cep telefonu numarasını form aracılığıyla veri sorumlusuna bildirmiştir. Buna rağmen test sonucu, veri sorumlusunun sisteminde 2011 yılından kalma eski bir telefon numarasına, yani ilgili kişinin dayısına ait numaraya gönderilmiştir. Böylece ilgili kişinin sağlık verisi üçüncü bir kişinin erişimine açılmıştır. Veri sorumlusu, eski numaranın daha önce ilgili kişi tarafından verilmiş olduğunu ve ilgili kişinin bu numaranın artık kullanılmaması yönünde herhangi bir bildirimde bulunmadığını, test sonucunun kamu sağlığı açısından ivedilikle bildirilmesi gerektiğini ve testin negatif çıkması nedeniyle somut bir zarar doğmadığını savunmuştur. Veri sorumlusu ayrıca, ilgili kişinin kötü niyetli olarak haksız kazanç elde etme gayesiyle hareket ettiğini ve üstün kamu yararı gereğince kamu yararının kişinin özel yararından üstün olduğunu ileri sürmüştür.

Kurul, değerlendirmesini esas olarak KVKK madde 4'teki "doğru ve gerektiğinde güncel olma" ilkesi üzerinden yapmıştır. İlgili kişi tarafından test sonucu için açıkça yeni bir telefon numarası verilmişken, veri kayıt sistemindeki eski numaranın kullanılmaya devam edilmesi veri sorumlusunun güncellik yükümlülüğünü yerine getirmediğinin göstergesi olarak kabul edilmiştir. Kurul ayrıca, kişisel verilerin doğru ve güncel tutulmasının yalnızca veri sorumlusunun operasyonel menfaati bakımından değil, ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da önemli olduğunu; veri sorumlularının yanlış veya eski verilerin kullanılmasını önleyecek makul süreç ve kanalları oluşturması gerektiğini vurgulamıştır.

Sağlık verisinin özel nitelikli kişisel veri olması da olayın önemini artırmıştır. Tam metinde ayrıca özel nitelikli kişisel verilerin işlenmesinde 31/01/2018 tarihli ve 2018/10 sayılı Kurul kararının dikkate alınmasının şart olduğu ve KVKK madde 12/4 uyarınca veri sorumluları ile veri işleyen kişilerin öğrendikleri kişisel verileri KVKK hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacının dışında kullanamayacağı hükmüne atıf yapılmıştır. Kurul, veri sorumlusunun "eski numaranın daha önce ilgili kişi tarafından verilmiş olması" veya "test sonucunun negatif olması" yönündeki savunmalarını, güncellik yükümlülüğünü ortadan kaldıran unsurlar olarak kabul etmemiştir. Sonuç olarak, güncel telefon numarası mevcut olmasına rağmen eski numaraya test sonucu gönderilmesi KVKK madde 4/2-(b)'deki doğru ve gerektiğinde güncel olma ilkesine aykırı bulunmuş; bu aykırılık KVKK madde 12/1 kapsamındaki veri güvenliği yükümlülüğünün ihlali olarak değerlendirilerek 30.000 TL idari para cezası uygulanmıştır.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 46

ÇEVRIMIÇI SPOR VE ŞANS OYUNLARI

Bir çevrimiçi yasal spor ve şans oyunları platformu tarafından canlı maç yayını faaliyeti sunumunun ticari nitelikli ileti göndermek suretiyle açık rıza alınması şartına bağlanması

Karar No **2023/1610** Tarih **21.09.2023**

YAPTIRIM

250.000 TL idari para cezası Ayrıca veri sorumlusunun, canlı maç yayını hizmetinden yararlanmayı ticari ileti gönderimi amacıyla kişisel verilerin işlenmesine yönelik açık rıza verilmesi şartına bağlayan uygulamasına son vermesi ve sonucundan Kurul'a bilgi vermesi yönünde talimat verilmiştir.

KARARIN ÖZETİ

İlgili kişi, çevrimiçi spor ve şans oyunları platformunda canlı maç yayını hizmetinden yararlanabilmek için ticari elektronik ileti izni vermek zorunda bırakıldığını, Kurul'un 2019/206 ve 2021/389 sayılı kararları uyarınca hizmetin açık rıza ön şartına bağlanamayacağını ileri sürmüştür. Canlı yayın hizmetine erişim için üç şart belirlenmiştir: (i) üyelik, (ii) son 120 saat içinde veya son 14 gün içinde kupon oynama ve pozitif bakiye bulundurma, (iii) ticari elektronik ileti onayı verme. Veri sorumlusu, canlı yayın hizmetinin platformun temel hizmetlerinden biri olmadığını, ek bir fayda niteliğinde olduğunu ve talep edilen iznin KVKK kapsamında açık rıza değil, 6563 sayılı Kanun kapsamında ticari elektronik ileti onayı olduğunu savunmuştur. Bu kapsamda Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik madde 7/9 uyarınca ticari ileti onayının hizmet temini için ön şart olarak ileri sürülemeyeceği düzenlenmesine atıf yapmış; Ticaret Bakanlığı'na yaptığı bilgi edinme başvurusunda bu düzenlemenin yalnızca temel hizmetler bakımından geçerli yorumlandığını belirterek, temel hizmet olmayan canlı yayın alanında bu şartın uygulanabileceğini savunmuştur. Ayrıca Kurul'un 2019/82 ve 2019/198 sayılı kararlarına da atıf yaparak sadakat programlarına özel indirimli fiyatlarla sunulan hizmetin açık rıza dayatması sayılamayacağı içtihadinin kendi durumuna da uygulanabileceğini ileri sürmüştür. Veri sorumlusu ayrıca üyelerin verdikleri ticari ileti onaylarını diledikleri zaman hiçbir sebep göstermeksizin ve her kanal üzerinden geri alabileceklerini belirtmiştir.

Kurul, canlı yayın hizmetine erişimin ticari ileti gönderimi amacıyla kişisel verilerin işlenmesine yönelik onay verilmesi şartına bağlandığını tespit etmiştir. Başka bir ifadeyle, ilgili kişi canlı yayından yararlanmak istediğinde ticari ileti amacıyla kişisel verilerinin işlenmesine de rıza vermek zorunda kalmaktadır. Veri sorumlusu, ticari ileti onayı alınması sürecindeki kişisel veri işleme faaliyetinin KVKK madde 5/2-(ç) (hukuki yükümlülük) ve madde 5/2-(f) (meşru menfaat) şartlarına dayandığını savunmuş olsa da Kurul, bu zorunlu bağlantının açık rızanın özgür iradeyle verilmesi unsurunu ortadan kaldırdığını ve söz konusu veri işleme faaliyetinin KVKK madde 5'teki başka bir işleme şartına da dayanmadığını değerlendirmiştir. Veri sorumlusunun canlı yayın hizmetini "ek fayda" olarak nitelendirmesi ve Ticaret Bakanlığı görüşüne dayanması bu sonucu değiştirmemiştir. Bu nedenle veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik gerekli tedbirleri almadığı sonucuna varılarak 250.000 TL idari para cezası uygulanmış; ayrıca canlı yayın hizmetinin ticari ileti amacıyla kişisel veri işlenmesine yönelik açık rıza şartına bağlanması uygulamasına son verilmesi ve sonucundan Kurula bilgi verilmesi yönünde talimat verilmiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

KARAR 47

KAMU / CEZA İNFAZ

İlgili kişinin erişim hakkı talebinin reddedilmesine ilişkin şikâyeti

Karar No **2022/1152** Tarih **20.10.2022**

YAPTIRIM

İdari para cezası uygulanmamıştır.

KARARIN ÖZETİ

İlgili kişi, bulunduğu ceza infaz kurumundaki dosyasına ve elektronik kayıtlara erişemediğini, kendisine ait bilgi ve belgelerden örnek alamadığını, kişisel verilerinin eksik veya yanlış olması hâlinde düzeltilmesi ve hangi amaçlarla kullanıldığını öğrenmesi yönündeki taleplerinin karşılanmadığını ileri sürmüştür. İlgili kişi, bu taleplerini hem KVKK hem de 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamında yöneltmiş; ayrıca başvurusunun reddi hâlinde Anayasa madde 40 ve 125 uyarınca itiraz mercii, süresi ve şeklini gösteren belge verilmesini ve şikâyetine ilişkin sözlü beyanının alınmasını talep etmiştir. Kurum, 4982 sayılı Kanun kapsamındaki taleplerin ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz gerektirmesi sebebiyle 4982 sayılı Kanun kapsamında olmadığını ilgili kişiye bildirmiştir. Ayrıca ilgili kişi, ceza infaz kurumu tarafından kendisine kapalı zarfla gönderilen yazıların ceza infaz kurumu tarafından açılarak okunduğunu, geç teslim edildiğini ve dosyasındaki kişisel verilerin başka kurumlarla rızası dışında paylaşıldığını iddia etmiştir.

Kurul, değerlendirmeyi ağırlıklı olarak KVKK madde 28/1-(d) istisnası üzerinden yapmıştır. Soruşturma, kovuşturma, yargılama veya infaz işlemleri kapsamında yargı makamları ya da infaz mercileri tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin KVKK kapsamı dışında olduğunu hatırlatmıştır. Bu nedenle kapalı zarfın infaz kurumu tarafından açılması, dosyanın elektronik kayıtlarının görülmesi, örnek alınması, kişisel verilerin düzeltilmesi veya işleme amacının öğrenilmesi gibi taleplerin infaz süreciyle bağlantılı olduğu ölçüde KVKK kapsamında incelenemeyeceği sonucuna ulaşılmıştır.

Buna karşılık, yazının ilgili kişiye gecikmeli teslim edildiği yönündeki iddianın doğrudan KVKK kapsamında bir kişisel veri işleme talebi oluşturmadığı belirtilmiştir. Kişisel verilerin başka kurum ve kuruluşlarla rıza dışında paylaşıldığı iddiası bakımından ise veri güvenliği ihlalini destekleyen somut belge veya delil sunulmadığından, şikâyetin esas yönünden değerlendirilemeyeceği kabul edilmiştir.

Sonuç olarak Kurul; infaz işlemleriyle bağlantılı veri işleme faaliyetlerinin KVKK madde 28/1-(d) kapsamında istisna olduğunu, geç teslim iddiasının KVKK kapsamında olmadığını ve üçüncü kişilerle hukuka aykırı paylaşım iddiasının da yeterli delille desteklenmediğini değerlendirerek veri sorumlusu hakkında ayrıca bir yaptırım uygulanmasına gerek olmadığına karar vermiştir.

Karar özetinin tam metnine bu linkten ulaşabilirsiniz.

Yazarlar

Cansu Özgüven
Kıdemli Avukat

Ayşegül Dağhan
Avukat