DL | Avukatlık Bürosu

KİŞİSEL VERİLERİ KORUMA HUKUKU
GÜNCEL GELİŞMELER
KASIM 2024

TÜRKİYE'DEKİ GELİŞMELER

VERİ İHLALİ BİLDİRİMLERİ

Zello Inc. tarafından KVK Kurumu'na bildirilen veri ihlali, 19.11.2024 tarihinde Kişisel Verileri Koruma Kurumu'nun ("KVK Kurumu") internet sitesinde yayımlanmıştır.

Veri sorumlusu Zello Inc.; bünyesindeki kişisel verilere, bir tehdit aktörü tarafından erişim sağlanarak ve fidye yazılım saldırısı suretiyle gerçekleşen veri ihlalini ("**Veri İhlali**" veya "**İhlal**") Kişisel Verileri Koruma Kurulu'na ("**KVK Kurulu**") bildirmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir;

- İhlalin tehdit aktörünün veri sorumlusu ile iletişime geçmesiyle tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının; kullanıcılar, aboneler/üyeler ile müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin; Zello hesabı oluştururken kullanıcılar tarafından sağlanan kullanıcı adı, karma şifre (MD5 algoritması ile şifrelenmiş), e-posta adresi ve telefon numarası olduğu,
- İhlalden 494.749 kişinin etkilendiği.

İlgili karara buradan ulaşabilirsiniz.

DUYURULAR VE HABERLER

KVK Kurumu tarafından "Sosyal Medyada Ebeveyn Paylaşımları *(Sharenting)*" hakkında bilgilendirme yazısı yayımlanmıştır.

KVK Kurumu'nun LinkedIn sayfasında paylaşılan yazıya göre ebeveynlerin çocuklarının fotoğraflarını ve özel anlarını sosyal medyada paylaşma eğilimi, sharenting olarak tanımlanmıştır. Bu paylaşımlara ilişkin riskler aşağıdaki şekilde ifade edilmiştir;

- Ebeveynlerin, çocuklarının mahremiyetini ve kişisel verilerini ("**Kişisel Veri**" veya "**Veri**") koruma yükümlülüğünün bulunması,
- Bu tür paylaşımların çocukların dijital izlerini oluşturduğu ve gelecekte olumsuz sonuçlara yol açabildiği,
- Çocukların rızası olmaksızın yapılan paylaşımların onların haklarını ihlal edebildiği,
- Bu tür paylaşımların hukuki sorumluluklar doğurabildiği,
- Ebeveynlerin, çocuklarının mahremiyeti ve dijital güvenlikleri için dikkatli olması gerektiği,

İlgili bilgilendirme yazısına buradan ulaşabilirsiniz.

KVK Kurumu tarafından "Oltalama *(Phishing)* Saldırılarında Riski Azaltmaya Yönelik Alınabilecek Tedbirler" hakkında bilgilendirme yazısı yayımlanmıştır.

KVK Kurumu'nun LinkedIn sayfasında paylaşılan yazıya göre oltalama saldırıları, kötü niyetli kişilerin kişisel verileri ele geçirmek için kullanıcıları kandırmaya çalıştığı yaygın bir siber tehdit olarak tanımlanmıştır. Bu itibarla, oltalamaya karşı alınabilecek önlemler aşağıdaki şekilde ifade edilmiştir;

- Çalışanlara siber tehditler hakkında farkındalık eğitimleri verilmesi,
- Hesap güvenliği için çok faktörlü kimlik doğrulama yöntemlerinin kullanılması,
- Güvenli e-posta ağ geçitleri, spam filtreleri ve tehdit koruma yazılımlarının kullanılması,
- URL filtreleme ve DNS güvenlik çözümleriyle şüpheli bağlantılara tıklanmasının önlenmesi,
- Sistem ve uygulamaların güvenlik ve yama güncellemelerinin düzenli olarak yapılması,
- Oltalama testleriyle kullanıcıların siber tehditlere karşı farkındalığının artırılması.

İlgili bilgilendirme yazısına buradan ulaşabilirsiniz.

KVK Kurumu tarafından "ChatGPT Örneği Özelinde Sohbet Robotları" hakkında bilgilendirme yazısı yayımlanmıştır.

KVK Kurumu'nun internet sitesinde yayımlanan bilgi notunda özetle; sohbet robotlarının kullanılmasında önceliklile kullanıcıların farkındalık düzeyinin önemi vurgulanmıştır. Kullanıcıların farkındalık eksiklikleri nedeniyle sohbet robotlarını kullanırken aşırı bilgi paylaşmalarının mahremiyet riskini artırdığı ifade edilmiştir.

Tüm bunlara ek olarak üreticilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na ("**KVKK**") uyumlu ve aşağıdaki hususlara dikkat ederek sohbet robotu geliştirmeleri gerektiği belirtilmiştir;

- Uluslararası standartlara uygun olması,
- Sertifikaların bulunması,
- Başlangıçtan itibaren mahremiyet ve varsayılan mahremiyet yaklaşımlarının tasarım sürecinin her aşamasında dikkate alınması *(GDPR kapsamındaki Privacy by Desing & Privacy by Default)*,
- Metin, ses, konuşma ve görüntü gibi iletileri içeren ortamlara yönelik güvenli yöntemler tercih edilmesi,
- Yapay zekâ alanında faaliyet gösteren geliştiricilerin, üreticiler, servis sağlayıcılar ve karar alıcıların KVK Kurulu tarafından belirlenen tavsiyelere dikkat edilmesi,
- Çocuklara yönelik olarak yaş tespitinin doğru ve güvenilir şekilde gerçekleştirilmesi *(Age Assurance)*,
- Özellikle, çocukların olumsuz deneyimler yaşamasını engellemek için proaktif bir yaklaşım benimsenmesi.

İlgili bilgi notuna buradan, konu hakkında hazırladığımız bilgi notumuza buradan ulaşabilirsiniz.

KVK Kurumu tarafından "Yeni Cihazlarla İnternet Güvenliği İçin İpuçları" hakkında bilgilendirme yazı yayımlanmıştır.

KVK Kurumu'nun LinkedIn sayfasında paylaşılan yazıya göre yeni cihazlarda güvenli internet kullanımı için ipuçları aşağıdaki şekilde ifade edilmiştir;

- Parolanın güçlü belirlenmesi ve kimseyle paylaşılmaması,
- Yaş sınırı olan uygulamalar, oyunlar veya videolara dikkat edilerek, yaşa uygun olmayanlar ile vakit geçirilmemesi,
- Telefon numarası, doğum tarihi, ev adresi vb. kişisel verilerin yabancılar ile paylaşılmaması,

- Herhangi bir sorun veya rahatsızlık veren bir durum yaşanması halinde güvenilen bir yetişkin veya ebeveynden yardım istenmesi,
- Güvenli Wi-Fi kullanılması ve kamuya açık güvenli olmayan ağlarda kişisel bilgilerin çalınma riskinin bulunması hakkında bilgi sahibi olunması,
- Ekran süresinin sınırlandırılması,
- Güvenilir bluetooth cihazlarına bağlanılması, aksi takdirde yabancı cihazlara bağlanılarak kişisel verilerin güvenliğinin risk altında olabileceği hakkında bilgi sahibi olunması,
- Konum bilgisinin paylaşılmaması.

İlgili bilgilendirme yazısına buradan ulaşabilirsiniz.

KVK Kurumu ile T.C. Ticaret Bakanlığı tarafından "Efsane Kasım" indirimleri kapsamında dikkat edilmesi gerekenler hakkında bilgilendirme yazıları yayımlanmıştır.

KVK Kurumu tarafından "Efsane Kasım" indirimleri kapsamında internet ortamında güvenliğin sağlanması için öneriler aşağıdaki şekilde ifade edilmiştir;

- Kampanya mesajlarının kaynağını doğrulamak,
- İnternet sitesinin güvenilir olup olmadığını kontrol etmek,
- Sanal kart kullanmak,
- Kişisel verilere ilişkin bilgilendirmelerin gözden geçirilmesi,
- İşlemlerinizi kişisel cihazlar üzerinden yapılması,
- Şüpheli durumlarda şifrelerin güncellenmesi.

T.C. Ticaret Bakanlığına bağlı Reklam Kurulu tarafından "Efsane Kasım" indirimleri kapsamında internet ortamında güvenliğin sağlanması için öneriler aşağıdaki şekilde ifade edilmiştir;

- Satıcı/sağlayıcı hakkında ön inceleme yapılması,
- İnternet sitesi adresinin satıcı veya sağlayıcıya ait olup olmadığının kontrol edilmesi,
- Sosyal medya aracılığıyla yönlendirilen sayfalara karşı dikkatli olunması,
- İnternet sitesinde SSL sertifikası, 3D security vb. güvenlik önlemlerinin olup olmadığı kontrol edilmesi,
- Ödeme yapmadan önce tüketiciye iletilmesi gereken ön bilgileri ayrıntılı okumaları gerektiği.

KVK Kurumu ilgili bilgilendirme yazısına buradan, T.C. Ticaret Bakanlığı ilgili bilgilendirme yazısına buradan ulaşabilirsiniz.

2025 yılı için belirlenen yeniden değerleme oranı uyarınca ve Cumhurbaşkanı'nın %50 artırma yetkisi kullanılmaması halinde KVK Kurulu tarafından uygulanacak idari para cezaları aşağıdaki gibi olacaktır.

27.11.2024 tarihli Resmi Gazete'de yayımlanan 574 Sıra No.lu Vergi Usul Kanunu Genel Tebliği uyarınca, 2025 yılı için yeniden değerleme oranı %43,93 olarak belirlenmiştir. Bu orana göre KVK Kurumu tarafından uygulanacak idari para cezaları aşağıdaki gibi güncellenmiştir;

- Aydınlatma yükümlülüğünün yerine getirilmemesi: 68.083 TL - 1.362.021 TL
- Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi: 204.285 TL - 13.620.402 TL
- KVK Kurulu Tarafından Verilen Kararların Yerine Getirilmemesi: 340.476 TL - 13.620.402 TL
- VERBİS'e Kayıt ve Bildirim Yükümlülüğüne Aykırı Hareket Edilmesi: 272.380 TL - 13.620.402 TL

- Bildirim Yükümlülüğünün Yerine Getirilmemesi: 71.965 TL - 1.439.300 TL

Ancak belirtmek gerekir ki, Cumhurbaşkanı tarafından %50 artırma yetkisi kullanılmadığı takdirde yukarıdaki tutarlar geçerli olacaktır. Söz konusu yetkinin kullanılması halinde idari para cezası tutarlarının da artması söz konusu olabilecektir.

İlgili Tebliğ'e buradan ulaşabilirsiniz.

Bilgi Teknolojileri ve İletişim Kurumu ("BTK") internet sitesinde İşletmeciler Tarafından Pazarlama, Bilgilendirme vb. Amaçlarla Yapılan Aramalar ve İkincil Numara Tahsisleri ile Yurtdışından Gönderilen SMS, MMS vb. Mesajlara Yönelik Düzenleme Taslağı'na yönelik kamuoyu görüşü alınacağı duyurulmuştur. BTK'nın 27 Kasım 2024 tarihli duyurusu ile Bilgi Teknolojileri ve İletişim Kurulu'nun 05.09.2024 tarihli ve 2024/İK-YED/330 sayılı Kararı ile, kamuoyu görüşü alınabilmesini teminen söz konusu Düzenleme Taslağı'nın 30 (otuz) gün süre ile BTK internet sitesinde yayımlanmasına karar verilmiştir.

Kamuoyu görüşlerinin en geç 27.12.2024 tarihine kadar duyurudaki görüş bildirme formu kullanılmak suretiyle belirtilen elektronik posta adreslerine gönderilmesi gerektiği ifade edilmiştir.

Söz konusu duyuruya buradan, Düzenleme Taslağı'na buradan ulaşabilirsiniz.

GÜNCEL KARARLAR

KVK Kurumu tarafından, sosyal medya platformu X aleyhine 1.470.000 TL idari para cezası verilmiştir.

Anadolu Ajansı'nın 14.11.2024 tarihli haberine göre; sosyal medya platformu tarafından kullanıcılarının güvenlik ve emniyeti amacıyla temin edilen e-posta ve telefon numaralarının X'e ait reklamcılık sistemlerinde sehven reklam amacıyla kullanıldığına ilişkin duyuru üzerine KVK Kurulu tarafından resen inceleme başlatıldığı ifade edilmiştir.

Türkiye çapında çok sayıda X kullanıcısı bulunması ve kişisel verilerin üçüncü kişilerin eline geçmiş olabileceği göz önünde bulundurularak, işlenen kişisel verilerin KVKK'nın 4. maddesindeki genel ilkelerden olan "hukuka ve dürüstlük kurallarına uygun olma" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine aykırılık tespit edilmesi ve X'in yeterli teknik ve idari tedbirleri almaması sebepleriyle KVK Kurulu tarafından X aleyhine 1.470.000 TL idari para cezasına hükmedilmiştir.

Anadolu Ajans'ın söz konusu haberine buradan ulaşabilirsiniz.

DÜNYADAKİ GELİŞMELER

DUYURULAR VE HABERLER

Birleşik Krallık Veri Koruma Otoritesi ("ICO") tarafından, işe alım süreçlerinin daha verimli yürütülebilmesi için kullanılacak yapay zeka araçları hakkında dikkat edilmesi gerekenler hususlara ilişkin bilgilendirme yazısı ve denetim raporu yayımlamıştır.

ICO'nun söz konusu yazısında, şirketlerin insan kaynakları departmanları tarafından işe alım süreçlerini daha verimli hale getirmek adına yapay zeka araçlarından yararlanabildiği, bu araçlar vasıtasıyla; iş başvurusu yapan adanların özgeçmişlerinin özetlendiği, potansiyel adayların tespit edildiği ve adayların puanlandırıldığı belirtilmiştir. Ancak işbu yapay zeka araçlarının kullanılması öncesinde sorulması gereken sorular ICO tarafından aşağıdaki gibi ifade edilmiştir;

- Veri Koruma Etki Analizinin tamamlanıp tamamlanmadığı,
- Kişisel veri işlenmesinin hukuki işleme sebeplerinin neler olduğu,
- Sorumlulukların belgelenip belgelenmediği ve veri işleme talimatlarının açıkça belirlenip belirlenmediği,
- Sağlayıcının yapay zekadaki önyargıyı önlemek adına önlemlerini alıp almadığı,
- Yapay zeka araçlarının şeffaflık ilkesini yerine getirip getirmediği,
- Gereksiz veri işlenmesinin nasıl engellenebileceği.

ICO tarafından yayımlanan bilgilendirme yazısına buradan, denetim raporuna buradan ulaşabilirsiniz.

ICO tarafından, Genomik Teknolojilerin Ortaya Çıkarabileceği Risklere İlişkin Rapor ("Rapor") yayımlanmıştır.

Yayımlanan Rapor'da, genomik teknolojilerin gelişmesi ile gelecekteki günlük hayatımızda; hastanelerin DNA verisini kullanarak olası hastalıkları tahmin ederek engellemek üzere sağlık hizmeti sunabileceği, sigorta şirketlerinin poliçeleri genetik sağlık verilerine göre tahsis edebileceği, giyilebilir teknoloji ile genetik veri işlenebileceği, bu kapsamda kişiselleştirilebilecekleri hususu belirtilerek bu kapsamdaki riskler aşağıdaki şekilde ifade edilmiştir;

- **Veri Güvenliği:** Bazı genomik verilerin anonimleştirilmesinin neredeyse imkansız olması sebebiyle yanlış kullanımı ve uyguz şekilde paylaşılmasını beraberinde getirebilmektedir.
  Ayrımcılık veya Önyargı: Genomik verilerin sigorta veya kolluk kuvvetlerince kullanılması sistematik ayrımcılığa yol açabilmektedir.
- **Şeffaflık ve Rıza:** Sektörler arası bu verilerin paylaşılması, ilgili kişilerce hangi kişisel verilerinin, ne amaçla kullanıldığına ilişkin bilgiye ulaşılmasını güçleştirebilmektedir.
- **Aile Arası Paylaşım:** Genomik verilerin aile bireyleri arasında kalıtımsal olarak aktarılması sebebiyle, aile içerisinde bir kişinin verileri diğer aile bireyleri hakkında hassas verileride ortaya çıkarabilmektedir.
- **Kullanım Amacı:** Genomik verilerin orijinal kullanım amacından sapmasıyla, veri minimizasyonu ve amaç sınırlaması konusunda endişelere yol açmaktadır.

ICO tarafından yayımlanan bilgilendirme yazısına buradan, Rapor'a buradan ulaşabilirsiniz.

Avrupa Veri Koruma Gözetçisi *("European Data Protection Supervisor" veya "EDPS")* tarafından "TechSonar 2025 Raporu yayımlanmıştır.

TechSonar 2025 Raporu'nda altı trend üzerinde durulmuştur. Bu trendler aşağıdaki gibidir:

- Geri alma ile güçlendirilmiş üretim *(Retrieval-Augmented Generation)*,
- Cihaz üzerinde yapay zeka *(On-Device Artificial Intelligence)*,
- Makine öğrenmesinde unutma *(Machine Unlearning)*,
- Çok modlu yapay zeka *(Multimodal Artificial Intelligence)*,
- Ölçülebilir gözetim *(Scalable Oversight)*,
- Nöro-sembolik yapay zeka *(Neuro-Symbolic Artificial Intelligence) ,*

Raporda ayrıca yapay zeka sistemlerinin, kişisel veri işlemeleri sebebiyle EDPS'nin iki bağlamda yapay zeka teknolojileri ile ilgili otorite rolü oynadığı belirtilmiştir. Bu kapsamda EDPS hem AB Yapay Zeka Yasası *(EU AI Act)* kapsamında yetkili otorite, hem de kişisel verilerin korunması bakımından yetkili otoritedir. Bu sebeple, bu seneki yayımlanan Rapor'da yapay zeka teknolojileri ve bu trendlerin kişilerin temel hak ve özgürlüklerini nasıl etkileyebileceklerine odaklanılmıştır.

Rapora buradan ulaşabilirsiniz.

Avrupa Komisyonu Yapay Zekâ Komitesi ("CAI") tarafından HUDERIA Metodolojisi kabul edilmiştir.

Yapay Zekâ, İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Hakkında Çerçeve Sözleşmesi'ne ("**Çerçeve Sözleşme**") taraf ülkeler bakımından risk değerlendirmesi bakımından yararlanabilecekleri HUDERIA Metodolojisi CAI'nın Strazburg'da gerçekleştirilen 12. Genel Kurul toplantısına kabul edilmiştir.

HUDERIA Metodolojisi açılım olarak; İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Açısından Yapay Zeka Sistemlerinin Risk ve Etki Değerlendirme Metodolojisi olarak ifade edilmektedir. HUDERIA'nın uluslararası insan hakları standartları ile yapay zekâ bağlamında risk yönetimine ilişkin mevcut teknik çerçevelerin kesiştiği noktada benzersiz ve kritik bir rol oynaması amaçlanmaktadır. HUDERIA, hem kamu hem de özel sektör aktörleri tarafından yapay zekâ sistemlerinin yaşam döngüsü boyunca insan hakları, demokrasi ve hukukun üstünlüğüne yönelik riskleri ve etkileri belirlemeye ve ele almaya yardımcı olmak için kullanılabilecektir.

CAI tarafından 2025 senesi içerisinde; İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Açısından Yapay Zekâ Sistemlerinin Risk ve Etki Değerlendirme Modeli'nin (HUDERIA Model) kabul edilmesi beklenmektedir.

HUDERIA Metodolojisi'ne buradan ulaşabilirsiniz.

GÜNCEL KARARLAR

Slovenya Veri Koruma Otoritesi tarafından, Dodo Pizza sahibi Fovella d.o.o. aleyhine mutfak çalışanlarını kapalı devre televizyon *(CCTV)* kullanarak gözetlediği ve bu görüntüleri şirket internet sitesinde izinsiz olarak yayımlaması sebepleriyle € 25.000 idari para cezasına hükmedilmiştir.

Slovenya Veri Koruma Otoritesi tarafından, çalışanların izlenmesinin ancak istisnai durumlarda ve kişilerin veya mülkün güvenliğini sağlamak amacıyla hukuka uygun şekilde yapılabileceği belirtilmiştir. Bu sebepler olmaksızın gerçekleştirilen izlemenin hukuka uygun olmadığı ifade edilmiştir. Ek olarak, işbu görüntülerin şirketin internet sitesinde yayımlanmasının hem Slovenya Mevzuatına hem AB Genel Veri Koruma Tüzüğü'ne ("**GDPR**") göre hukuka uygun olmadığı vurgulanmıştır. Bu itibarla, Dodo Pizza sahibi Fovella d.o.o. aleyhine € 25.000 idari para cezası verilmesiyle birlikte; ilgili kişileri aydınlatmaması sebebiyle kınama cezası verilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

Norveç Veri Koruma Otoritesi tarafından, Çalışma ve Sosyal Yardım İdaresi *(Labour and Welfare Administration)* aleyhine € 1.700.000 idari para cezasına hükmedilmiştir.

Norveç Veri Koruma Otoritesi tarafından, Çalışma ve Sosyal Yardım İdaresi'ne yönelik olarak Eylül 2023'te yapılan incelemede yönetim sistemlerinin veri koruma düzenlemeleri ile uyumlu olmadığı ve log kayıtlarının gizliliklerinin yeterli olmaması sebebiyle Çalışma ve Sosyal Yardım İdaresi aleyhine € 1.700.000 idari para cezasına hükmedilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

Norveç Veri Koruma Otoritesi tarafından, Eidshog Belediyesi aleyhine € 21.000 idari para cezasına hükmedilmiştir.

Norveç Veri Koruma Otoritesi tarafından gerçekleştirilen incelemeler sonucunda, Eidshog Belediyesi'nin bir muhbir ile ilgili kişisel verileri yayımladığı ortaya çıkmıştır. Ek olarak, Eidshog Belediyesi'nin iki eski çalışanın; herhangi bir hukuki dayanak olmaksızın ve gerekli anonimleştirme ve gizlilik yöntemleri kullanılmaksızın Eidshog Belediyesi'ne yöneltilen muhbir hakkındaki şikayet bildirimine erişim sağladıkları Norveç Veri Koruma

Otoritesi tarafından saptanmıştır. Bu ihlaller sonucunda Eidskog Belediyesi aleyhine € 21.000 idari para cezasına hükmedilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

Norveç Veri Koruma Otoritesi tarafından, University of Agder aleyhine € 12.700 idari para cezasına hükmedilmiştir.

Şubat 2024 tarihinde, University of Agder'de çalışan bir kişi tarafından; Ağustos 2018'den beri çalışanların, öğrencilerin ve üniversite dışı kişilerin kişisel verilerinin, Microsoft Teams üzerindeki açık dosyalar içerisinde saklandığı ve çalışanlarca erişilebildiği tespit edilmiştir. Söz konusu ihlailin Ağustos 2018'den beri devam etmekte olduğu belirtilmiştir. Söz konusu erişim sebebiyle 16.000 ilgili kişi verisinin etkilendiği belirtilmiştir. Erişilen veriler arasında; isim, ulusal kimlik numaraları, sınav bilgileri, sınav deneme sayıları ve özel düzenlemeler hakkında bilgi bulunmaktadır. Aynı zamanda bu veriler arasında Ukrayna'dan gelen mültecilerin bilgileri bulunmaktadır. Tüm bu bilgiler doğrultusunda; Norveç Veri Koruma Otoritesi tarafından University of Agder aleyhine € 12.700 idari para cezasına hükmedilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

Fransız Veri Koruma Otoritesi tarafından, çevrimiçi fal hizmetleri sağlayan Cosmospace ve Telemaque şirketleri aleyhine toplam € 400.000 idari para cezası hükmedilmiştir.

Fransa Ulusal Bilişim ve Özgürlük Komisyonu tarafından 2021 yılında yürütülen araştırmalar sonucunda, Cosmospace ve Telemaque şirketlerinin özel nitelikli kişisel verileri, özellikle sağlık ve cinsel yönelim verilerini, ilgili kişinin açık rızası olmaksızın telefon, çevrimiçi sohbet ve mesaj vasıtalarıyla topladığı, bu verileri çok uzun süreler boyunca sakladığı, açık rıza vermeyen kişilere reklam amaçlı mesajlar gönderildiği ve Cosmospace tarafından kullanıcılar ile gerçekleştirilen telefon konuşmaları, ilgili kişilerin rızası olmaksızın kaydedildiği tespit edilmiştir. Bu ihlaller sonucunda, toplam 1.500.000 kişinin kişisel verilerinin işlenmiş olması, ihlalin ciddiyeti ve şirketlerin mali durumları göz önünde bulundurularak, Cosmospace aleyhine € 250.000, Telemaque aleyhine ise € 150.000 idari para cezası öngörülmüştür.

Kararın detaylarına buradan ulaşabilirsiniz.

Hamburg Veri Koruma Otoritesi tarafından ulusal çapta yürütülen soruşturma sonucunda kredi tahsilat hizmeti veren şirket aleyhine € 900.000 idari para cezasına hükmedilmiştir.

Hamburg Veri Koruma Otoritesi tarafından kredi tahsilat hizmeti veren şirketlere yönelik başlatılan incelemeler neticesinde ismi açıklanmayan bir şirkete yerinde yapılan yerinde incelemeler sonucunda söz konusu şirketin, herhangi bir hukuki dayanak olmaksızın kişisel verileri imha etmediği tespit edilmiştir. Söz konusu kararda; hukuki olarak beş sene saklama süresi olmasına rağmen şirketin, bu süre içerisinde kişisel verileri imha etmediği ifade edilmiştir. Bu itibarla, Hamburg Veri Koruma Otoritesi tarafından şirket aleyhine € 900.000 idari para cezasına hükmedilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.