DL | Avukatlık Bürosu

KİŞİSEL VERİLERİ KORUMA KURULU'NUN YENİ YAYINLANAN KARAR ÖZETLERİ

DL'den
NOTLAR SERİSİ
-XXX-

09 Eylül 2026

İÇİNDEKİLER

1. 10.06.2026 Tarihli ve 2026/1183 Sayılı Karar

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

Konunun Özeti:

Bir tasarruf finansman şirketinin, marka elçiliği programı kapsamında müşterilerinden üçüncü kişilere ait iletişim bilgilerini temin ederek bu kişilere pazarlama amaçlı SMS gönderdiği ve arama yaptığı iddia edilmiştir. Veri sorumlusu, ilgili kişinin görüşme sırasında bilgi almak istemeye devam ettiğini ve bu nedenle açık rıza verdiğini ileri sürmüştür.

Kurul'un Değerlendirmesi:

Kurul, üçüncü kişi tarafından aktarılan iletişim bilgilerinin işlenmeye başlanmasından önce geçerli bir veri işleme şartının bulunması gerektiğini, ilgili kişinin görüşmeye devam etmesinin veya kampanya hakkında bilgi almak istemesinin tek başına açık rıza olarak kabul edilemeyeceğini değerlendirmiştir. Açık rızanın belirli bir konuya ilişkin olması, bilgilendirmeye dayanması ve özgür iradeyle açıklanması gerektiği ve aydınlatma ile açık rıza süreçlerinin birbirinden ayrı yürütülmesi gerektiği vurgulanmıştır.

Öne Çıkan Hukuki İlke:

Zımni davranışlar açık rıza yerine geçmez. Özellikle pazarlama süreçlerinde kişinin aramayı sonlandırmaması, görüşmeye devam etmesi veya ürün/hizmet hakkında bilgi almak istemesi, kişisel verilerinin pazarlama amacıyla işlenmesine ilişkin geçerli bir açık rıza bulunduğu anlamına gelmemektedir.

Kurul'un Kararı:

Kişisel verilerin geçerli bir işleme şartı bulunmaksızın işlendiği gerekçesiyle Kanun'un 12/1 maddesine aykırılık tespit edilmiş ve Kanun'un 18/1-(b) bendi uyarınca **1.000.000 TL** idari para cezası uygulanmasına karar verilmiştir. İlgili kişinin başvurusunun süresinde yanıtlandığı tespit edildiğinden bu iddia bakımından ayrıca işlem tesis edilmemiştir.

Şirketler Açısından Değerlendirme:

Üçüncü kişilerden referans, tavsiye, müşteri önerisi, marka elçisi vb. mekanizmalarla iletişim bilgisi toplanan pazarlama süreçlerinin yeniden değerlendirilmesi gerekir. Kişinin iletişim bilgilerinin üçüncü bir kişi tarafından paylaşılması, tek başına pazarlama iletişimi bakımından geçerli bir işleme şartı sağlamamaktadır. Ayrıca ilk iletişim kurulmadan önce veya ilk iletişim sırasında uygulanacak aydınlatma ve açık rıza mekanizmalarının süreç bazında tasarlanması, 33çağrı merkezi kayıtlarında aydınlatma ve rıza akışının ayrıca güvence altına alınması önem taşımaktadır.

2. 15/08/2024 Tarihli ve 2024/1393 Sayılı Karar

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

Konunun Özeti:

Uçuş sırasında sunulan Wi-Fi hizmetinden yararlanabilmek amacıyla yolcuların soyadı, koltuk numarası veya bilet numarası gibi bilgilerinin internet servis sağlayıcının portalı üzerinden doğrulanması ve havayolu şirketi ile internet servis sağlayıcı arasında aktarılması söz konusudur. Şikâyet kapsamında, hizmetten yararlanmanın kişisel verilerin paylaşılmasına ilişkin açık rıza verilmesi şartına bağlandığı ileri sürülmüştür.

Kurul'un Değerlendirmesi:

Kurul, havayolu şirketi ile internet servis sağlayıcının söz konusu veri işleme faaliyeti bakımından iki ayrı veri sorumlusu olduğunu değerlendirmiştir. Yolcunun doğrulanması ve Wi-Fi hizmetinin sunulması bakımından kişisel verilerin işlenmesinin Kanun'un 5/2(c), (ç) ve (e) bentlerindeki işleme şartlarına dayanabileceği, bu nedenle ayrıca açık rıza alınmasının gerekli olmadığı sonucuna varılmıştır. Buna rağmen ilgili kişiye açık rıza verilmesinin zorunlu olduğu izleniminin yaratılması, ilgili kişinin yanıltılması ve yanlış yönlendirilmesi olarak değerlendirilmiş ve hukuka ve dürüstlük kurallarına uygunluk ilkesine aykırılık kabul edilmiştir.

Öne Çıkan Hukuki İlke:

Açık rıza, diğer kişisel veri işleme şartlarının yerine ikame edilmemeli veya gereksiz şekilde talep edilmemelidir. İşleme faaliyetinin Kanun'un 5/2 maddesinde yer alan bir işleme şartına dayanabildiği durumlarda açık rızanın hizmetten yararlanmanın koşulu olarak sunulması, ilgili kişinin yanıltılması ve hukuka ve dürüstlük kurallarına aykırılık sonucunu doğurabilir.

Kurul'un Kararı:

İnternet servis sağlayıcı hakkında, ilgili kişiden açık rıza talep edilerek yanıltılması ve yanlış yönlendirilmesi nedeniyle Kanun'un 4/2(a) ve 12/1 maddelerine aykırılık kapsamında **90.000 TL** idari para cezası uygulanmasına karar verilmiştir. Aydınlatma yükümlülüğüne ilişkin iddia usul nedeniyle incelemeye alınmamış, yurt dışına aktarım iddiası bakımından ise havayolu şirketi yönünden ayrıca işlem tesis edilmemiştir.

Şirketler Açısından Değerlendirme:

Şirketlerin kişisel veri işleme faaliyetleri için öncelikle uygulanabilir veri işleme şartını belirlemeleri ve açık rızayı varsayılan/genel bir hukuki dayanak olarak kullanmaktan kaçınmaları gerekir. Özellikle üyelik, hizmet sunumu, müşteri doğrulama ve dijital platformlarda kullanıcı akışlarının incelenerek, hizmetin sunulması için zorunlu olan veri işleme faaliyetlerinin gereksiz açık rıza kutucuklarına bağlanıp bağlanmadığının kontrol edilmesi önem taşımaktadır. Ayrıca farklı şirketlerin dahil olduğu veri işleme süreçlerinde tarafların veri sorumlusu/veri işleyen sıfatlarının ve aralarındaki veri aktarımının ayrıca değerlendirilmesi gerekmektedir.

3. 08/08/2024 Tarihli ve 2024/1361 Sayılı Karar

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 hakkında;

Konunun Özeti:

Veri sorumlusunun eğitim hizmetleri kapsamında güvenlik kamerası ve telefon görüşmelerinde kişisel veri işlediği, internet sitesinde analitik çerez kullandığı ve ileitşim formunu dolduran kişilerden reklam, promosyon ve kampanyalar dahil olmak üzere çeşitli amaçlarla kişisel verilerinin kullanılmasına ilişkin tek bir açık rıza aldığı ileri sürülmüştür. Ayrıca ilgili kişinin başvurusunun usulüne uygun yanıtlanmadığı iddia edilmiştir.

Kurul'un Değerlendirmesi:

Kurul, güvenlik kamerasıyla görüntü kaydının ilgili mevzuattan kaynaklanan hukuki yükümlülük kapsamında hukuka uygun olduğunu, ancak aydınlatma yükümlülüğünün Kanun'un 10'uncu maddesine uygun şekilde yerine getirilmediğini değerlendirmiştir. Zorunlu olmayan analitik çerezlerin açık rıza olmaksızın çalıştırılmasını hukuka aykırı veri işleme olarak değerlendiren Kurul, bu çerezler bakımından opt-in mekanizması uygulanması gerektiğini belirtmiştir. Ayrıca hizmet hakkında bilgi almak amacıyla iletişim formunu dolduran kişilerden, aynı işlem içerisinde reklam, promosyon ve kampanya amaçlı veri işleme için de rıza alınmasının açık rızanın "belirli bir konuya ilişkin olma" ve "özgür iradeyle açıklanma" unsurlarını ihlal ettiğine karar vermiştir.

Öne Çıkan Hukuki İlke:

(i) Aydınlatma ve açık rıza birbirinden ayrılmalıdır. Yalnızca açık rıza metni niteliğindeki bir "yasal uyarı" aydınlatma yükümlülüğünü karşılamaz. (ii) Zorunlu olmayan çerezler için opt-in yaklaşımı uygulanmalıdır. Açık rıza gerektiren çerezler, kullanıcı tarafından aktif olarak onay verilmeden çalıştırılmamalıdır. (iii) Açık rıza amaç bazında ayrıştırılmalıdır. Bir hizmetten bilgi almak için gerekli iletişim bilgilerinin işlenmesi ile reklam/pazarlama amaçlı veri işleme tek bir açık rıza altında birleştirilmemelidir. (iv) Pazarlama amaçlı açık rıza hizmetin ön şartı yapılamaz.

Kurul'un Kararı:

Veri sorumlusu hakkında aydınlatma yükümlülüğünün ihlali ve hukuka aykırı veri işleme nedeniyle toplam **265.000 TL** idari para cezası uygulanmıştır. Ayrıca aydınlatma metinlerinin düzeltilmesi, zorunlu olmayan çerezler için uygun açık rıza mekanizmasının kurulması, farklı amaçların açık rıza metninde ayrıştırılması ve reklam/pazarlama amaçlı rızanın hizmetin ön şartı olmaktan çıkarılması yönünde talimat verilmiştir. İlgili kişinin sözlü olarak yanıtlanan başvurusuna ilişkin olarak ise başvuruların Kanun ve ilgili Tebliğ uyarınca etkin ve uygun şekilde sonuçlandırılması gerektiği hatırlatılmıştır.

Şirketler Açısından Değerlendirme:

Şirketlerin internet sitesi ve dijital kanallarındaki çerez uygulamalarını, özellikle analitik ve reklam/pazarlama çerezlerinin kullanıcı onayı alınmadan çalışıp çalışmadığı bakımından gözden geçirmesi, aydınlatma metni ile açık rıza metinlerini birbirinden ayırması ve farklı amaçlar için alınan rızaları ayrı ve spesifik şekilde kurgulaması gerekir. Ayrıca bir ürün veya hizmetten yararlanmak, bilgi talep etmek ya da iletişim kurulmasını sağlamak için gerekli veri işleme faaliyetleri ile reklam/pazarlama faaliyetleri birbirinden ayrılmalı ve pazarlama rızasının hizmetin sunulması için zorunlu tutulmamasına dikkat edilmelidir. İlgili kişi başvurularının da yalnızca fiilen cevaplanması değil, yazılı veya elektronik ortamda, gerekçeli ve usulüne uygun şekilde sonuçlandırılması sağlanmalıdır.

4. 08/08/2024 Tarihli ve 2024/1359 Sayılı Karar

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

Konunun Özeti:

İlgili kişi, bir trafik kazası sonrasında araç değer kaybı başvurusunda bulunmuş ve sigorta şirketinin, kendisi tarafından paylaşılmadığını ileri sürdüğü IBAN bilgisine nasıl ulaştığını sorgulamıştır. Sigorta şirketi ise IBAN bilgisinin aynı kazaya ilişkin hasar bildirimi sırasında, ilgili mevzuat kapsamında ve ilgili kişinin zarar gören üçüncü kişi sıfatıyla sunulması gereken belgeler çerçevesinde elde edildiğini, daha sonra aynı kazaya ilişkin değer kaybı ödemesinin gerçekleştirilmesi amacıyla kullanıldığını belirtmiştir.

Kurul'un Değerlendirmesi:

Kurul, ilgili kişinin IBAN bilgisinin, kazaya ilişkin hasar bildirimi sırasında üçüncü kişi tarafından sigorta şirketine aktarılmasının ilgili mevzuat uyarınca hukuka uygun olduğunu değerlendirmiştir. Şirketin bu şekilde hukuka uygun olarak elde ettiği IBAN bilgisini, aynı kaza kapsamında yapılan değer kaybı başvurusu sonrasında ödeme gerçekleştirmek amacıyla kullanmasının, Kanun'un 5/2-(e) bendinde düzenlenen "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" işleme şartına dayandığı kabul edilmiştir. Bu nedenle söz konusu veri işleme faaliyeti bakımından ayrıca bir hukuka aykırılık tespit edilmemiştir.

Öne Çıkan Hukuki İlke:

Kişisel verinin daha önce hukuka uygun şekilde elde edilmiş olması, verinin her türlü sonraki kullanımını otomatik olarak hukuka uygun hale getirmez ancak aynı olay ve amaçla doğrudan bağlantılı, hakkın tesisi/kullanılması/korunması için zorunlu olan sonraki işlemler ayrıca Kanun'un 5'inci maddesindeki uygun bir işleme şartına dayanabilir. Somut olayda Kurul, hasar bildirimi kapsamında hukuka uygun elde edilen IBAN bilgisinin aynı kazaya ilişkin değer kaybı ödemesinde kullanılmasını bu kapsamda değerlendirmiştir.

Kurul'un Kararı:

IBAN bilgisinin hasar bildirimi kapsamında hukuka uygun olarak elde edildiği ve aynı kazaya ilişkin değer kaybı ödemesi amacıyla kullanılmasının Kanun'un 5/2-(e) bendine dayandığı değerlendirilerek bu hususta herhangi bir işlem tesis edilmemiştir. İlgili kişi başvurusunun şirket içindeki işleyiş aksaklığı nedeniyle geç yanıtlanması bakımından ise başvuruların etkin, hukuka ve dürüstlük kurallarına uygun ve gerekçeli şekilde sonuçlandırılması gerektiği şirkete hatırlatılmıştır.

Şirketler Açısından Değerlendirme:

Şirketlerin farklı süreçlerde elde edilen kişisel verilerin sonraki kullanımını değerlendirirken verinin ilk elde edilme hukuki sebebinin yanı sıra sonraki kullanımın amacı, ilk işleme faaliyetiyle bağlantısı ve uygulanabilir ayrı bir işleme şartının bulunup bulunmadığını değerlendirmesi gerekir. Özellikle hasar, tazminat, ödeme ve uyuşmazlık süreçlerinde daha önce hukuka uygun şekilde elde edilen verilerin aynı olayla bağlantılı işlemlerde yeniden kullanılmasının hukuki dayanağı süreç bazında ortaya konulmalıdır. Ayrıca ilgili kişi başvurularının şirket içindeki yanlış birime yönlendirilmesi veya iş birimleri arasındaki koordinasyon eksikliği nedeniyle geciktirilmemesi için başvuruların merkezi ve kontrollü şekilde yönetilmesi önem taşımaktadır.

5. 08/08/2024 Tarihli ve 2024/1350 Sayılı Karar

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

Konunun Özeti:

İlgili kişi, elektronik haberleşme işletmecisi tarafından kendisine birbirine yakın tarihlerde ve benzer içerikte çok sayıda reklam/pazarlama içerikli SMS gönderildiğini, bu iletileri çağrı merkezi görüşmelerinde reddetmesine rağmen gönderimlerin devam ettiğini ileri sürmüştür. Veri sorumlusu ise SMS'lerin bir kısmının kampanya süresinin sona ermesine ilişkin mevzuattan kaynaklanan bilgilendirme yükümlülüğü kapsamında, bir kısmının ise sözleşmede yer alan ret imkânının kullanılmamış olması nedeniyle gönderildiğini savunmuştur.

Kurul'un Değerlendirmesi:

Kurul, kampanya süresinin sona ermesi konusunda abonelerin bilgilendirilmesinin mevzuattan kaynaklanan bir yükümlülük olduğunu kabul etmekle birlikte, bu yükümlülüğün yerine getirilmesi amacıyla aynı veya benzer içerikte 20'den fazla SMS'in yaklaşık iki buçuk aylık süre içerisinde sık aralıklarla gönderilmesini ilgili kişinin makul beklentisini aşan bir veri işleme faaliyeti olarak değerlendirmiştir. Veri sorumlusunun Kanun'un 5/2-(ç) bendindeki işleme şartına dayanıyor olması, işleme faaliyetinin Kanun'un 4'üncü maddesindeki hukuka ve dürüstlük kurallarına uygunluk ilkesine tabi olduğu gerçeğini değiştirmemektedir. Kurul ayrıca, açık rıza metninin sözleşme içerisinde yer almasının ilgili kişileri yanıltabileceğini ve açık rızanın unsurlarını sakatlayabileceğini belirterek açık rıza metninin sözleşmeden ayrı sunulmasını uygun bulmuştur.

Öne Çıkan Hukuki İlke:

Geçerli bir veri işleme şartının bulunması, veri işleme faaliyetinin sınırsız şekilde gerçekleştirilebileceği anlamına gelmez. İşleme faaliyeti ayrıca hukuka ve dürüstlük kurallarına uygun, belirli amaçla bağlantılı, sınırlı ve ölçülü olmalıdır. Özellikle mevzuattan kaynaklanan bilgilendirme yükümlülükleri kapsamında gerçekleştirilen iletişimlerde dahi iletişimlerin sıklığı ve içeriği ilgili kişinin makul beklentisini aşmamalıdır. Ayrıca açık rıza metinlerinin sözleşme metnine dahil edilmesi, ilgili kişiyi yanıltabilecek veya rızanın özgür iradeyle verilmesi unsurunu etkileyebilecek nitelikteyse bundan kaçınılmalıdır.

Kurul'un Kararı:

Veri sorumlusu hakkında, cep telefonu numarasının hukuki yükümlülük kapsamında işlenebilmesine rağmen aynı içerikteki SMS'lerin sık aralıklarla gönderilmesi suretiyle hukuka ve dürüstlük kurallarına uygunluk ilkesinin ihlal edilmesi nedeniyle **100.000 TL** idari para cezası uygulanmıştır. Ayrıca açık rıza metninin sözleşme metninden ayrı olarak sunulmasının uygun olacağı veri sorumlusuna hatırlatılmıştır.

Şirketler Açısından Değerlendirme:

Şirketler, kişisel veri işleme faaliyetlerinin hukuki dayanağını belirlemekle yetinmemeli, işlemenin sıklığı, kapsamı, yöntemi ve ilgili kişinin makul beklentisi bakımından da değerlendirme yapmalıdır. Özellikle mevzuattan kaynaklanan bildirimler ile pazarlama iletişimlerinin ayrıştırılması, zorunlu bildirimlerin pazarlama iletişimine dönüşmemesi ve aynı içeriğin gereğinden fazla tekrarlanmaması önem taşımaktadır. Ayrıca açık rıza alınan metinlerin sözleşme hükümlerinden ayrıştırılması ve ilgili kişinin hangi işlem için rıza verdiğini açıkça anlayabileceği bir yapı kurulması gerekir.

6. 18/04/2024 Tarihli ve 2024/592 Sayılı Karar

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

Konunun Özeti:

Banka çalışanı olan ilgili kişi, bir müşteriyle gerçekleştirdiği ve kayıt altına alınan telefon görüşmesinde hakaret ve küfür içerikli ifadeler kullanıldığını ileri sürerek yasal yollara başvurmak amacıyla görüşme kaydının kendisine verilmesini talep etmiştir. Banka, kayıtlarda müşteriye ait kredi ve gecikme durumu gibi müşteri sırrı niteliğinde bilgilerin bulunması nedeniyle kaydın paylaşılmasının mümkün olmadığını savunarak talebi reddetmiştir.

Kurul'un Değerlendirmesi:

Kurul, Kanun'un 11/1-(b) bendinde yer alan kişisel verilerin işlenip işlenmediğini öğrenme ve buna ilişkin bilgi talep etme hakkının, ilgili kişinin kendi kişisel verilerine erişim hakkını da kapsadığını değerlendirmiştir. Somut olayda ilgili kişinin talebinin müşteri sırrına erişmeye değil, kendisiyle yapılan görüşmeye ve hakaret iddiasını kanıtlamaya yönelik olduğu belirtilmiştir. Kayıtta üçüncü kişiye ait müşteri sırrı niteliğinde bilgiler bulunması, ilgili kişinin kendi kişisel verilerine erişiminin tamamen engellenmesini gerektirmemektedir. Bu nedenle Kurul, üçüncü kişiye ait müşteri sırrı niteliğindeki bilgilerin maskelenmesi suretiyle görüşme kaydının veya yazılı dökümünün ilgili kişiye sağlanması gerektiğine karar vermiştir.

Öne Çıkan Hukuki İlke:

Bir kişisel veri kaydında üçüncü kişilere ait kişisel veya gizli bilgiler bulunması, ilgili kişinin kendi kişisel verilerine erişim hakkının kategorik olarak reddedilmesi için tek başına yeterli değildir. Veri sorumlusu, mümkün olduğu ölçüde üçüncü kişiye ait bilgileri maskeleyerek ilgili kişinin kendi kişisel verilerine erişimini sağlamalıdır.

Kurul'un Kararı:

Bankanın, ilgili kişinin talep ettiği telefon görüşme kayıtlarını üçüncü kişinin müşteri sırrı niteliğindeki bankacılık işlem verilerini maskeleyerek yazılı döküm veya dijital ortamda ilgili kişiye sağlaması yönünde talimat verilmiştir. Ayrıca ilgili kişi başvurularının etkin, hukuka ve dürüstlük kurallarına uygun ve gerekçeli şekilde sonuçlandırılması gerektiği bankaya hatırlatılmıştır.

Şirketler Açısından Değerlendirme:

İlgili kişi başvuruları değerlendirilirken, kayıtta üçüncü kişilere ait verilerin bulunması nedeniyle talebin tamamen reddedilmesi yerine veri minimizasyonu ve maskeleme yaklaşımı benimsenmelidir. Özellikle çağrı merkezi kayıtları, e-posta yazışmaları, kamera kayıtları, toplantı kayıtları ve benzeri karma içerikli veri setlerinde, ilgili kişinin kendi kişisel verileri ile üçüncü kişilere ait veriler ayrıştırılarak erişim sağlanıp sağlanamayacağı değerlendirilmelidir. Başvuruların ilgili birimler arasında kaybolmaması için merkezi bir başvuru yönetim mekanizmasının kurulması ve her başvurunun Kanun'un 13'üncü maddesi ve ilgili Tebliğ kapsamında usulüne uygun şekilde sonuçlandırılması da önem taşımaktadır.

7. 22/02/2024 Tarihli ve 2024/282 Sayılı Karar

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

Konunun Özeti:

İlgili kişi, internet hizmetinin nakledilmesi sonrasında kimlik belgesinin yeniden talep edildiğini ve gerekli belgeleri sunmaması nedeniyle aboneliğinin feshedildiğini belirtmiştir. Ayrıca kişisel verilerinin imha edilmesini, sözleşme örneğinin gönderilmesini ve verilerinin aktarıldığı üçüncü kişilerin bildirilmesini talep etmiştir. Veri sorumlusu ise kimlik bilgilerinin sözleşme ve mevzuat kapsamındaki yükümlülükler doğrultusunda işlendiğini, ancak sözleşmede grup şirketlerine aktarım bakımından açık rıza niteliğinde hükümlere de yer verdiğini belirtmiştir.

Kurul'un Değerlendirmesi:

Kurul, kimlik bilgilerinin Kanun'un 5/2-(c), (ç) ve (e) bentleri kapsamında işlenebileceğini ve işleme sebebi devam ettiği sürece derhal imha edilmesinin gerekmediğini değerlendirmiştir. Ancak geçerli bir açık rıza dışı işleme şartı mevcutken ayrıca açık rıza alınmasının ilgili kişiyi yanıltabileceğini ve hukuka ve dürüstlük kurallarına uygunluk ilkesine aykırılık oluşturabileceğini belirtmiştir.

Öne Çıkan Hukuki İlke:

Bir kişisel veri işleme faaliyeti bakımından açık rıza dışında geçerli bir işleme şartının bulunması halinde ayrıca açık rıza alınmamalıdır. Açık rıza, diğer işleme şartlarının yerine ikame edilmemeli, mevcut başka bir hukuki sebebe rağmen açık rıza alınması ilgili kişinin yanıltılması ve yanlış yönlendirilmesi sonucunu doğurabileceğinden hukuka ve dürüstlük kurallarına uygunluk ilkesine aykırılık oluşturabilecektir. Ayrıca açık rıza alınması gereken durumlarda, açık rızanın sözleşme hükümlerinden ayrıştırılması ve Kanun'da öngörülen tüm unsurları taşıması gerekmektedir.

Kurul'un Kararı:

Veri sorumlusu hakkında **350.000 TL** idari para cezası uygulanmış, sözleşmedeki açık rıza niteliğindeki hükümlerin çıkarılması, ilgili kişiye sözleşme örneğinin ve grup şirketleri listesinin verilmesi ve kişisel verilerin amaçla bağlantılı ve asgari süreyle saklanması yönünde talimat verilmiştir. Ayrıca ilgili kişinin kimlik bilgilerinin amaçla bağlantılı ve asgari süreyle sınırlı olarak saklanması, ıslak imzalı sözleşme örneğinin ilgili kişiye gönderilmesi ve kişisel verilerin aktarıldığı grup şirketlerinin listesinin paylaşılması yönünde talimat verilmiştir.

Şirketler Açısından Değerlendirme:

Şirketlerin sözleşmelerinde kişisel veri işleme ve aktarımına ilişkin hükümleri belirlerken öncelikle açık rıza dışındaki işleme şartlarını değerlendirmesi ve geçerli bir hukuki sebep mevcutsa ayrıca açık rıza almaması gerekmektedir. Açık rıza gereken durumlarda ise rıza, sözleşmeden ayrıştırılmış ve hizmetin ön şartı olmayacak şekilde alınmalıdır.

8. 26/12/2024 Tarihli ve 2024/2196 Sayılı Karar

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

Konunun Özeti:

Veri sorumlusunun sistemlerine gerçekleştirilen fidye yazılımı saldırısı sonucunda bazı veriler şifrelenmiş ve sistemlere erişim sağlanmıştır. İhlal kapsamında çalışanlara ait çeşitli kişisel verilerin yanı sıra müşterilere ait verilerin de etkilenmiş olabileceği değerlendirilmiştir. Veri sorumlusu, ihlalden etkilenen kişiler ve veri kategorileri konusunda Kurul'a farklı ve birbiriyle çelişen beyanlarda bulunmuş ve ayrıca ihlal öncesinde mevcut olduğunu belirttiği bazı teknik ve idari tedbirlere ilişkin yeterli tevsik edici belge sunamamıştır.

Kurul'un Değerlendirmesi:

Kurul, ihlalden etkilenen kişi ve veri kategorileri hakkında çelişkili beyanda bulunulmasını, gerekli bilgi ve belgelerin sunulmamasını, güvenlik açığının tespit edilememesini, log kayıtlarına erişilememesini, güvenlik testlerinin yetersiz kalmasını, iki faktörlü kimlik doğrulamanın ihlal sonrasında uygulanmaya başlanmasını ve 9 şirketin sistemlerinin aynı saldırıdan etkilenmesini dikkate almıştır. Özellikle ağ segmentasyonunun yetersiz olması ve özel nitelikli veriler bakımından güvenli şifreleme tedbirlerinin ihlal öncesinde uygulanmaması, risklerin önceden yeterince belirlenmediğini ve uygun tedbirlerin alınmadığını göstermiştir.

Öne Çıkan Hukuki İlke:

Veri güvenliği tedbirleri, ihlal gerçekleştikten sonra alınan önlemlerle sınırlı olmamalı; veri sorumlusu mevcut risk ve tehditleri önceden belirleyerek uygun teknik ve idari tedbirleri proaktif şekilde uygulamalıdır. Ayrıca ihlal sonrasında etkilenen kişi ve veri kategorilerinin doğru şekilde tespit edilmesi ve Kurul'a sunulan bilgilerin tutarlı ve tevsik edilebilir olması önem taşımaktadır.

Kurul'un Kararı:

Veri sorumlusunun KVKK m.12/1 kapsamında gerekli teknik ve idari tedbirleri almaması nedeniyle **250.000 TL** idari para cezası uygulanmasına karar verilmiştir.

Şirketler Açısından Değerlendirme:

Şirketlerin düzenli risk değerlendirmeleri ve güvenlik testleri gerçekleştirmesi, MFA, güvenli şifreleme, ağ segmentasyonu ve yeterli loglama gibi teknik tedbirleri ihlal öncesinde uygulaması gerekmektedir. Ayrıca veri ihlali halinde etkilenen kişi ve veri kategorilerinin doğru şekilde belirlenmesi, ihlal kayıtlarının ve logların korunması ve Kurul'a sunulacak bilgi ve belgelerin tutarlı ve doğrulanabilir olması önem taşımaktadır.

9. 07/11/2024 Tarihli ve 2024/1899 Sayılı Karar

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

Konunun Özeti:

Veri sorumlusunun pazarlama amacıyla kullandığı kullanıcı hesabına yetkisiz erişim sağlanmış ve bu hesap üzerinden herkese açık bırakılan klasörlere ve FTP sunucusuna erişilmiştir. İhlalden yaklaşık 70.000 kişinin ad-soyad, e-posta, iletişim ve adres bilgilerinin etkilendiği tespit edilmiştir.

Kurul'un Değerlendirmesi:

Kurul, kişisel veri içeren klasörlerin "herkese açık" şekilde bırakılmasını, yetkisiz erişimlerin zamanında tespit edilememesini ve ihlal sonrasında güçlü parola politikasının uygulanmaya başlanmasını dikkate almıştır. Özellikle erişim yetkilerinin uygun şekilde sınırlandırılmaması ve ihlal öncesinde güçlü parola kullanımına ilişkin yeterli tedbirlerin alınmaması, veri sorumlusunun veri güvenliğinin takip ve kontrolünde eksiklik bulunduğunu göstermiştir.

Öne Çıkan Hukuki İlke:

Kişisel verilere erişim yetkileri görev ve ihtiyaçla sınırlı olmalı, kişisel veri içeren dosyalar yetkisiz erişime açık bırakılmamalı ve güçlü parola politikaları ihlal sonrasında değil, önceden uygulanmalıdır.

Kurul'un Kararı:

Veri sorumlusunun KVKK m.12/1 kapsamında gerekli teknik ve idari tedbirleri almaması nedeniyle **700.000 TL** idari para cezası uygulanmasına karar verilmiştir.

Şirketler Açısından Değerlendirme:

Şirketlerin erişim yetki ve kontrol matrisleri oluşturması, kişisel veri içeren dosya ve klasörlerin erişim izinlerini düzenli olarak kontrol etmesi, güçlü parola politikaları uygulaması ve yetkisiz erişimleri zamanında tespit etmeye yönelik loglama ve takip mekanizmalarını etkin şekilde işletmesi gerekmektedir.

10. 08/06/2023 Tarihli ve 2023/1017 Sayılı Karar

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

Konunun Özeti:

Saldırgan, veri sorumlusunun uygulamasındaki bir güvenlik açığını kullanarak iki kez sisteme yetkisiz erişim sağlamış ve veri tabanındaki verileri sistem dışına aktarmıştır. İhlalden kullanıcı adı, ad-soyad, e-posta, doğum tarihi, cinsiyet, ülke ve IP adresi gibi veriler etkilenmiş, etkilenen kişiler arasında çocukların da bulunduğu ve verilerin satışa sunulduğu anlaşılmıştır.

Kurul'un Değerlendirmesi:

Kurul, veri sorumlusunun ihlali kendi sistemleri üzerinden tespit edememesi, düzenli loglama ve güvenlik takibinin yeterli olmaması, ihlal öncesinde sızma testi yapılmaması, aynı güvenlik açığının ikinci kez kullanılmasını önleyecek mekanizmaların bulunmaması ve yama yönetimi uygulamalarının ihlal sonrasında başlatılmasını veri güvenliği bakımından eksiklik olarak değerlendirmiştir.

Öne Çıkan Hukuki İlke:

Sızma testleri, zafiyet taramaları, düzenli loglama, güvenlik takibi ve yama yönetimi ihlal sonrasında alınacak önlemler değil, önleyici güvenlik tedbirlerinin bir parçasıdır.

Kurul'un Kararı:

Veri sorumlusunun KVKK m.12/1 kapsamında gerekli teknik ve idari tedbirleri almaması nedeniyle **1.500.000 TL** idari para cezası uygulanmasına karar verilmiştir.

Şirketler Açısından Değerlendirme:

Şirketlerin kişisel veri işleyen sistemlerinde düzenli sızma testleri ve zafiyet taramaları gerçekleştirmesi, log kayıtlarını düzenli olarak izleyerek yetkisiz erişimleri zamanında tespit edebilecek mekanizmalar kurması ve tespit edilen güvenlik açıklarının hızlı şekilde giderilmesini sağlayacak yama yönetimi süreçlerini işletmesi gerekmektedir. Ayrıca, tespit edilen bir güvenlik açığının tekrar kullanılmasını önlemek amacıyla gerekli kontrollerin uygulanması ve güvenlik testlerinin yalnızca ihlal sonrasında değil, düzenli ve proaktif şekilde gerçekleştirilmesi önem taşımaktadır.

11. 08/02/2024 Tarihli ve 2024/197 Sayılı Karar

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

Konunun Özeti:

Üniversite, öğrencilerin ders devam durumunu takip etmek amacıyla parmak izi sistemi kullanmış ve bazı öğrencilerden açık rıza almıştır. Kurul, parmak izi verisinin özel nitelikli kişisel veri olması ve yoklama için daha az müdahaleci alternatif yöntemlerin bulunması nedeniyle uygulamayı incelemiştir.

Kurul'un Değerlendirmesi:

Kurul, parmak izi verisinin işlenmesinin Kanun'un 6. maddesi kapsamında geçerli bir işleme şartına dayanmadığını ve açık rıza bulunsa dahi işlemenin ölçülülük ilkesine aykırı olduğunu değerlendirmiştir. Ders yoklaması gibi bir amaç için biyometrik veri işlenmesi yerine imza veya benzeri alternatif yöntemlerin kullanılabileceği belirtilmiştir.

Öne Çıkan Hukuki İlke:

Açık rıza alınması, ölçüsüz bir kişisel veri işleme faaliyetini tek başına hukuka uygun hale getirmez. Özellikle biyometrik veri gibi özel nitelikli veriler bakımından amaca ulaşmak için daha az müdahaleci yöntemlerin bulunup bulunmadığı değerlendirilmelidir.

Kurul'un Kararı:

Parmak iziyle yoklama uygulamasının durdurulmasına, mevcut parmak izi verilerinin imha edilmesine ve yoklama işlemlerinin alternatif yöntemlerle yürütülmesine karar verilmiştir.

Şirketler Açısından Değerlendirme:

Şirketlerin biyometrik veri işleme faaliyetlerinde yalnızca geçerli bir işleme şartının bulunup bulunmadığını değil, aynı zamanda işlemenin amaçla bağlantılı, sınırlı ve ölçülü olup olmadığını değerlendirmesi gerekmektedir. Aynı amaca daha az müdahaleci yöntemlerle ulaşılabiliyorsa biyometrik veri işlenmesinden kaçınılmalı, açık rıza alınması da ölçülülük ilkesine aykırı bir uygulamayı meşrulaştırmak için kullanılmamalıdır. Özellikle çalışan devam takibi, giriş-çıkış kontrolü gibi süreçlerde alternatif yöntemlerin değerlendirilmesi önem taşımaktadır.

12. 09/05/2024 Tarihli ve 2024/728 Sayılı Karar

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

Konunun Özeti:

Saldırgan, veri sorumlusunun Başkanı ve CEO'sundan geliyormuş izlenimi veren sahte bir e-posta ile çalışanı yanıltarak üye listesini talep etmiştir. Çalışan, talebi doğrulamadan listeyi harici bir e-posta adresine göndermiş ve 217 kişinin ad-soyad, üyelik numarası ve bazı durumlarda e-posta adresleri saldırgana aktarılmıştır.

Kurul'un Değerlendirmesi:

Kurul, veri sorumlusunun ihlal öncesinde e-posta güvenliğine yönelik riskleri yeterince değerlendirmemesi ve gerekli güvenlik kontrollerini ihlal sonrasında güçlendirmesi ile çalışanın talebi doğrulamadan kişisel veri içeren dosyayı paylaşmasını dikkate almıştır. Çalışanlara eğitim verilmiş olması tek başına yeterli görülmemiş, çalışanların güvenlik farkındalığının uygulamada da sağlanması gerektiği değerlendirilmiştir.

Öne Çıkan Hukuki İlke:

Çalışan kaynaklı oltalama saldırılarına karşı yalnızca eğitim verilmesi yeterli olmayıp, teknik kontroller ve doğrulama mekanizmalarıyla desteklenen bir veri güvenliği sistemi kurulmalıdır.

Kurul'un Kararı:

Gerekli teknik ve idari tedbirlerin alınmaması nedeniyle 750.000 TL, veri ihlalinin Kurul'a süresinde bildirilmemesi nedeniyle 250.000 TL olmak üzere toplam **1.000.000 TL** idari para cezası uygulanmıştır.

Şirketler Açısından Değerlendirme:

Şirketlerin çalışanları hedef alan oltalama ve sosyal mühendislik saldırılarına karşı düzenli farkındalık eğitimleri gerçekleştirmesi ve bu eğitimleri uygulamalı testlerle desteklemesi önemlidir. Özellikle kişisel veri içeren dosyaların harici adreslere gönderilmesi gibi yüksek riskli işlemlerde çok faktörlü kimlik doğrulama, e-posta güvenlik filtreleri, erişim kontrolleri ve ek doğrulama mekanizmaları kullanılmalıdır. Ayrıca çalışanların üst düzey yöneticilerden geldiği görünen olağandışı talepleri doğrulamadan yerine getirmemesi için açık prosedürler oluşturulmalı ve veri ihlallerinin tespit edilmesi halinde Kurul'a en kısa sürede bildirim yapılmasını sağlayacak iç süreçler oluşturulmalıdır.

13. 23/12/2022 Tarihli ve 2022/1375 Sayılı Karar

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

Konunun Özeti:

Bir çalışanın internetten indirdiği programın açılması sonucunda fidye yazılımı veri sorumlusunun 797 sunucusuna bulaşmış ve bazı dosyalar şifrelenmiştir. İhlalden toplam 4.885 kişi etkilenmiş, kimlik, adres, IBAN, telefon, fotoğraf, pasaport ve kan grubu gibi kişisel veriler ihlal kapsamında yer almıştır.

Kurul'un Değerlendirmesi:

Kurul, ihlal öncesinde gerçekleştirilen sızma testlerinde tespit edilen kritik ve yüksek seviyeli güvenlik açıklarının giderilmemesini, zayıf parola politikalarını, "şifreler.txt" gibi dosyalarda kullanıcı adı ve şifrelerin tutulmasını, ağ erişimlerinin yeterince sınırlandırılmamasını, güncel olmayan işletim sistemlerinin kullanılmasını ve çalışanların yeterli güvenlik farkındalığına sahip olmamasını dikkate almıştır. Ayrıca sistemler arasındaki ağ segmentasyonunun yetersiz olması nedeniyle tek bir çalışanın yaptığı işlemin çok sayıda sunucuyu etkilediği değerlendirilmiştir.

Öne Çıkan Hukuki İlke:

Sızma testleri ve güvenlik kontrolleri yalnızca yapılmakla kalmamalı, tespit edilen güvenlik açıkları zamanında giderilmeli ve sonuçları takip edilmelidir. Çalışan farkındalığı ile erişim, parola, yama ve ağ güvenliği gibi teknik tedbirler birlikte uygulanmalıdır.

Kurul'un Kararı:

Gerekli teknik ve idari tedbirlerin alınmaması nedeniyle 800.000 TL, veri ihlalinin Kurul'a 23 gün gecikmeli bildirilmesi nedeniyle 200.000 TL olmak üzere toplam **1.000.000 TL** idari para cezası uygulanmıştır.

Şirketler Açısından Değerlendirme:

Şirketlerin sızma testi ve zafiyet taramalarında tespit edilen açıkları yalnızca raporlamakla yetinmemesi, bunların kapatılmasını ve kapatıldığının doğrulanmasını sağlaması gerekir. Özellikle güçlü parola politikası, MFA, güncel işletim sistemi ve yazılım kullanımı, ağ segmentasyonu, erişim yetkilerinin sınırlandırılması ve yama yönetimi gibi temel güvenlik tedbirleri düzenli olarak kontrol edilmelidir. Ayrıca çalışanların internetten yazılım indirme, şüpheli dosya açma ve güvenlik prosedürlerine aykırı hareket etme risklerine karşı düzenli ve uygulamalı eğitimlerle desteklenmesi önemlidir. İhlal halinde ise olayın tespitinden itibaren Kurul'a en kısa sürede bildirim yapılmasını sağlayacak iç prosedürlerin oluşturulması ve gerekli kayıtların tutulması gerekir.

14. 30/11/2023 Tarihli ve 2023/2007 Sayılı Karar

İşveren tarafından işyerinde kamera vasıtasıyla görüntü ve ses kaydı alınması hakkında;

Konunun Özeti:

İşveren, güvenlik kulübesinde bulunan kamera aracılığıyla görüntü ve ses kaydı almıştır. İlgili kişi, kayıtlar hakkında bilgilendirilmediğini ve ses kaydı alındığını sonradan öğrendiğini belirtmiştir. İşveren ise kayıtların güvenlik ve bir hakkın tesisi amacıyla kullanıldığını savunmuştur.

Kurul'un Değerlendirmesi:

Kurul, güvenliğin sağlanması amacıyla görüntü kaydı alınmasının yeterli olduğu durumda ayrıca ses kaydı alınmasının zorunlu olmadığını değerlendirmiştir. Ses kaydının alınması, aynı amaca ulaşmak için daha sınırlı bir yöntem mevcut olduğundan veri sorumlusunun meşru menfaati kapsamında değerlendirilememiştir. Bu nedenle ses kaydının herhangi bir hukuki işleme şartına dayanmadığı ve hukuka aykırı olduğu sonucuna varılmıştır.

Öne Çıkan Hukuki İlke:

Kamera ile görüntü kaydı alınması hukuka uygun olsa dahi, aynı amaç için gerekli olmayan ses kaydının alınması ayrıca hukuka uygun hale gelmez. Veri sorumlusu, daha az müdahaleci bir yöntemle amacına ulaşabiliyorsa ölçülülük ve zorunluluk ilkelerine uygun hareket etmelidir.

Kurul'un Kararı:

Ses kaydı alınması nedeniyle **125.000 TL** idari para cezası uygulanmasına ve hukuka aykırı şekilde işlenen ses kayıtlarının imha edilerek sonucunun Kurul'a bildirilmesine karar verilmiştir.

Şirketler Açısından Değerlendirme:

İşyerlerinde kamera sistemleri kurulurken görüntü ve ses kaydı ayrı ayrı değerlendirilmelidir. Güvenlik amacı görüntü kaydıyla sağlanabiliyorsa ayrıca ses kaydı alınmamalıdır. Kamera sistemlerinin kullanım amacı, hukuki sebebi, kapsamı ve saklama süresi önceden belirlenmeli, çalışanlar ve diğer ilgili kişiler uygun şekilde aydınlatılmalıdır. Ayrıca hukuka aykırı bir kayıt tespit edilmesi halinde yalnızca silme işleminin yapılması yeterli olmayıp, imha işleminin gerçekleştirildiğini gösteren kayıt ve belgelerin de tutulması önem taşımaktadır.

15. 19/10/2023 Tarihli ve 2023/1796 Sayılı Karar

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

Konunun Özeti:

Teknik bir konfigürasyon sorunu nedeniyle müşterinin ad-soyad, telefon, adres, üyelik ve sipariş bilgilerinin internet sitesi üzerinden üçüncü kişilerin erişimine açık hale geldiği tespit edilmiştir. Veri sorumlusu, sorunun hizmet aldığı veri işleyenin sisteminden kaynaklandığını savunmuştur.

Kurul'un Değerlendirmesi:

Kurul, veri sorumlusunun kişisel veri işleme faaliyetlerinde veri işleyen kullansa dahi sorumluluğunun ortadan kalkmayacağını ve teknik ve idari tedbirlerin alınmasından veri işleyenle birlikte müştereken sorumlu olduğunu değerlendirmiştir. Ayrıca canlıya alınan teknik değişikliklerin yeterli şekilde test edilmemesi ve kontrol edilmemesi nedeniyle kişisel verilere hukuka aykırı erişimin önlenemediği sonucuna varılmıştır.

Öne Çıkan Hukuki İlke:

Veri işleyene ilişkin sözleşmeyle teknik ve idari tedbir alma yükümlülüğünün veri işleyene bırakılması, veri sorumlusunun sorumluluğunu ortadan kaldırmaz. Veri sorumlusu, veri işleyen tarafından yürütülen süreçleri de denetlemeli ve gerekli kontrolleri yaptırmalıdır.

Kurul'un Kararı:

Kişisel verilerin internet sitesinde sınırsız kişilerin erişimine açılması nedeniyle veri sorumlusuna **200.000 TL** idari para cezası uygulanmıştır.

Şirketler Açısından Değerlendirme:

Şirketler, dışarıdan hizmet aldıkları veri işleyenlerin faaliyetlerini yalnızca sözleşme üzerinden kontrol etmekle yetinmemeli, teknik ve idari tedbirlerin gerçekten uygulanıp uygulanmadığını düzenli olarak denetlemelidir. Özellikle internet sitesi, CDN, bulut hizmetleri ve benzeri teknik sistemlerde yapılan değişiklikler canlıya alınmadan önce güvenlik ve erişim kontrollerinden geçirilmelidir. Veri işleyen kaynaklı bir teknik sorun meydana gelmesi halinde dahi veri sorumlusunun Kanun'un 12'nci maddesi kapsamındaki sorumluluğunun devam ettiği dikkate alınarak, hizmet sağlayıcılarla yapılan sözleşmelerde denetim, güvenlik, test, ihlal bildirimi ve müdahale süreçleri açıkça düzenlenmelidir.

16. 21/09/2023 Tarihli ve 2023/1610 Sayılı Karar

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

Konunun Özeti:

Veri sorumlusu, canlı maç yayınını izlemek isteyen üyelerden ticari elektronik ileti onayı alınmasını zorunlu tutmuştur. İlgili kişi, temel hizmetlerden biri olmasa dahi bu uygulamanın açık rızanın özgür iradeyle verilmesi ilkesine aykırı olduğunu ileri sürmüştür.

Kurul'un Değerlendirmesi:

Kurul, bir hizmetten yararlanmanın ticari ileti gönderilmesine yönelik rıza/onay verilmesi şartına bağlanmasının, açık rızanın özgür iradeyle verilmesi unsurunu zedelediğini değerlendirmiştir. Bu nedenle söz konusu veri işleme faaliyetinin Kanun'un 5'inci maddesinde yer alan geçerli bir işleme şartına dayanmadığı ve veri güvenliği yükümlülüklerinin ihlal edildiği sonucuna varılmıştır.

Öne Çıkan Hukuki İlke:

Bir ürün veya hizmetin sunulması, kişisel verilerin pazarlama veya ticari iletişim amacıyla işlenmesine yönelik rıza verilmesi şartına bağlanmamalıdır. Rızanın hizmetten yararlanabilmek için zorunlu hale getirilmesi, özgür irade unsurunu zedeleyebilir.

Kurul'un Kararı:

Veri sorumlusuna **250.000 TL** idari para cezası uygulanmasına ve canlı yayın hizmetinin ticari ileti onayı verilmesi şartına bağlanması uygulamasına son verilmesine karar verilmiştir..

Şirketler Açısından Değerlendirme:

Şirketler, sundukları ürün veya hizmetlerin pazarlama amaçlı veri işleme faaliyetlerine yönelik açık rıza veya ticari ileti onayı verilmesine bağlanıp bağlanmadığını gözden geçirmelidir. Hizmetin sunulması için gerekli olmayan pazarlama faaliyetleri ayrı ve isteğe bağlı olarak kurgulanmalı, hizmetten yararlanmak isteyen kişilerin pazarlama iletişimine onay vermemesi hizmete erişimlerini engellememelidir. Ayrıca açık rıza ile 6563 sayılı Kanun kapsamındaki ticari elektronik ileti onayının hukuki nitelikleri birbirinden ayrıştırılmalı ve her bir süreç için uygun hukuki dayanak belirlenmelidir.