GRC | LEGAL HUKUK BÜROSU

BÜLTEN

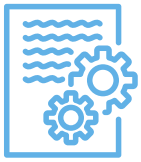
KİŞİSEL VERİLERİN KORUNMASI HUKUKU

Kişisel Verilerin Korunması Kanunu ve ikincil mevzuatı yürürlük tarihinden bugüne güncellemesi sık yaşanan ve yaşayan bir hukuktur. Yalnızca Kanun, Yönetmelik ve Tebliğ ile değil, Kurul Kararları, İlke Kararları ve Kurul Karar Özetleri ile de veri koruma alanıyla ilgili birçok usul ve esas belirlenmektedir. Dolayısıyla aylık bültenlerimiz, Kişisel Verileri Koruma Kurulu uygulamalarından ilgililerini haberdar etmeyi ve güncelliği sağlamayı amaçlamaktadır.

Haziran ayında Kişisel Verileri Koruma Kurulu tarafından **Çerez Uygumaları Hakkında Rehber**, **Sadakat Programlarının Kişisel Verilerin Korunması Mevzuatı Kapsamında İncelenmesine İlişkin Rehber Taslağı** ve **Veri İhlal Bildirimleri** yayımlanmıştır.

VERİ İHLAL BİLDİRİMLERİ

"Veri güvenliğine ilişkin yükümlülükler" başlıklı KVKK m. 12/5. *"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."* hükmünü amirdir.



2022 Haziran ayında Kişisel Verileri Koruma Kurumu internet sitesi olan www.kvkk.gov.tr alan adlı sitede **beş** adet veri ihlal bildirimi yayınlanmıştır.

2 Haziran - MBtech Mühendislik ve Danışmanlık Ltd. Şti.

Veri sorumlusunun **fidye yazılımı saldırısı**na maruz kaldığı, 28.05.2022 tarihide tespit edilen ihlalin başlama tarihinin araştırıldığı, etkilenen kişisel veri kategorilerinin detayları hala araştırılmakla birlikte; **kimlik, iletişim, lokasyon, özlük, müşteri işlem, finans, mesleki deneyim ve görsel ve işitsel kayıtlar**dan oluştuğu; etkilenen kişi sayısının 500 ve kişilerin çalışanlar, kullanıcılar ve müşteriler/potansiyel müşteriler olduğu bilgilerine yer verilmiştir.

7 Haziran - Pegasus Hava Taşımacılığı Anonim Şirketi

- Veri sorumlusu çalışanı uçuş ekiplerinin uçuş planlamalarının yapılması ve gerekli koordinasyonun sağlanması amacıyla kurulan servisin **tarayıcı listeleme özelliğinin açık olması** sebebi ile sistemlere yetkisiz erişim söz konusu olduğu,
- 21.03.2022 tarihinde sistemde bulunan ve açık olduğu tespit edilen browser listening (tarayıcı listeleme) özelliğinin 24.03.2022 tarihinde kapatılarak güvenlik açığının giderildiği, ihlalin ise daha sonra **bilgi güvenliği istihbarat servisleri izleme araçları** üzerinden 31.05.2022 tarihinde tespit edildiği, sosyal medya hesapları ve bazı internet sitelerinde, konu hakkında yetkisiz erişim yapan kişilerce kendilerini tanıtıcı metinler yayımlandığı, yetkisiz erişim sağlayan üçüncü kişilerin paylaşımları üzerine, kendileri ile iletişime geçilerek, erişilen **kişisel verilerin imha edilmesinin talep edildiği**,
- ihlalden etkilenen kişisel verilerin kimlik, iletişim ve lokasyon kategorileri dahilinde; **pilot ve kabin ekibi çalışanlarının** adı, soyadı, telefon numarası, e-posta adresi, unvanı, geçmiş tarihlerde yapmış oldukları uçuş bilgileri, uçuş lokasyonları ile bu çalışanların bir kısmının fotoğraf ve imza görselleri olduğu, etkilenen kişi sayısının henüz tespit edilemediği bilgilerine yer verilmiştir.

22 Haziran - Barçın Spor Malzemeleri Ticaret ve Sanayi Anonim Şirketi

187.930 ilgili kişiye ait kişisel verilerin bulunduğu **excel formatındaki dosyanın csv formatına dönüştürülmesi için kullanılan ara yazılım program** aracılığıyla verilerin üçüncü kişiler tarafından elde edildiği, ihlalin bir internet sitesinde yer alan haber aracılığıyla öğrenildiği, ihlalden etkilenen ilgili kişi gruplarının **kullanıcılar, müşteriler ve potansiyel müşteriler** ve kişisel veri kategorilerinin **kimlik** (isim, soyisim, cinsiyet), **iletişim** (telefon numarası, e-mail adresi), **müşteri işlem** (müşteri id'si) ve diğer (siteye üye olduğu tarih) bilgileri olduğu, üçüncü kişilerin eline geçmiş olan excel tablosunda yer alan müşteri id'lerinin veri sorumlusu sistemlerimizdeki müşteri id'leriyle uyuşmadığı, etkilenen kişi sayısının **187.930** olduğu bilgilerine yer verilmiştir.

29 Haziran - Tofisa Tekstil Sanayi ve Ticaret Limited Şirketi

Çağrı merkezine müşterilerden gelen aramalarda, **teslim almadıkları kargo bedellerine ilişkin icra takibi başlayacağına ilişkin çeşitli hukuk bürolarından mesaj ve arama aldıkları** bilgisinin verildiği, kontroller sonucunda çağrı merkezini arayanların, **veri işleyen** (Dolunay Kargo Lojistik Otomotiv İnşaat Sanayi ve Tic. Ltd Şti.) **ile paylaşılan kişiler olduklarının tespit edildiği,** veri sorumlusunun veri işleyen ile iletişime geçmek istediği ancak başarısız olduğu, ilgili kişilere ait **isim, soyisimleri, telefon numaraları, e-posta adresleri**nin veri işleyen ile paylaşılmakta olduğu, isim, soyisim ve telefon numaralarının hukuka aykırı olarak kullanıldığı, etkilenen ilgili kişilerin **müşteriler ve potansiyel müşteriler** ve kişi sayısının **42.373** olduğu ve bu sayının veri işleyen kayıtlarında bulunan kargo teslimi yapılmayan kişi sayısı olduğu bilgilerine yer verilmiştir.

29 Haziran - ARG Denizcilik İnşaat Otomotiv Sanayi ve Ticaret Ltd. Şti, İstek Gemi İnşa Bakım İnşaat Hırdavat Sanayi ve Ticaret Ltd. Şti, Safter Ulubay

İhlalin bilgisayardaki **dosyalara erişimin engellenmesi** suretiyle gerçekleştiği ve kaynağının sabotaj olarak belirtildiği, 21.06.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği, ihlalden veri sorumlusu çalışanlarına ait kimlik, iletişim ve özlük bilgilerinin etkilendiği, her bir veri sorumlusu için ihlalden etkilenen kişi sayısının tahmini 2000 olduğu bilgilerine yer verilmiştir.

KAMUOYU DUYURUSU

16 Haziran – "Sadakat Programlarının Kişisel Verilerin Korunması Mevzuatı Kapsamında İncelenmesine İlişkin Rehber Taslağı" Hakkında Kamuoyu Duyurusu

Günümüzde müşteri bağlılığını geliştirmeye yönelik sadakat programları pek çok işletme tarafından uygulanmakta ve bu programlar yoluyla veri sorumluları tarafından ilgili kişilerin muhtelif kişisel verileri işlenmektedir. Bu kapsamda Kurum tarafından hazırlanan Rehber Taslağı kamuoyu incelemesine açılmış olup 16.07.2022 tarihine kadar öngörülen bir aylık zaman diliminde görüş ve değerlendirmeler kabul edilmektedir.

Sadakat Programlarının Kişisel Verilerin Korunması Mevzuatı Kapsamında İncelenmesine İlişkin Rehber Taslağı

Rehber kapsamında sadakat programları, *"Müşterinin işletme açısından belirli ya da belirlenebilir olmasını sağlayacak kişisel verilerinin işlenmesi suretiyle alışveriş karşılığında çeşitli kriterler çerçevesinde müşteriye puan/hediye/avantaj sağlanması,* ***müşterinin alışveriş alışkanlıklarının takip edilmesi,*** *işlenen kişisel verilerin analiz edilmesi suretiyle* ***kişiselleştirilmiş ürün/hizmet teklifleri sunulması*** *gibi stratejilerin* ***tamamının veya bazılarının*** *firmalarca tek taraflı veya bir program ortaklığı kapsamında uygulanması yoluyla* ***müşteriye menfaat sağlarken aynı zamanda uygulayıcı firmanın satış ve karlılığını artırmayı hedefleyen programlar"*** olarak tanımlanmıştır.

Rehber Taslağı'nda sadakat türlerinin farklı çeşitleri tanımlanmaktadır. Bunlar; Puan Tabanlı Sadakat Programları, Katmanlı Sadakat Programları, Ücret Tabanlı Sadakat Programları / VIP Üyelik Programları, Geri Ödemeli Sadakat Programları, Değere Dayalı Programlar, Ortaklık Programları, Oyun Programları ve Karışık Sistemli Programlar olarak sayılmıştır.

Sadakat programları kapsamında işlenen kişisel veriler genel olarak, i. müşteri tarafından aktif ve gönüllü bir şekilde sağlanan kişisel veriler, ii. müşteri tarafından pasif olarak sağlanan kişisel veriler (sadakat programının mobil uygulama üzerinden kullanılması halinde IP'sinin işlenmesi, konum verisinin işlenmesi gibi), iii. diğer kaynaklardan sağlanan müşteri verileri (bir müşteri tarafından aktif olarak sağlanan verileri, pasif olarak toplanan diğer kullanıcı verilerini veya tanımlanmamış veri kümelerinden alınan verileri analiz ederek ve bu birleşik verilere dayanarak analizler yapılması yoluyla elde edilen veriler) olarak sınıflandırılabilir.

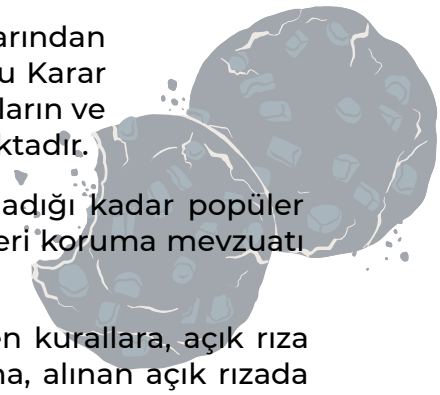
Sadakat programlarında yürütülen faaliyeti **sadakat sözleşmesi** ile sağlayan işletmelerin *kazanılan puanların hesaplanması, puanlara dair bilgi verilmesi, kullanım süresi dolacak puanların hatırlatılması* gibi işlemlerde sözleşmenin ifası hukuka uygunluk nedenine dayanılması mümkün kılınmış olup bu minvaldeki bildirimler için Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik m. 7 uyarınca ayrıca onay alınmasına gerek bulunmadığı yorumu yapılmıştır.

Hizmetin kural olarak açık rıza şartına bağlanmaması gerekliliği sadakat uygulamaları bağlamında işlenen kişisel veriler açısından da geçerliliğini koruyacaktır ancak belli koşulların varlığı halinde sadakat uygulamasına katılmak için verilerin işlenmesine açık rıza verilmesinin veri sorumlusunca talep edilmesi, hizmetin rıza şartına bağlanması olarak değerlendirilmeyebilecek ve hukuka uygun olduğu kabul edilebilecektir. **Sadakat programları kapsamında açık rıza verilmemesi halinde ürün/hizmetin sunulmaması değil, ürün/hizmetin ek menfaat olmaksızın sunulması söz konusu olmaktadır.**

Kişilerin mağazada alışveriş yaptıkları durumda SMS ile telefonlarına iletilen kodu görevliye söylemeleri neticesinde ticari elektronik ileti gönderimi yapıldığına ilişkin gelen ihbarlara da bu Rehber Taslağı'nda aşağıdaki şekilde yanıt verilmiştir:

- Kişilerin telefonuna gönderilecek olan SMS'in amacının ne olduğu ve bu SMS ile iletilen kodun verilmesi halinde ne gibi sonuçlar doğuracağı hususunun, katmanlı aydınlatmanın bir gereği olarak ilk aşamada veri sorumlusunun mağazalarda yetkilendirdiği kişiler tarafından ilgili kişilere açık ve anlaşılır bir biçimde aktarılması, ayrıca aydınlatma yükümlülüğünün yerine getirilebilmesini teminen yine söz konusu SMS içeriklerinde de gerekli kanalların sağlanmasının,
- Mağazalarda gerçekleştirilen alışverişler ile ilgili ödeme esnasında ilgili kişilere SMS ile doğrulama kodu gönderilerek üyelik sözleşmesi, kişisel verileri işleme izni, ticari elektronik ileti onayı vb. birbirinden farklı işleme faaliyetlerinin tek bir eylemle gerçekleştirilmesine yönelik uygulamalara son verilmesi, söz konusu işleme faaliyetlerine yönelik seçenek sunulmak suretiyle ayrı ayrı açık rıza alınmasının,
- Bunun yanı sıra, veri sorumlularınca açık rıza alınması ve aydınlatma yükümlülüğü işlemlerinin birlikte gerçekleşmesine neden olabilecek durumlardan kaçınılmasının,
- Ticari elektronik ileti gönderimi için açık rıza alınmasını teminen SMS doğrulama kodu gönderilmesine yönelik bir uygulamaya gidilmesi halinde ise söz konusu işlemde alınacak açık rızanın tüm unsurları kapsamasının önem arz ettiğine dair bir kamuoyu duyurusu Kurumun internet sayfasında yayımlanmış olup sadakat programı uygulayıcısı veri sorumlularının söz konusu hususlara da dikkat etmeleri gerekmektedir.

ÇEREZ UYGULAMALARI HAKKINDA REHBER



Güncel tarihli Kurul Karar Özeti ile çerez uygulamalarından kaynaklanan bir ihlale 800.000 TL idari para cezası verilmiştir. Bu Karar Özeti ve başkaca sinyaller ile Kurul'un radarında dijital uygulamaların ve bunların ihtiva ettikleri açıklıkların bulunduğu kanaatine varılmaktadır.

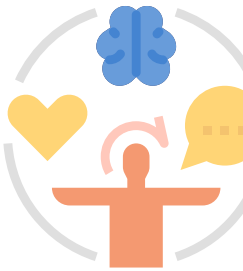
E-ticaret ve online satış gibi uygulamaların daha önce hiç olmadığı kadar popüler olduğu bu ekosistemde Çerez Uygulamaları Hakkında Rehber veri koruma mevzuatı ile ilgilenen tüm paydaşlar için beklenen bir haber niteliğindedir.

Rehber'de çerez türleri ve tanımlarına, dikkate alınması gereken kurallara, açık rıza gerektiren ve gerektirmeyen senaryolardaki çerez kullanımlarına, alınan açık rızada bulunması gereken unsurlara, uygun aydınlatmanın yapılmasına oldukça yoğun teknik detaylarla birlikte yer verilmektedir.

Önemli olduğunu düşündüğümüz noktalara aşağıda özet olarak değinilmiştir.

AÇIK RIZA İŞLEME ŞARTI DAHİLİNDEKİ ÇEREZ KULLANIM SENARYOLARI

Sosyal Eklenti Takip Çerezleri: Birçok sosyal ağ, üyeleri tarafından "açıkça talep edildiği" kabul edilebilecek bazı hizmetleri sağlamak için, internet sitesi sahiplerinin internet sitelerine entegre edebilecekleri sosyal eklenti modülleri sunmaktadır. Bu modüller davranışsal reklamcılık, analitik veya pazar araştırması gibi ilave amaçlarla, üye olan/olmayan kişileri üçüncü taraf çerezler yardımıyla izlemek için kullanılabilmektedir. Bu çerezlerin kullanıcı tarafından açıkça talep edilen bir işlevselliği sağlamak için **"kesinlikle gerekli"** olduğu kabul edilemeyecektir. Açık rıza olmaksızın sosyal ağların, ağlarına üye olmayanlar hakkında sosyal eklentiler aracılığıyla veri toplaması için herhangi bir yasal dayanağın bulunması olası değildir.



Çevrim İçi Davranışsal Reklamcılık Çerezleri: Davranışsal reklamcılık için kullanılan çerezler açık rıza gerektirmektedir. Bu durumda açık rıza gerekliliği; doğal olarak gösterim sıklığı, finansal kayıt tutma, reklam ortaklığı, tıklama sahtekârlığını algılama, araştırma ve pazar analizi, ürün geliştirme ve hata ayıklama amacıyla kullanılan çerezler de dâhil olmak üzere reklamcılık amacıyla kullanılan ilgili çerezleri kapsar; zira bu amaçlardan hiçbirinin, Kriter B'nin gerektirdiği şekilde, kullanıcı tarafından açıkça talep edilen bilgi toplumu hizmetleri kapsamında bir hizmet ya da işlevsellikle ilgili olmadığı açıktır.

Çerez duvarı bir ziyaretçinin internet sitesinde yer alan tüm çerezlerin kullanılmasına onay vermedikçe internet sitesinin içeriğini görüntülemesini engelleyen uygulamadır. Açık rızanın özgür bir biçimde verilebilmesi kapsamında çerez duvarlarının ilgili kişinin rızasını ortaya koyarken gerçek bir seçim yapmasını engellemesi söz konusu olabilir. Her olay özelinde değerlendirme yapılması kaydıyla, ilgili kişilerin bir hizmeti elde edebilmeleri için çerez duvarı dışında belirli birtakım adil alternatifler sunulması söz konusu olabilecektir.

Çerez Kullanımında Doğru Uygulama

Çerez kapsamında açık rıza alınırken siteye girildiği anda bir çerez yönetim paneli (pop-up ya da bant gibi uygulamalar) çıkması ve söz konusu panelde **eşit derecede** *(renk, büyüklük, punto açısından)* **"kabul et", "reddet" ve "tercihler" butonlarının sunulması** iyi uygulama örneği olarak belirtilmiştir.

Kişisel verilerin elde edilmesi sırasında aydınlatma yükümlülüğünün yerine getirilmesi gerekmekte olup söz konusu **çerez yönetim paneline, çerezler yoluyla kişisel veri işlenmesine dair bir açıklama veya gerekirse bir link konulması** doğru bir uygulama olarak belirlenmiştir. Bu kapsamda, **açık rıza ile işlenmesi gereken çerezlerin yönetim panelinde ilk elde pasif biçimde gelmesi önem arz etmektedir.**

Çevrim içi reklamcılık çerezlerinin kullanımında, kullanım sözleşmesi veya koşulları gibi belgeler içerisine iliştirme (bundled) yöntemiyle açık rıza alınmasının mümkün olmayacağına **da dikkat etmek gerekmektedir.**