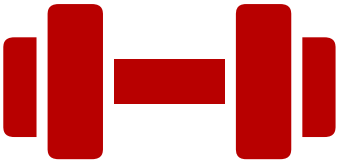
MAYIS-HAZİRAN 2020

KVKK KURUL KARARLARI

BERKERBERKER

04.05.2020
Karar Tarihi : 27/02/2020
Karar No : 2020/167
Konu Özeti : Spor salonu hizmeti sunan sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun Kararı



Spor salonu hizmeti sunan şirketin (veri sorumlusu), üyelerinin giriş-çıkış kontrolünde el okutma sistemine geçilmesi gibi biyometrik verileri içeren bazı özel nitelikli kişisel verileri işlemesi ve bu bilgilerin güvenli şekilde muhafaza edildiğinden şüphe duyulması üzerine ilgili kişilerce Kuruma intikal ettirilen şikâyetin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27/02/2020 tarih ve 2020/167 sayılı Kararı ile;

6698 sayılı Kanunun "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6 ncı maddesinde kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olarak belirlendiği, özel nitelikli kişisel veriler arasında yer alan biyometrik veri tanımına ise Kanunda yer verilmemekle birlikte, 25.05.2018 tarihinde yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğünde (GDPR) biyometrik verinin; "yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler" olarak tanımlandığı,

GDPR'ın Recital bölümünün 51 inci maddesinde de biyometrik verilerle ilgili açıklamalara yer verildiği ve fotoğrafların işlenmesinin doğrudan biyometrik veri olarak nitelendirilemeyeceği, yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde, bu verilerin biyometrik verilerin tanımı kapsamında kabul edileceği açıklamalarına yer verildiği, dolayısıyla bir verinin biyometrik veri kapsamında değerlendirilebilmesi için o verinin sadece o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olmasının kriter alındığının değerlendirildiği,

Danıştay 15. Dairesinin 2014/4562 Esas sayılı kararında ise biyometrik yöntemlerin, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği belirtilerek, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerin bulunduğunun ifade edildiği

hususlarından hareketle bir spor tesisine giriş esnasında el ve parmak izinin taranması suretiyle kişilerin kimlik doğrulamasının yapılması hususunda adı geçen veri sorumlusunun özel nitelikli kişisel veri niteliğindeki biyometrik veri işleme faaliyetinde bulunduğunun değerlendirildiği,

Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinde de, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin ancak hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceğinin düzenlendiği,

Bu ilkelerden, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin, işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemesi gerektiği,

Ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği, kişisel verilerin işlenmesinin ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın, aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar için ve gerektiği kadar toplanması, amacın gerektirdiği yerlerde kullanılması ve amaç için gerekli olandan uzun süre tutulmaması gerektiği,

dikkate alındığında spor salonuna giriş için veri sorumlusu tarafından uygulanan "el ve parmak izi taraması" sisteminin, üyelerin açık rızası olsa bile hizmetten faydalanmak için üyelere sunulmasının, kişisel verilerin işlenmesinde ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olmadığı değerlendirilmiş olup, bu itibarla;

- Spor kulübüne giriş ve çıkışların kontrolü amacıyla getirilen avuç içi izinin taranması suretiyle kişilerin kimlik doğrulamasının yapılmasının, biyometrik veri kapsamında değerlendirilmeyeceği ve bu sistemin yanı sıra dileyen üyelerin kart göstermek suretiyle tesisten faydalandıkları iddia

edilse de avuç içi tarama sisteminin biyometrik veri tanımını karşıladığı, bu sistemin yanı sıra seçimlik hak sunulsa bile biyometrik veri içeren bir sistemin tesis giriş ve çıkışlarında kullanılmasının Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinin (2) numaralı fıkrasının (ç) bendindeki ölçülülük ilkesine aykırı olduğu kanaatine varılması nedeniyle;

Şirketin söz konusu uygulamasının Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği sonucuna varıldığından, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında veri sorumlusu hakkında **225.000 TL** idari para cezası uygulanmasına,

- Veri sorumlusu tarafından bugüne kadar işlenen ve muhafaza edilen el, parmak ve avuç izi ile ilgili verilerin Kanunun 7 nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine uygun olarak ivedilikle yok edilmesi, eğer ilgili özel nitelikli verilerin üçüncü kişilere aktarılması söz konusu ise, yok etmeye yönelik işlemlerin bu verilerin aktarıldığı üçüncü kişilere ivedilikle bildirilmesinin sağlanması ve biyometrik veri ile giriş çıkış işlemleri yapılmasının ve biyometrik veri işlemenin durdurulması hususunda **veri sorumlusunun talimatlandırılmasına,**
- İlgili kişinin veri sorumlusuna bünyesinde bulunan kişisel verilerinin silinmesi talebine istinaden, talebin yerine getirildiğine ve söz konusu kişisel verilerin silindiğine ilişkin ilgili kişinin bilgilendirilmesi ve söz konusu silme işlemine ilişkin tevsik edici bilgi ve belgelerin Kurumumuza iletilmesi hususunda **Şirketin talimatlandırılmasına,**
- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerinin de hatırlatılması suretiyle veri sorumlusunun **Aydınlatma Metninin usulüne uygun olarak güncellenmesi hususunda talimatlandırılmasına**

karar verilmiştir.

07.05.2020
Karar Tarihi : 27/02/2020
Karar No : 2020/173
Konu Özeti : Amazon Turkey Perakende Hizmetleri Limited Şirketince işlenen kişisel veriler hakkında yapılan başvuru

Kurumumuza intikal eden bir ihbar dilekçesinde ve eklerinde özetle;

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (6563 sayılı Kanun) uyarınca hizmet sağlayıcı ve aracı hizmet sağlayıcı niteliğinde olan www.amazon.com.tr üzerinden yürütülen faaliyetlerin kişisel verilerin korunması mevzuatına uygun olması gerektiği; ancak ilgili site üzerinden yürütülen faaliyetler ile mevzuatın ihlal edildiği,
- Amazon.com.tr internet sitesi ve bağlı uygulamalar aracılığıyla sunulan hizmetlere ilişkin olarak ne üyelik hesabı oluşturulurken ne de alışveriş yapılırken, reklam, kampanya veya promosyon amacıyla elektronik ticari ileti gönderebilmek için açık rıza alınmadığı, açık rıza dışında bir işleme nedeninin varlığına ilişkin açıklama yapılmadığı,
- Sitenin “Kullanım ve Satış Şartları” sayfasının girişinde “Amazon Europe Core SARL, Amazon Turkey Perakende Hizmetleri Limited Şirketi ve/veya iştirakleri ("Amazon"), Amazon.com.tr' yi (internet sayfası) ziyaret ettiğinizde veya burada alışveriş yaptığınızda, Amazon ürünlerini veya hizmetlerini kullandığınızda, mobil Amazon uygulamalarını kullandığınızda veya yukarıdakilerle bağlantılı olarak Amazon tarafından sunulan hizmetleri kullandığınızda (toplu olarak "Amazon Hizmetleri") size internet sayfası özellikleri ve diğer ürünler ve hizmetler sunmaktadır. Amazon Hizmetleri aracılığıyla kişisel bilgilerinizin nasıl toplandığını ve işlendiğini anlayabilmek adına lütfen Gizlilik Bildirimimizi ve Çerezler Bildirimimizi inceleyin.” ifadesine yer verildiği,
- Elektronik İletişimler başlıklı birinci maddede “Herhangi bir Amazon Hizmeti'ni kullandığınızda veya masaüstünüzden veya mobil cihazınızdan bize e-postalar, SMS veya diğer iletişimler gönderdiğinizde bizimle elektronik olarak iletişim kurmuş olursunuz. Sizinle, örneğin e-posta, SMS, uygulama içi anlık iletişimler gibi çeşitli şekillerde veya internet sayfasında e-posta mesajları veya iletişimler göndererek veya yayınlayarak veya Mesaj Merkezimiz gibi diğer Amazon Hizmetleri aracılığıyla elektronik olarak iletişim kuracağız. Sözleşmesel amaçlı olarak, bizden elektronik olarak iletişim almaya onay vermektesiniz ve size elektronik olarak temin ettiğimiz tüm sözleşmelerin, bildirimlerin, açıklamaların ve diğer iletişimlerin, uygulanan kanunlar farklı bir iletişim şeklini öngörmediği sürece, söz konusu iletişimlerin yazılı olmasına ilişkin her türlü yasal gerekliliğe uygunluk gösterdiğini kabul etmektesiniz.” ifadesinin kullanıldığı,

- Bu ifadeler birlikte değerlendirildiğinde, amazon.com.tr sitesini sadece ziyaret eden bir kişinin ilgili hükümleri kabul ettiği ve sadece internet sitesini ziyaret etmekle elektronik olarak iletişim almaya onay verdiği şeklinde bir uygulamaya gidildiğinin görüldüğü,
- Amazon hizmetini kullanmak suretiyle elektronik iletişime onay vermiş sayılmanın ve bu nedenle kullanıcılara elektronik ticari ileti göndermenin 6698 sayılı Kanunun 5'inci maddesinin 2'inci fıkrasında yer alan "bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla gerekli olma" şeklindeki hukuka uygunluk sebebi kapsamında değerlendirilemeyeceği,
- Alışveriş yapabilmek için zorunlu olan üye hesabı oluşturulması amacıyla "Kullanım ve Satış Şartları"nı kabul ederek elektronik iletişim izni verilmiş sayılmanın özgür irade ile verilmiş bir açık rıza olarak değerlendirilemeyeceği, nitekim Kişisel Verileri Koruma Kurumu (Kurum) internet sitesinde yer verilen karar özetleri bölümünde, "Açık rızanın Hizmet Şartına Bağlanması" başlığı altında hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağının belirtildiği,
- amazon.com.tr "Gizlilik Bildirimi" sayfasının "Amazon Kişisel Bilgilerinizi Paylaşıyor mu?" kısmının "Kişisel Bilgilerin Türkiye Dışına Aktarılması" alt başlığı altında "Kişisel bilgilerinizi saklamak ve işbu Gizlilik Bildirimi'nde açıklanan amaçlar çerçevesinde işlemek için Avrupa Birliği'ne ve Avrupa Birliği'nden Amerika Birleşik Devletleri'ne aktarabiliriz." şeklindeki ifadeden kişisel verilerin yurt dışına aktarıldığının anlaşıldığı; ancak hâlihazırda amazon.com.tr internet sitesi ve bağlı mobil uygulamalar aracılığı ile sunulan hizmetlere ilişkin ne üyelik hesabı oluşturulurken ne de alışveriş yapılırken, kişisel verilerin yurt dışına aktarılması için açık rıza alınmadığı,
- yurt dışına aktarıma ilişkin olarak Kurul izni alınmamış ise, herhangi bir açık rıza da alınmadığından 6698 sayılı Kanunun 9'uncu maddesinin ihlal edilmiş olacağı, bunun da Kurulca yapılacak inceleme ile ortaya çıkarılabileceği

ifade edilerek, yukarıda belirtilen hususlar doğrultusunda konunun Kurumumuzca incelenmesi ve gereğinin yapılması talep edilmektedir.

Söz konusu başvuruya ilişkin olarak Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/140 sayılı Kararı ile resen inceleme başlatılmasına karar verilmiş olup, Kurumumuz tarafından 27.06.2019 tarihli dilekçede belirtilen iddialar ile ilgili olarak gerekli incelemelerin yapılabilmesini teminen veri sorumlusundan söz konusu iddialar karşısındaki savunması ve savunmasına esas bilgi ve belgeler istenilmiştir.

Veri sorumlusundan 17.07.2019 tarihinde alınan yazıda ise özetle;

- Hukuka aykırı olarak ticari elektronik ileti gönderildiğine ilişkin iddiaların dayanaktan yoksun olduğu, herhangi bir kanıtlayıcı belgeye dayanmadığı ve başvuranın söz konusu taleplerini Ticaret Bakanlığına iletmesi gerektiği,
- Kurulun ticari elektronik iletiler gibi ilke kararlarını ve Kurulun bu alandaki yetkisini kabul etmek ve saygı göstermekle birlikte, konuya ilişkin usul ve esasların münferiden elektronik ticarete ilişkin mevzuat kapsamında düzenlenmiş olduğu, ihbar edenin bu mevzuat kapsamındaki şikayet mekanizmasını kullanmak yerine şikayetini varsayımsal tahminlere dayandırarak Kurumumuza iletmiş olduğu,
- Amazon Turkey'in, müşterilerinin kişisel verilerini yürürlükteki mevzuata uygun işlemek konusunda şeffaflık sağlamak amacıyla "Kullanım Koşulları" ve "Gizlilik Bildirimi" metinlerini sunduğu,
- Yalnız hesap oluşturulmasından sonra kayıtlı müşterilerle Amazon ürün ve hizmetlerine ilişkin elektronik iletişim kurulduğu; Amazon hesabı oluşturulduğunda ilgili müşterinin "Amazon Hesabınızı Oluşturun" sekmesine tıklayarak "Gizlilik Bildirimi"ni de kabul ettiği ("Hesap oluşturarak işbu Gizlilik Bildirimi'nde belirtilen uygulamaları kabul etmektesiniz."); aynı şekilde kayıtlı bir müşteri site üzerinden sipariş verdiğinde kendisine "Gizlilik Bildirimi"nin kabul edildiğine dair tekrar hatırlatma yapıldığı ("Sipariş verdiğinizde Amazon.com.tr'nin Gizlilik Bildirimini, Kullanım ve Satış Koşullarını ve Çerez Bildirimini kabul etmiş olursunuz."),
- Amazon Turkey'in ayrıca kayıtlı müşterilerine ticari elektronik ileti almak istedikleri alanları kolayca seçmeleri, sınırlandırmaları veya diledikleri zaman ticari elektronik ileti almayı reddetmeleri için imkan sağladığı,
- Kayıtlı müşterilerin kişisel verilerinin Türkiye dışına aktarıldığından/aktarılabileceğinden sadece haberdar olmadığı ayı zamanda "Gizlilik Bildirimi"ni onaylayarak bu hususu kabul etmiş olduğu,
- Amazon Turkey'in yurt dışına veri aktarım taahhütnameleri ile ilgili yazışmaların Kurumumuzla sürdürülmekte olduğu,
- Yukarıda yer alan açıklamalar ışığında Amazon Turkey'in kişisel verileri yurtdışına hukuka aykırı aktardığı, e-ticaret mevzuatına aykırı hareket ettiği iddialarının asılsız olduğu ve varsayımlara dayandığı ifade edilerek, ihbarın dayanaktan yoksun olması nedeniyle reddedilmesi gerektiği belirtilmiştir.

Öte yandan, konuya ilişkin olarak Kurumumuza ihbarda bulunan şahsın Ticaret Bakanlığı'na yapmış olduğu Amazon.com.tr uygulamalarının elektronik ticaret ve kişisel verilerin korunması mevzuatı hükümlerine aykırılık teşkil ettiği yönündeki başvurusu Bakanlığın 17.04.2019 tarihli 43541135 sayılı yazısı ile "konunun KVKK çerçevesinde değerlendirilmesi" talebiyle Kurumumuza iletilmiştir.

Kurumumuza intikal eden ihbar, ilgili kişinin iddiaları, veri sorumlusundan alınan bilgi ve belgeler ve ilgili mevzuat hükümleri çerçevesinde aşağıda başlıklar halinde değerlendirilmiştir.

1. **6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun)** 5'inci maddesinin (1) numaralı fıkrası hükmü gereğince kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. **Maddenin (2) numaralı fıkrasında ise, ilgili kişinin açık rızası olmaksızın kişisel verilerin hangi hallerde işlenebileceği düzenlenmiştir.**

Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin 5'inci maddesinin (1)'nci fıkrası hükmü gereğince hizmet sağlayıcının, mal ve hizmetlerini tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içeriklerle tanınırlığını artırmak amacıyla alıcıların elektronik iletişim adreslerine gönderdiği ticari elektronik iletiler için kendisi tarafından önceden onay alınır. Onay, reddetme hakkı kullanılıncaya kadar geçerlidir. Bu madde kapsamında alınacak onayın ise yine **Yönetmeliğin 7'inci maddesinin (1)'inci fıkrası** hükmü gereğinceyazılı olarak veya her türlü elektronik iletişim aracıyla alınabilmesi öngörülmüştür. Onayda ise alıcının ticari elektronik ileti gönderilmesini kabul ettiğine dair olumlu irade beyanı, adı ve soyadı ile elektronik iletişim adresi yer alır. Yine bu doğrultuda **Yönetmeliğin 12'inci maddesinin (2)'nci fıkrası** gereğince ***kişisel verilerin; üçüncü kişilerle paylaşılabilmesi, işlenebilmesi ve başka amaçlarla kullanılabilmesi için ilgili kişiden önceden onay alınması gerekir.***

Kişilerin iletişim bilgilerinin pazarlama amaçlı iletiler göndermeden önce veya en geç elektronik ileti gönderme onayının alındığı sırada işlenmesinin Kanunun 5'inci maddesinde yer alan işleme şartlarından açık rıza kapsamında olduğu değerlendirilmekte olup, ilgili kişilerin açık rızaları veya Kanunun 5'inci maddesinin 2'nci fıkrasında yer alan işleme şartlarından herhangi biri olmaksızın e-postalarına veya telefonlarına iletiler gönderilmesi Kişisel Verileri Koruma Kurulunun 16.10.2018 tarih ve 2018/119 sayılı İlke Kararında da düzenlenerek belirtilen şekilde faaliyette bulunan veri sorumluları hakkında Kanunun 18'inci maddesi kapsamında işlem tesis edileceği hususu belirtilmiştir.

Veri Sorumlusunun iddiası, ticari elektronik iletilerin Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik hükümleri kapsamında değerlendirilmesi gerektiği ve söz konusu mevzuat kapsamında şikayet mekanizmasının Ticaret Bakanlığının sorumluluğunda olduğu, şikayet başvurusunda bulunabilmek için gerekli hususların Kurumumuza intikal ettirilen başvuruda yer almadığı ve bu konudaki sorumluluğun da Kurumumuzda olmadığı yönündedir.

Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin amacı, 1'inci maddede, "elektronik iletişim araçlarıyla yapılan ticari iletişime dair bilgi verme yükümlülüklerine ve ticari elektronik iletilerde uyulması gereken hususlara ilişkin usul ve esasları düzenlemek" olarak belirlenmiş olup, yönetmeliğin tanımlar başlıklı 4'üncü maddesinde ticari elektronik ileti, "Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletiler" olarak tanımlanmıştır.

Ticari elektronik iletiye ilişkin ayrı bir mevzuat bulunmakla birlikte, telefon numarası, e-posta adresi gibi bilgilerin bir veri kayıt sisteminde depolanması suretiyle kişilere ticari nitelikli iletiler gönderilmesi, bir kişisel veri işleme faaliyetine işaret etmektedir. Dolayısıyla ticari nitelikli bir elektronik iletinin ticari elektronik ileti gönderilmesine ilişkin mevzuata uygun olarak gönderilmesi gerekmekle birlikte, bu mesajların iletilmesi için kullanılan iletişim kanallarının kişisel veri niteliğinde olması nedeniyle ticari elektronik iletilerin gönderilmesi süreçlerinin aynı zamanda kişisel verilerin korunması mevzuatına da uygun olması gerekmektedir. Bu bağlamda, Kurulun konuya ilişkin almış olduğu ilke kararı, ticari elektronik iletilerin gönderilmesine ilişkin değil, kişisel verilerin işlenmesi süreçlerine ilişkin bir karardır.

Somut olayda, veri sorumlusu hakkında Kurumumuza ihbarda bulunan şahıs tarafından Kurumumuzun yanı sıra Ticaret Bakanlığına da başvuruda bulunulmuş olup, Ticaret Bakanlığı söz konusu başvuruyu "kişisel verilerin korunması mevzuatı kapsamında değerlendirilmek üzere" Kurumumuza intikal ettirmiş olup, bu durumun, söz konusu başvurunun kişisel verilerin korunması düzenlemeleri bağlamında ele alınması gerekliliğini ortaya koyduğu değerlendirilmektedir.

Diğer yandan, Kurumumuz tarafından veri sorumlusu şirkete yönelik başlatılan inceleme, Kurumumuza intikal eden ihbarın değerlendirilmesini müteakip, Kanunun 15'inci maddesinin 1 numaralı fıkrasında verilen yetki çerçevesinde Kurulun resen başlatmış olduğu bir incelemedir. Tarafımızca yapılan incelemede, www.amazon.com.tr sayfasında bir üyelik profili oluşturulmak suretiyle, iletişim bilgisinin pazarlama amaçlı iletiler gönderilmesi amacıyla işlenmesi hususunda ilgili kişilerin açık rızasının alınıp alınmadığı kontrol edilmiş olup, üyelik yapılabilmesi için gerekli bilgilerin girilmesi sırasında herhangi bir açık rıza alınmadığı, üyelik sürecinin tamamlanmasının ardından girilen "Hesabım" sekmesinde "İletişim Tercihleri" bölümünde Genel Ayarlar" başlığında, "e-postalar şu anda ……. E-posta adresine gönderiliyor" açıklamasının yer aldığı, "Promosyon E-postaları" başlığına tıklandığında ise "haberdar olmak istediğiniz tüm iletişim kategorilerini seçin" ifadesine yer verilmekle birlikte, 10 adet başlığın önceden tıklanmış olarak ekranda belirdiği, bu bölümün en altında ise "lütfen bana artık pazarlama e-postaları göndermeyin" kutucuğunun yer aldığı görülmektedir.

Kanunun Tanımlar başlıklı 3'üncü maddesinin 1 numaralı fıkrasının (a) bendinde açık rıza, belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür irade ile açıklanan rıza" olarak tanımlanmıştır. Kanunda yer verilen tanım çerçevesinde veri sorumluları tarafından ilgili kişilerden alınacak açık rıza beyanlarında opt-out yani bireyin önceden onayını almaksızın kişisel verilerinin işlenmesine otomatik onay verdiklerinin kabul edildiği ve kişilere bu onayı kaldırmaları yönünde imkân veren bir sistemin değil, opt-in yani bireyin bilinçli eylemi ile kişisel verilerinin işlenmesine onay vereceği bir sistemin kullanılması gerekmektedir.

Veri sorumlusunca Gizlilik Bildiriminde yapılan açıklamada, "Amazon.com.tr'yi ziyaret ederek işbu Gizlilik Bildiriminde belirtilen uygulamaları kabul etmekte ve onaylamaktasınız" ifadesinin yer aldığı, böylece ilgili kişilerin kişisel verilerinin işlendiğinden sadece haberdar olmadığı ayı zamanda "Gizlilik Bildirimi"ni onaylayarak bu hususu kabul etmiş olduğu iddiası yer almaktadır. Ancak, üyelik oluşturulurken herhangi bir aşamada açık rıza alınması yoluna gidilmediği tarafımızca yapılan incelemede tespit edilmiştir. Gizlilik bildirimindeki ifade, aydınlatma yapılırken aynı zamanda kişilerden açık rıza alınması yoluna gidildiği izlenimini yaratmaktadır. Bilindiği üzere açık rıza dışında işleme nedenlerinin varlığı halinde açık rıza alınması yoluna gidilmesi, dürüstlük kuralına aykırılık şeklinde yorumlandığı gibi, diğer yandan açık rıza gerektiren veri işleme süreçleri bakımından da aydınlatmanın yapılması ile açık rızanın alınmasının birlikte yapılması yürürlükteki mevzuata uygun kabul edilmemektedir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5'inci maddesinin 1'inci fıkrasının (f) bendinde, kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği düzenlenmiştir. Bu kapsamda veri sorumlusunca web sitesinde yayımlanan "Gizlilik Bildirimi", birçok bilgi içermesi, veri işlemeye ilişkin genel bir bilgilendirme olması nedeniyle kişisel verilerin işlenmesine ilişkin ilgili kişilere aydınlatma yapıldığı ve açık rıza alındığı anlamına gelmemektedir.

Bu kapsamda, veri sorumlusunun ilgili kişilerin iletişim bilgilerini işlemek suretiyle ticari elektronik ileti göndermek hususunda ilgili kişilerin açık rızasını almadığı, açık rıza dışında da bir işleme nedenine dayanmadığı dikkate alındığında Kanunun 12'nci maddesinde yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü yerine getirmediği kanaatine varılmaktadır.

2. Yine Kanunun 4'üncü maddesinin 2 numaralı fıkrası hükmü gereğince kişisel verilerin işlenmesinde "hukuka ve dürüstlük kurallarına uygun olma", "belirli, açık ve meşru amaçlar için işlenme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine uyulması zorunludur.

Veri sorumlusu, “Gizlilik Bildirimi” metninde “Belirli bilgileri vermemeyi tercih edebilirsiniz, ancak bu durumda Amazon Hizmetlerinin çoğundan yararlanamazsınız.” ya da “Çerezlerimizi engellerseniz veya reddederseniz alışveriş sepetinize ürün ekleyemez, satın alma aşamasına geçemez veya oturum açmanızı gerektiren herhangi bir Amazon hizmetini kullanamazsınız.” diyerek kişisel verilerin işlenmesini hizmet şartına bağlamaktadır. Kurumumuzun internet sayfasında da yayımlanan kararıda sözleşmenin taraflarına ait kişisel veri işlenmesi durumunda ayrıca açık rıza alınması ve de açık rızayı üyeliğin ve hizmetin dolayısıyla sözleşmenin bir koşulu olarak dayatılmasının; diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği ve ayrıca hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı dikkate alındığında, bu durumun Kanunun 4’üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ve işlenme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil ettiği değerlendirilmektedir.

Amazon.com.tr’nin topladığını beyan ettiği veriler ise şunlardır: “ad, adres, telefon numarası, ödeme bilgileri; yaş; konum bilgisi; satın alımların gönderildiği kişiler; 1-Tık ayarlarında listelenen kişiler (adresler ve telefon numaraları dâhil); arkadaşların ve diğer kişilerin e-posta adresleri; veri sorumlusuna gönderilen değerlendirmelerin ve e-postaların içeriği; profildeki kişisel bilgiler ve fotoğraflar; Amazon hizmetleri ile bağlantılı olarak saklanan resimler ve video, kimlik ve duruma ilişkin bilgiler ve belgeler; kurumsal ve finansal bilgiler; kredi geçmişi bilgileri; KDV numaraları.” İlgili kişinin arkadaşlarının bilgileri, kendisi bakımından kişisel veri olmakla birlikte ayrıca bu bireylere ait birer kişisel veri niteliğini de taşımaktadır. Böylece üye ile Amazon.com.tr arasında bir sözleşmenin ifası veya üyenin açık rızası kapsamında, üyenin temas kişilerine ait e-posta adresleri de bu kişilerin açık rızalarına dayanmaksızın işlenmektedir. Öte yandan “kredi geçmişi bilgileri, duruma ilişkin bilgiler, kurumsal ve finansal bilgiler” Kanunda yer alan genel ilkeler bağlamında değerlendirildiğinde, bu verilerin orantılı ve sınırlı bilgiler olmadığı, işlenen verilerin ilgili kişiler tarafından en azından öngörülebiliyor olması gerekmekte olup veri sorumlusunca “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine aykırı hareket edildiği değerlendirilmektedir.

3. Kanunun 8 inci maddesinde “(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; 5’inci maddenin ikinci fıkrasında, yeterli önlemler alınmak kaydıyla, 6’ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.” hükmü düzenlenmiştir.

Veri sorumlusunun "Gizlilik Bildirimi" incelendiğinde 'Amazon Kişisel Bilgilerinizi Paylaşıyor mu?' başlığı altında açıklanan şekillerde paylaşım yapıldığı belirtilerek son maddede "Yukarıda belirtilenler haricinde, hakkınızdaki kişisel bilgiler üçüncü taraflarla paylaşıldığında, bir bildirim alacaksınız ve bu bilgileri paylaşmamayı seçme şansınız olacaktır." ifadesine yer verilmiştir. Metinde yer aldığı şekilde ilgili kişinin kişisel verilerini paylaşmamayı tercih etme şansının mümkün olması, ancak ilgili kişinin açık rızasına istinaden verilerinin işlenmesi halinde geçerli olabilecektir. Çünkü Kanunun 8'inci maddesinin 2 ve 3 numaralı fıkraları kapsamında gerçekleştirilen veri aktarımı işlemlerinde ilgilinin açık rızası aranmayacağı gibi (Kanunun 5'inci maddesinin 2 numaralı fıkrası, 6'ncı maddesinin 3 numaralı fıkrası ve diğer kanunlarda öngörülen hallerde yapılan işlemeler), bu durumlarda ilgili kişinin verilerini paylaşmamayı tercih etme şansı da bulunmayacaktır. Öte yandan, açık rızanın en geç aktarma faaliyeti gerçekleştiği sırada alınması lazımdır, bundan sonra alınacak açık rıza mevzuata uygun kabul edilemez. Dolayısıyla, aktarım faaliyetinin gerçekleşmesinden sonra rızanın geri alınabileceğinin söylenmesi kanun lafzının tersine yorumlanması olarak değerlendirilmektedir. Açık rıza alınmadan aktarılan verilerin rıza geri alındıktan sonra akıbetinin ne olacağının bilinmemesi de ayrı bir tartışma konusudur. Dolayısıyla kişisel verilerin aktarılmasına ilişkin gizlilik bildiriminde yer alan muğlak ifadeler, aktarıma ilişkin Kanun hükümlerine aykırı hareket edildiği kanaati uyandırmaktadır.

4. Kanunun 9'uncu maddesi, *"(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. (2) Kişisel veriler, 5'inci maddenin ikinci fıkrası ile 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; yeterli korumanın bulunması, yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir. (3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir."* hükmünü içermektedir.

Yapılan incelemede veri sorumlusunun yurtdışına veri aktarımını sağlamak amacıyla Kurulun onayını almak üzere taahhütname mektuplarını Kurula sunduğu görülmüştür. Ancak Kurulun henüz bu yönde bir karar vermediği ve yeterli korumaya sahip ülkelerin de henüz belirlenmediği değerlendirildiğinde kişisel verilerin yurtdışına aktarılması için tek yöntem ilgilinin açık rızasının alınması olarak değerlendirilmektedir.

Veri sorumlusundan alınan yazıda hali hazırda mevzuata uygun olarak yurtdışına veri aktarım faaliyeti yapıldığı belirtilmiş olsa da "Amazon Hesabınızı Oluşturun" sekmesine tıklayarak "Gizlilik Bildirimi"nin de kabul edildiği ("Hesap oluşturarak işbu Gizlilik Bildirimi'nde belirtilen uygulamaları kabul etmektesiniz."); aynı şekilde kayıtlı bir müşteri, site üzerinden sipariş verdiğinde kendisine "Gizlilik Bildirimi"nin kabul edildiğine dair tekrar hatırlatma yapıldığı ("*Sipariş verdiğinizde*

Amazon.com.tr'nin Gizlilik Bildirimini, Kullanım ve Satış Koşullarını ve Çerez Bildirimini kabul etmiş olursunuz") belirtilerek ilgili kişilerin rızasının alındığı veri sorumlusunca iddia edilmekle birlikte, zımni irade beyanı ile onay alınmasının mevzuata uygun kabul edilemeyeceği değerlendirilmektedir. Kanun çerçevesinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır. Açık rıza, ilgili kişinin, işlenmesine izin verdiği verinin sınırlarını, kapsamını ve süresini de belirlemesini sağlayacaktır. Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar "battaniye rızalar" olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır. Bu kapsamda "Gizlilik Bildirimi"ne onay verildiği yönünde yapılacak bilgilendirme ile "veri işleme" kapsamına giren bütün fiillerin (çerezlerle izleme, aktarma, paylaşma, depolama vb.) tek bir rıza beyanı ile onaylanmasının hukuka uygun olmadığı mütalaa edilmektedir. Mevcut hukuki düzenlemeler çerçevesinde veri sorumlusunun kişisel verilerin yurtdışına aktarılması konusunda Kanunun 9'uncu maddesinin 1 numaralı fıkrasında yer aldığı üzere ilgili kişilerin açık rızasını alması gerektiği, ancak veri sorumlusunun yurt dışına aktarıma ilişkin bir açık rıza alma yoluna gitmediği, yalnızca amazon hizmetlerinin kullanılması suretiyle gizlilik bildiriminde yer alan hususların kabul edilmiş olduğu varsayımının Kanuna uygun bir açık rıza olarak nitelendirilemeyeceği, bu durumun Kanunun 12'nci maddesinde yer alan veri güvenliğine ilişkin yükümlülüklere aykırılık oluşturduğu kanaatine varılmıştır.

5. Kanunun 10'uncu maddesinde yer alan hüküm gereğince, *"kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11'inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür."*

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5'inci maddesinin 1'inci bendinin f fıkrasına göre *"Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."*

Veri sorumlusunun internet sitesindeki "Kullanım ve Satış Şartları" metni incelendiğinde Amazon Europe Core SARL, Amazon Turkey Perakende Hizmetleri Limited Şirketi ve/veya iştirakleri ("Amazon"), Amazon.com.tr (internet sayfası) ziyaret edildiğinde veya buradan alışveriş yapıldığında; Amazon ürünleri, hizmetleri, mobil Amazon uygulamaları veya yukarıdakilerle bağlantılı olarak Amazon tarafından sunulan hizmetler kullanıldığında (toplu olarak "Amazon Hizmetleri") ilgili kişilere internet sayfası özelliklerinin, diğer ürünlerin ve hizmetlerin sunulduğu beyan edilmiştir.

Anlaşıldığı üzere yapılan işleme faaliyeti site ziyaret edildiğinde başlamaktadır. Öyle ki çerezler hakkında hazırlanan metinde siteyi ziyaret eden kişilerin tarayıcılarını veya cihazını tanımak, ilgileri hakkında daha fazla bilgi sahibi olmak; gerekli özellik, hizmetleri sağlamak ve aşağıda sayılanların da aralarında bulunduğu ek amaçlar için çerezlerin, piksellerin ve diğer teknolojilerin (hep birlikte "çerezler" olarak anılacaktır) kullanıldığı beyan edilmiştir. Bu durumda sitede gerekli metinlere yer verildiği savından yola çıkılarak Kanunda hüküm altına alınan aydınlatma yükümlülüğünün yerine getirildiği sonucuna varmak mümkün değildir. Siteyi ilk defa ziyaret eden bir kişinin daha henüz veri sorumlusu ile bir sözleşme ilişkisi içine girip girmeyeceğinin ya da kişisel verilerinin işlenmesine açık rızası olup olmayacağının belirli olmaması düşünüldüğünde yalnızca siteye girmiş olması ile verilerinin işlenmesi yönünde açık iradesini beyan ettiği düşünülemeyecektir. Farklı veri işleme araçları kullanılarak site ziyareti ile birlikte veri işlenmeye başlanması için aydınlatmanın öncelikle web sitesine giriş aşamasında yapılması gerekmektedir. Ancak site girişinde farklı araçlarla (ör. Çerezler) kişisel verilerin işlendiğine dair bir bilgilendirme sunulmamakla birlikte (ör. pop-up mesajlar) yapılan işleme için izin verilmesine dair bir istem de mevcut değildir (ör. Sitemizde gezinmeye devam etmek için çerez bildirimimize onay vermelisiniz). Bu durum hem işleme faaliyetindeki açık rıza şartına hem aydınlatma yükümlülüğüne aykırılık teşkil etmekte olup, web sitesine girişle birlikte kişisel verilerin işlenmeye başlamasına karşın aydınlatmanın yapılmaması, veri sorumlusunun çerezler vasıtasıyla işlenen söz konusu kişisel verilere ilişkin aydınlatma yükümlülüğünü Kanunun 10'uncu maddesinde ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde düzenlendiği şekilde yerine getirmediği kanaatini oluşturmuştur.

www.amazon.com.tr'ye ilişkin yürütülen resen inceleme neticesinde yukarıda yer verilen değerlendirmeler sonucunda;

- Veri sorumlusunun ilgili kişilerin iletişim bilgilerini işlemek suretiyle ticari elektronik ileti göndermek hususunda ilgili kişilerin açık rızasını usulüne uygun olarak almadığı, açık rıza dışında da bir işleme nedenine dayanmadığı, diğer yandan üyenin temas kişilerine ait e-posta adreslerinin de bu kişilerin açık rızalarına dayanmaksızın işlendiği, ayrıca veri sorumlusu tarafından Kanunun 4'üncü maddesinde yer alan genel ilkelere aykırı hareket edildiği,
- Veri sorumlusunun "Gizlilik Bildirimi"nde 'Amazon Kişisel Bilgilerinizi Paylaşıyor mu?' başlığı altında "Yukarıda belirtilenler haricinde, hakkınızdaki kişisel bilgiler üçüncü taraflarla paylaşıldığında, bir bildirim alacaksınız ve bu bilgileri paylaşmamayı seçme şansınız olacaktır." ifadesine yer verildiği, metinde yer aldığı şekilde ilgili kişinin kişisel verilerini paylaşmamayı tercih etme şansının mümkün olmasının, ancak ilgili kişinin açık rızasına istinaden verilerinin işlenmesi halinde geçerli olabileceği, ancak usulüne uygun bir açık rıza alınmadığı dikkate alındığında, kişisel verilerin aktarılmasına ilişkin Kanun hükümlerine aykırı hareket edildiği,

- Kişisel verilerin yurt dışına aktarılması konusunda Kanunun 9'uncu maddesinde yer alan yeterli korumanın bulunduğu ülkelerin Kurulca henüz belirlenmediği, veri sorumlusunun yazılı taahhüdünün Kurum tarafından onaylanmadığı da dikkate alındığında, veri sorumlusunun kişisel verilerin yurtdışına aktarılması konusunda Kanunun 9'uncu maddesinin (1) numaralı fıkrasında yer aldığı üzere ilgili kişilerin açık rızasını alması gerektiği, ancak veri sorumlusunun yurt dışına aktarıma ilişkin usulüne uygun bir açık rıza alma yoluna gitmediği, yalnızca amazon hizmetlerinin kullanılması suretiyle gizlilik bildiriminde yer alan hususların kabul edilmiş olduğu varsayımının Kanuna uygun bir açık rıza olarak nitelendirilemeyeceği

dikkate alındığında veri sorumlusu tarafından Kanunun 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülüklerin yerine getirilmemesinden dolayı Kanunun 18'inci maddesinin (1) numaralı maddesinin (b) bendi kapsamında **1.100.000 TL idari para cezası uygulanmasına,**

- Veri sorumlusunca web sitesinde yayımlanan "Gizlilik Bildirimi"nin, birçok bilgi içermesi, veri işlemeye ilişkin genel bir bilgilendirme olması nedeniyle kişisel verilerin işlenmesine ilişkin ilgili kişilere aydınlatma yapıldığı anlamına gelmediği göz önünde bulundurulduğunda ihbar edilen web sitesine girişle birlikte çerezler vasıtasıyla kişisel verilerin işlenmeye başlamasına karşın, çerezler, üyelik girişi gibi veri işlemenin başladığı hiçbir aşamada aydınlatma yükümlülüğünün, Kanunun 10'uncu maddesinde ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde düzenlenen usul ve esaslara uygun olarak yerine getirilmediği kanaati oluştuğundan Kanunun 10'uncu maddesinde düzenlenen Aydınlatma Yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında Kanunun 18'inci maddesinin (1) numaralı fıkrasının (a) bendi uyarınca **100.000 TL idari para cezası uygulanmasına,**

- Veri sorumlusunun yukarıda tespit edilen ihlaller göz önünde bulundurularak kişisel veri işleme süreçlerini ve bununla uyumlu şekilde "Gizlilik Bildirimi", "Kullanım ve Satış Şartları" ve "Çerez Bildirimi" metinlerini güncelleyerek web sitesini ve uygulamalarını Kanuna uygun hale getirerek sonucundan Kurula bilgi vermesi yönünde **talimatlandırılmasına,**

karar verilmiştir.

07.05.2020
Karar Tarihi : 22/04/2020
Karar No : 2020/315
Konu Özeti : Dernek, vakıf ve sendikaların Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulması

I. Kararın Konusu ve Hukuki Dayanağı

6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) 16 ncı maddesinin ikinci fıkrasında yer alan "Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir." hükmüne göre kural olarak kişisel veri işleyen gerçek ve tüzel kişilerin Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğü bulunmakla birlikte Kişisel Verileri Koruma Kurulu (Kurul) tarafından bu yükümlülüğe istisna getirilebilmektedir.

6698 sayılı Kanunun 16 ncı maddesinin verdiği yetkiye dayanarak Sicile kayıt yükümlülüğüne istisna getirilen veri sorumluları ile ilgili 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararı ile;

- Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler,
- 18/01/1972 tarihli ve 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler,
- 04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler,
- 22/04/1983 tarihli ve 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler,
- 19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar,
- 1/6/1989 tarihli ve 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler

Sicile kayıt yükümlülüğünden istisna tutulmuştur.

Anılan Kurul kararının 3 üncü maddesinde yer alan “04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler” ifadesinin kapsamı, yorumlanması ve uygulamada yaşanan bazı tereddütler nedeniyle Kuruma iletilen görüş taleplerinin değerlendirilmesi sonucunda;

- Sicile kayıt yükümlülüğüne istisna getirilen 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararının 3 üncü maddesinde yer alan “04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler.” ifadesinin “yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalar” şeklinde değiştirilmesinin,
- Anılan Kararın Kurum internet sayfası ve Resmi Gazetede yayımlanmasının

gerektiği kanaatine varılmıştır.

II. Sonuç

6698 sayılı Kanunun 16 ncı maddesi gereği Sicile kayıt yükümlülüğüne istisna getirilen 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararının 3 üncü maddesinde yer alan dernek, vakıf ve sendikalarla ilgili istisna hususundaki başvurular üzerine Kurul tarafından yapılan değerlendirme sonucunda;

- Sicile kayıt yükümlülüğüne istisna getirilen 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararının 3 üncü maddesinde yer alan “04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler.” ifadesinin “yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalar” olarak değiştirilmesinin,
- Anılan Kararın Kurum internet sayfası ve Resmi Gazetede yayımlanmasının

kabulüne oybirliği ile karar verilmiştir.

13.05.2020
Karar Tarihi : 12/03/2020
Karar No : 2020/213
Konu Özeti : Bir internet servis sağlayıcısının veri ihlali hakkında Karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Şirketin müşterilerinin paket değişikliği, fatura ödeme, arıza bildirimi gibi abonelik işlemlerini yapmalarına olanak sağlayan ve kendilerine tanımlanan kullanıcı adı ve şifre ile giriş yapabildikleri bir Online İşlem Merkezi bulunduğu,
- Şirketin fatura ödeme sisteminde online (çevrimiçi) işlemlerde fatura ödemesi yapılamadığı ve sorunun Şirkete müşteriler tarafından bildirildiği,
- Müşterinin ödeme yaptığı sırada ekranda "fatura seçilmesi gerektiği" uyarısı belirdiği,
- Sorun giderilmek üzere çalışma yapılırken bir güvenlik açığının ortaya çıktığı,
- Güvenlik açığı sebebiyle müşterilerin **kredi kartı bilgilerinin üçüncü taraflarca görüntülendiği,**
- İhlalin kök nedeninin uygulamaya bilgi kaydı (log) üreten özelliklerin eklenerek "debug" ile düzeltilmesi girişiminin olduğu,
- **69 kişiye ait kart bilgisinin 649 adet Şirket müşterisi tarafından görüntülendiğinin** tespit edildiği,

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun **12.03.2020** tarih ve **2020/213** sayılı Kararı ile;

- Yazılım geliştiricilere sözlü olarak aktarılmış olan değişiklik talebinin test ortamında değil de gerçek ortamda yapılmasının, uygulamada yapılan değişikliklerin canlıya (gerçek/çalışır ortam) alma süreçleri ile ilgili prosedürlerin uygulanmadığının göstergesi olduğu bu durumun ise teknik ve idari tedbir eksikliği olduğu,
- Test süreçlerinin yetersizliği veri sorumlusunun kendisi tarafından belirtilmiş olup bu durumun uygulama güvenliği açısından veri sorumlusunun gerekli teknik ve idari tedbirleri almadığının göstergesi olduğu,
- Sistem ara yüzlerinde kişisel verilerin ya hiç gösterilmediğinin ya da maskelendiğinin şirket tarafından belirtilmiş olmasına rağmen müşterilere ait kimlik ve finans verilerinin yapılan hata sonucunda görüntülenebilmesinin teknik bir eksiklik olduğu,
- Veri sorumlusunun bir veri güvenliği politikasının bulunduğu ancak bu politikanın yürürlük tarihinin veri ihlalinin gerçekleştiği tarihten **sonra** olduğu dikkate alınarak,

6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **300.000 TL idari para cezasının** uygulanmasına karar verilmiştir.

28.05.2020
Karar Tarihi : 28.05.2020
Karar No : 2020/443
Konu Özeti : EasyJet Plc Veri İhlali Bildirimi

Veri sorumlusu sıfatını haiz olan EasyJet Plc (EasyJet) tarafından Kuruma gönderilen 26.05.2020 tarihli yazıda özetle;

- EasyJet'in üst düzey saldırganlar tarafından gerçekleştirilen ve kişisel verilere erişilmesine yol açan bir bilgi güvenliği sorununa maruz kaldığı,
- İhlalin 17.10.2019 ile 04.03.2020 tarihleri arasında gerçekleştiği,EasyJet'in sistemlerine yetkisiz erişimden ilk olarak 22.01.2020 tarihinde haberdar olduğu,
- 10.03.2020 tarihinde yolcu rezervasyon bilgilerini elde eden özel üretim bir kötü amaçlı yazılımın tespit edildiği,
- 20.05.2020 tarihinde saldırıdan etkilenen kişiler arasında 6.846 tanesinin Türkiye'de mukim olduğunun (müşteriler tarafından rezervasyon yapılırken bildirilen fatura adreslerine istinaden) tespit edildiği,
- İhlalden Türkiye'de mukim 3 kişinin irtibat bilgileri (adı, soyad ve e-posta adresi), uçuş bilgileri (uçak kalkış tarihi, kalkış noktası, varış noktası ve bilet referansı), işlem bilgileri (işlem tutarı ve cinsi) ve ödeme bilgilerinin (bilet alan kişinin tokenlaştırılmamış düz metin halinde kart numarası, son kullanma tarihi ve cvv bilgisi) etkilendiği,
- 6843 kişinin ise irtibat bilgileri (adı, soyad ve e-posta adresi), uçuş bilgileri (uçak kalkış tarihi, kalkış noktası, varış noktası ve bilet referansı), işlem bilgilerinin (işlem tutarı ve cinsi) etkilendiği,

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

16.06.2020
Karar Tarihi : 16.06.2020
Karar No : 2020/468
Konu Özeti : Halk Sigorta A.Ş. Veri İhlali Bildirimi

Veri sorumlusu sıfatını haiz olan Halk Sigorta A.Ş. (Halk Sigorta) tarafından Kuruma gönderilen yazıda özetle;

- İhlalin, istifa ederek iş akdi sona erdiren bir çalışanın, iş ilişkisi sona erdikten sonra daha önce sorgu yapmak için yetkili olduğu yazılımdaki trafik ve kasko sigortası dosyalarına yetkisiz bir şekilde erişmesi sonucu meydana geldiği,
- İhlalin 30.01.2020 ve 08.04.2020 tarihleri arasında gerçekleştiği,
- İhlalin 10.04.2020 tarihinde Halk Sigorta tarafından yapılan periyodik kontrol sırasında tespit edildiği,
- İhlalden etkilenen kişi gruplarının, sigortalılar, kaza mağdurları, eksperler, acente çalışanları, sürücüler, servis çalışanları, tedarikçi çalışanları olduğu,
- İhlalden etkilenen kişisel verilerin, sigorta hasar dosyasında bulunan ad, soyad, adres, telefon no, vergi kimlik numarası, T.C. kimlik numarası, plaka, şase no, ruhsat, eski hasar bilgileri ve ehliyet bilgisi olduğu, ihlalden etkilenen özel nitelikli kişisel verilerin ise engellilik bilgisi, sağlık bilgisi ve alkol raporu olduğu,
- İş akdi sona erdirilen kişiye ait kullanıcı bilgisi ile işten ayrılma tarihinden sonra 6933 adet farklı eksper dosyasına erişim gerçekleştirildiği,
- İhlali gerçekleştiren kişi hakkında savcılığa suç duyurusunda bulunulduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 03/03/2020
Karar No : 2020/191, 2020/192, 2020/193, 2020/194
Veri Sorumlusu: Muhtelif faktoring şirketleri
Konu Özeti: Risk Merkezindeki verilerin muhtelif faktoring şirketleri tarafından ihlal edildiğine ilişkin ihbar hakkında

Kuruma intikal eden ihbarda özetle; sorgu adetlerinde ilgi çekici değişim gözlemlenen Risk Merkezi üyeleri hakkında Risk Merkezi Yönetimi tarafından yapılan inceleme neticesinde, üyelerin bazı çalışanları tarafından Risk Merkezinden yapılan sorgulamaların kanunen yetkili olmayan kişilerle paylaşıldığının ve/veya amaç dışı kullanıldığının tespit edildiği belirtilmiştir. Konu hakkında başlatılan inceleme çerçevesinde;

5411 sayılı Bankacılık Kanununun "Risk Merkezi" başlıklı Ek 1 inci maddesi (fıkra 10 vurgulanmıştır) çerçevesinde, Risk Merkezi tanımlanarak anılan merkezde yapılacak işlemler, sır saklama yükümlülüğü ve gizlilik gibi hususlara ilişkin ayrıntılar ilgili madde kapsamında düzenlenmiştir.

5411 sayılı Kanun'un 159 uncu maddesi ise sırların açıklanmasına ilişkin düzenlemeleri içermektedir. İlgili hüküm kapsamında anılan kanuna aykırı olarak sırları ifşa edenler hakkında ağır yaptırımlar öngörülmüş olup; sırların kendileri ya da başkaları için yarar sağlamak amacıyla açıklanmış olması durumunda da cezaların altıda bir oranında artırılacağı vurgulanmıştır.

Benzer şekilde, 5411 sayılı Kanunun 73 üncü maddesi sır yükümlülüğünü düzenlemektedir. Anılan maddenin dördüncü fıkrasında yer alan hüküm ile sır saklama yükümlülüğünün istisna olduğu durumlar, "sadece belirlenen amaçlar ile sınırlı kılınması koşuluyla" söz konusu olmaktadır. Yani, amacı dışında işlenecek her türlü veri, istisna kapsamı dışında değerlendirilecektir. Nitekim söz konusu ihbara konu olan eylemlerde de ihlale sebebiyet verdiği iddia olunan kişiler, belirtilen amaçlar ile sınırlı kalmaksızın birçok gerçek ve tüzel kişiye ilişkin verilere erişmiş; üstelik bazıları bu verileri de yetkisiz üçüncü kişilere aktarmışlardır. Anılan sebeplerle, söz konusu eylemlerin 5411 sayılı Kanunu da ihlal ettiği değerlendirilmektedir.

Benzer şekilde, Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği (Risk Merkezi Yönetmeliği), TBB Risk Merkezinin kuruluşuna, faaliyetine ve çalışmasına, Türkiye Bankalar Birliği Risk Merkezi yönetiminin oluşumuna, toplanmasına ve karar almasına, Türkiye Bankalar Birliği Risk Merkezine verilen bilgilerin kapsam, biçim ve içeriğine ve bunların paylaşılmasına, paylaşılacak bilgilerin kapsam ve içeriğine, ücretlendirilmesine ve üyelerce ödenecek aidatların belirlenmesine ilişkin usul

ve esasları düzenlemektedir. Risk Merkezi Yönetmeliği'nin "Tanımlar" başlıklı 3 üncü maddesinin birinci fıkrasının (j) bendi uyarınca üye; "kredi kuruluşları ile Türkiye Bankalar Birliği Risk Merkezine Kurul tarafından üye olması uygun görülen her bir finansal kuruluş" olarak tanımlanmıştır. Bu kapsamda, ihbara konu olan faktoring şirketlerinin her biri üye niteliğini haizdir. Yine, Risk Merkezi Yönetmeliği'nin "Risk Merkezi üyelerinin sorumlulukları" başlıklı 17 nci maddesinin birinci fıkrasının (b) ve (c) bentleri kapsamında üyeler, Risk Merkezi ile gizlilik sözleşmesi yapmak ve Risk Merkezinden temin ettiği her türlü bilgi ve belgenin gizliliğinin sağlanmasına yönelik her türlü önlemi almak ve Risk Merkezinden temin ettiği bilgileri yalnızca kendi iç işlemlerinde kullanmak, diğer üyeler dahil herhangi bir gerçek ve tüzel kişi ile paylaşmamak ile sorumlu tutulmuştur. Ayrıca, "Gizlilik" başlıklı 19 uncu madde doğrultusunda, Risk Merkezi'nde bulunan sır nitelikli bilgilerin kanunen yetkili kılınan mercilerden başkalarına açıklanması durumunda 5411 sayılı Kanunun 159 uncu maddesinde öngörülen yaptırımların uygulanacağı belirtilmiştir.

Ayrıca, "Türkiye Bankalar Birliği Risk Merkezi Üyelerinin Müşterilerinin Risk Merkezi Nezdindeki Bilgilerinin Kendilerine ya da Onay Vermeleri Koşuluyla Belirledikleri Gerçek veya Tüzel Kişilere Verilmesine İlişkin Esas ve Usuller Hakkında Yönetmelik" kapsamında, TBB Risk Merkezi üyelerinin müşterilerinin TBB Risk Merkezi nezdindeki bilgilerinin, kendilerine ya da onay vermeleri koşuluyla belirledikleri gerçek veya tüzel kişilere verilmesini teminen başvuru ve onay verme sürecine ilişkin esas ve usuller düzenlemektedir. Diğer bir ifade ile, Risk Merkezindeki bilgilerin ne şekilde sorgulanabileceği ve temin edilebileceği hususları da ayrı bir yönetmelik kapsamında düzenlenmektedir.

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Genel ilkeler" başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; "a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." şeklinde sayılan ilkelere uyulmasının zorunlu olduğu düzenleme altına alınmıştır. Bu ilkelerden kişisel verilerin "belirli, açık ve meşru amaçlar için işlenme" ilkesi, kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve gerçekleştirilme amacının belirliliğini sağlayacak detayda ortaya konulmasını sağlar. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir. Bir diğer önemli ilke olan "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması" ilkesine göre, işlenen veriler belirlenen amaçların gerçekleştirilmesine elverişli olmalı, amacın gerçekleştirilmesiyle ilgili olmayan veya sonradan ortaya çıkması muhtemel

ihtiyaçların karşılanmasına yönelik veri işleme yoluna gidilmemelidir. Burada önemli olan, amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınılmasıdır. Ölçülülük ilkesi ise, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması yani veri işlemenin, amacı gerçekleştirecek ölçüde olması demektir. Anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulması hukuki bir gerekliliktir. Kanundaki düzenlemede yer alan "belirli, açık ve meşru amaçlar için işlenme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması" ilkeleri ile 5411 sayılı Kanunun 73 üncü maddesinin dördüncü fıkrasında yer verilen "sadece belirlenen amaçlar ile sınırlı kılınması koşuluyla" şartı benzerlik göstermektedir. Dolayısıyla, somut olay değerlendirilirken anılan kişisel verilerin işlenmesine ilişkin ilkeler özellikle önem teşkil edecektir.

Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendi uyarınca kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, (e) bendi uyarınca kişisel verilerin işlenmesi; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (ç) bendi uyarınca ilgili kişi; kişisel verisi işlenen gerçek kişiyi, (ı) bendi uyarınca veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişiyi ifade etmektedir. Buna göre, ihbara konu olan faktoring şirketleri veri sorumlusu niteliğini haiz olup ihlal iddiasına konu eylemler bakımından şirket çalışanı kişisel veri işleme faaliyetinde bulunmuştur. Bu veri işleme faaliyetinin de yetki sınırını aşmak suretiyle hukuka aykırı bir şekilde gerçekleştiği değerlendirilmektedir.

Kanunun 12 nci maddesinin beşinci fıkrasında ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükme bağlanmıştır. Ayrıca, Kurumumuz resmi internet sitesinde yayımlanan 24.01.2019 tarih ve 2019/10 sayılı Kurul kararıyla "en kısa sürede" ibaresinin "72 saat" olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına karar verilmiştir.

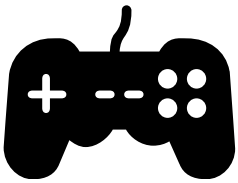
Bu itibarla;

Risk Merkezi üzerinden yapılan sorgu adetlerinde dikkat çekici değişiklik gözlenen Faktoring Şirketleri hakkında Kurulumuza yapılan ihbarın incelenmesi neticesinde, ihbara konu kişisel veri işleme faaliyetlerinde; Kanunun 4 üncü maddesinde sayılan genel ilkelere riayet edilmediği; söz konusu faaliyetlerin Kanunun 12 inci maddesinin birinci fıkrasında düzenlenen kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak yükümlülüklerine aykırılık teşkil ettiği tespit edilmiş ve **veri ihlalinin süresi, veri ihlalinden etkilenen kişi sayısı, ihlale ilişkin bildirimde bulunulmaması dikkate alınarak; Kişisel Verileri Koruma Kurulunun 03/03/2020 tarih ve 2020/191, 2020/192, 2020/193, 2020/194 kararları ile söz konusu 4 şirket hakkında**

Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli tedbirleri almadıkları gerekçesiyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi çerçevesinde toplam **950.000 TL,**

Kanunun 12 nci maddesinin (5) numaralı fıkrası uyarınca ihlale ilişkin Kuruma ve ilgili kişilere bildirim yapılmadığı gerekçesiyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi çerçevesinde toplam **450.000 TL,**
idari para cezası uygulanmasına karar verilmiştir.

Karar Tarihi : 16/04/2020
Karar No : 2020/286
Konu Özeti: **Bir oyun şirketinin veri ihlal bildirimi hakkında karar**



Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Oyun şirketinin oyuncu verilerine yasal olmayan yollarla hackerlar tarafından iki farklı yerden hukuka aykırı erişim gerçekleştirildiği,
- Hackerların, şirketin bulut sistemlerine, belirli olmayan kaynaklardan temin ettikleri kimlik bilgileri kullanarak erişmiş olduğu,
- Hackerların, oyuncu verilerine erişim sağladıklarının log kayıtlarından tespit edildiği, bu yetkisiz erişimin tespit edilmesinden sonra sistemde oyuncu giriş bilgilerinin değiştirildiği,
- Türkiye'de ihlalden etkilenen kişi sayısının 39,995 olduğu,
- İhlalden etkilenen kişi kategorilerinin kullanıcılar olduğu,Etkilenen kişisel verilerin, isim, soy isim, posta kodu, mahalle ve/veya ikamet ettiği şehir, doğum tarihi, e-posta adresi, fotoğraf, oyuncu kullanıcı adı ve şifresi, telefon numarası ve Facebook tanımlayıcısı da dâhil, özel nitelikli olmayan kimlik, irtibat ve konum bilgileri olduğu,
- Belirtilen verilerin tamamının olayın kapsamına her aşamada dahil olmadığı, örneğin, Türkiye'de yerleşik 39.995 kişi içerisinden 1.527 kişinin telefon numaralarına ve 51 kişinin doğum tarihine erişim sağlandığının düşünüldüğü,
- Türkiye'de yerleşik kişilere e-posta yoluyla bildirimde bulunulduğu, ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 16.04.2020 tarih ve 2020/286 sayılı Kararı ile;

- Türkiye'de ihlalden etkilenen kişi sayısının 39.995 olduğu,
- Etkilenen kişisel verilerin, isim, soy isim, posta kodu, mahalle ve/veya ikamet ettiği şehir, doğum tarihi, e-posta adresi, fotoğraf, kullanıcı adı ve şifresi, telefon numarası ve Facebook tanımlayıcısı da dâhil, özel nitelikli olmayan kimlik, irtibat ve konum bilgileri olduğu,
- Bir bulut sistemi bulunan veritabanına saldırganlar tarafından erişim sağlanmasının yapılan zafiyet testlerin yetersiz olmasının ve gerekli önlemlerin alınmadığının göstergesi olduğu,
- Veri sorumlusu tarafından ihlal öncesi alınması gereken teknik tedbirlerin (güvenlik ajanının ağ sistemine konuşlandırılması, kötü niyetli IP adreslerinin sistemden engellenmesi, oyuncu hesaplarının yetkisiz erişimlerden korunması için gerekli önlemlerin alınması, hackerlar tarafından kullanılan mekanizmaların ve IP'lerin gözlenmesi için 7x24 gerçek zamanlı gözetleme sistemini de içeren, geliştirilmiş gözetleme ve alarm sistemlerinin faaliyete geçirilmesi) ihlal sonrası devreye alınmasının gerekli teknik ve idari tedbirlerin alınmadığının göstergesi olduğu hususları dikkate alındığında,

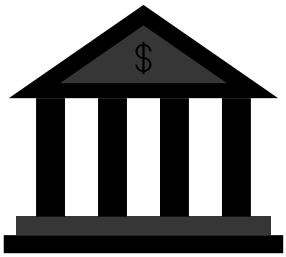
Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan Şirket hakkında;

Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **1.000.000 TL**,

Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne aykırı hareket eden Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **100.000 TL** olmak üzere

Toplam **1.100.000 TL** idari para cezası uygulanmasına karar verilmiştir.

Karar Tarihi : 05/05/2020
Karar No : 2020/344
Konu Özeti: Bir bankanın veri ihlali hakkında Karar



Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Bankanın Uyum ve İç Kontrol Grubu tarafından düzenli gerçekleştirilen iç kontrol faaliyetleri kapsamında, 2 ayrı şubesinde toplam 3 personel tarafından, Türkiye Bankalar Birliği Risk Merkezince Bankaya sağlanan bireysel nitelikteki kredi bilgilerini içeren KKB sorgu ekranlarından şüpheli sorgulamaların yapıldığının gözlemlendiği,
- Bu işlemlerin detaylı incelenmesi talebiyle konunun Teftiş Kurulu Başkanlığına ihbar edildiği,
- Teftiş Kurulu soruşturması sonucunda; Bireysel Müşteri ilişkileri Yöneticisi, Bireysel Müşteri İlişkileri Yönetici Yardımcısı, İşletme Müşteri İlişkileri Yönetici Yardımcısı unvanlarında çalışan ve olaya sebep olan 3 personelin görev ve iş tanımları gereği KKB sorgulama ekranına yetkileri bulunduğu, ancak söz konusu 3 personelin kendilerine tanımlanan KKB sorgulama yetkilerini Bankanın erişim ve bilgi güvenliği politikalarına aykırı şekilde amacı dışında kullandığı,
- Banka müşterisi olmayan toplam 7.706 kişinin bireysel nitelikteki kredi bilgilerine hukuka aykırı erişildiği,
- 3 personelin söz konusu sorgulamalara konu olan kişilerin TCKN'lerini şahsi telefonları üzerinden üçüncü kişi/kişilerden temin ettikleri, personelin söz konusu verileri bankanın sistemlerini kullanarak aktardığına ilişkin bir bulgu olmadığı ancak şahsi telefonları üzerinden elektronik haberleşme programları kullanarak Banka dışına aktarmış olabileceği

ifadelerine yer verildiğinden hareketle yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 05.05.2020 tarih ve 2020/344 sayılı Kararı ile;

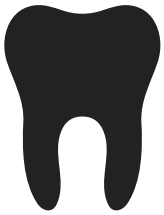
- İhlalden 25.288 kişinin etkilendiği, etkilenen kişilerden 17.582'sinin Banka müşterisi olduğu, 7.706 kişinin Banka müşterisi olmadığı dikkate alındığında özellikle Banka müşterisi olmayan kişilere ait KKB sorgulamaları için Banka tarafından zamanında gerekli teknik ve idari tedbirlerin almadığının değerlendirildiği,
- Kişisel Veri Güvenliği Rehberinde teknik tedbirler arasında yer alan "Kişisel Veri Güvenliğinin Takibi" başlığı altında belirtilen hususların aksine, Bankanın şubelerinden birinde ihlale sebep olan personelin ihlal fiillerinin 10.07.2017 tarihinde başlamasına rağmen; bu ihlal fiilinin 08.07.2019 tarihinde tespit edildiği; benzer şekilde Bankanın başka bir şubesindeki ihlal fiillerinin başlangıç tarihleriyle tespit tarihleri arasında 18 ay gibi oldukça uzun bir süre bulunduğu, bu durumun kişisel veri güvenliği takibi noktasında veri sorumlusu tarafından güvenlik yazılımı mesajlarının, erişim kontrolü kayıtlarının ve diğer raporlama araçlarının düzenli olarak kontrol edilmediğinin göstergesi olduğu,

- Kişisel Veri Güvenliği Rehberinde idari tedbirler arasında yer alan “Çalışanların Eğitilmesi ve Farkındalık Çalışmaları” başlığı altında ifade edilen, veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumluluklarının, görev tanımlarında belirlenmesi ve çalışanların bu konudaki rol ve sorumluluğunun farkında olmasının sağlanması gerektiği, ancak bunun veri sorumlusu tarafından sağlanmadığının görüldüğü,
- Veri sorumlusu tarafından ihlal öncesi yapılması gereken kullanıcı yetki ve rollerine yönelik kontrollerin ve düzenlemelerin ihlal sonrasında gerçekleştirilmiş olmasının gerekli idari tedbirlerin zamanında alınmadığının göstergesi olduğu,
- Veri sorumlusu tarafından ihlal öncesi yapılması gereken KKB sorgulama limitlendirilmesi gibi kritik önemi haiz tedbirlerin ihlal sonrasında gerçekleştirilmiş olmasının gerekli teknik tedbirlerin yeterince alınmadığının göstergesi olduğu,

dikkate alınarak, Kanunun 12 nci maddesinin (1) numaralı fıkrasına uygun olarak gerekli teknik ve idari tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **1.000.000 TL** idari para cezası uygulanmasına karar verilmiştir.

23/06/2020

Karar Tarihi : 23.06.2020
Karar No : 2020/485
Konu Özeti: Sezgi Dental Ağız ve Diş Sağlığı Polikliniği Veri İhlal Bildirimi



Veri sorumlusu sıfatını haiz olan Sezgi Dental Ağız ve Diş Sağlığı Polikliniği (Sezgi Dental) tarafından Kuruma gönderilen yazıda özetle;

- Sezgi Dental eski çalışanı diş hekiminin işten çıkartılması sonrasında poliklinik hastaları ile ilgili verileri yetkisiz olarak elde ettiği ve işten ayrıldığı,
- İşten ayrılan diş hekiminin Sezgi Dental kliniği hastalarına yeni açmış olduğu iş yeri ile ilgili tanıtıcı reklam amaçlı mesaj gönderdiği,
- Klinikte hasta kayıtlarının barındırıldığı bir otomasyon sisteminin kullanıldığı, bu otomasyon sisteme tüm diş hekimlerinin kendilerine özel olarak verilen kullanıcı adı ve şifre ile erişim sağlandığı,
- Söz konusu diş hekiminin çalıştığı dönem içerisinde bu otomasyon sistemine erişim yetkisinin bulunduğu, kendisine işten çıkartılması ile ilgili bildirim yapılmasından sonra hasta verilerini kopyalamış olduğunun tahmin edildiği,
- İhlalin 02.06.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin, kimlik ve iletişim verileri olduğu,
- hlalden etkilenen kişi sayısının tahmini 2.500 olduğu, otomasyon sistemine kayıtlı bulunan tüm hastalara sms gitmemesi sebebiyle kişi ve kayıt sayısının tespit edilemediği ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

23/06/2020
Karar Tarihi : 23.06.2020
Karar No : 2020/486
Konu Özeti: Avivasa Emeklilik ve Hayat A.Ş. Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan Avivasa Emeklilik ve Hayat A.Ş. (Avivasa) tarafından Kuruma gönderilen yazı ve ekinde özetle;

- Bir e-posta kullanıcısı tarafından 12 Haziran 2020 tarihinde Avivasa'ya iletilen ihbar sonucu inceleme çalışmalarının başlatıldığı, iletilen ihbarda bir internet sitesi üzerinden Avivasa'ya ait kişisel verilerin para karşılığında satıldığı iddiasının yer aldığı,
- İhlalden etkilenen kişisel veri kategorilerine yönelik ihbarda bilgi bulunmadığı,
- İhlalden etkilenen kişi ve kayıt sayısının bilinmediği,
- Konunun aynı zamanda adli makamlara da iletildiği,
- İlgili Sulh Ceza Hakimliğinin söz konusu internet sayfasına yönelik erişim engelleme Kararının bulunduğu bilgilerine yer verilmiş olup, yazı ekinde yer alan ilgili erişim engelleme Kararında *"…erişimin engellenmesi talebine konu olan içerik incelendiğinde, içerikte talepte bulunan şirketin müşterilerine ait olduğu değerlendirilen müşterilerin yaşadıkları şehir, yaş ve cep telefonu numarası gibi kişisel nitelikteki bir kısım verilerin liste halinde siteye konulduğu…"* tespitlerinin yer aldığı anlaşılmıştır.

Konuya ilişkin inceleme devam etmektedir.

23/06/2020

Karar Tarihi : 23.06.2020
Karar No : 2020/487
Konu Özeti: Avon Kozmetik Ürünleri Sanayi ve Ticaret A.Ş. Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan Avon Kozmetik Ürünleri Sanayi ve Ticaret A.Ş (Avon Türkiye) tarafından Kuruma gönderilen yazıda özetle;

- Avon Türkiye'nin bağlı olduğu İngiltere'de yerleşik Avon Cosmetics Limited'e (Avon Global) 7 Haziran 2020 tarihinde fidye yazılımı saldırısının gerçekleştiği,
- Saldırının bazı sistemlerin kesintiye uğramasına ve Türkiye'de dahil Avon'un uluslararası operasyonlarında belirli verilerin şifrelenmesine neden olduğu, etkilenen sistemlerdeki belirli verilerin tehdit aktörü tarafından kopyalanmış olması ve bu verilerin kişisel veriler içermesi ihtimalinin bulunduğu,
- Avon Türkiye'nin bağlı bulunduğu İngiltere'de yerleşik Avon Global ile aynı yazılımları kullandığı,
- Etkilenen kişisel veri kategorisi belirleme çalışmalarının devam ettiği,
- Etkilenen kişi sayısı ve kişilere ait kayıt sayısını belirleme çalışmalarının devam ettiği,
- Avon Türkiye'nin ağırlıklı olarak çalışanların ve Avon ürünlerini doğrudan satış yolu ile tüketicilere tali satıcılığını yapmakta olan Avon temsilcilerinin verilerine sahip olduğu bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmektedir.

BERKERBERKER

Hukuk Bürosu
Büyükdere Cad. No.185
Kanyon Kompleksi C Blok
K:8 D:9 34394 Şişli, İstanbul
+90 212 353 03 00
+90 212 353 03 02
info@berkerberker.com