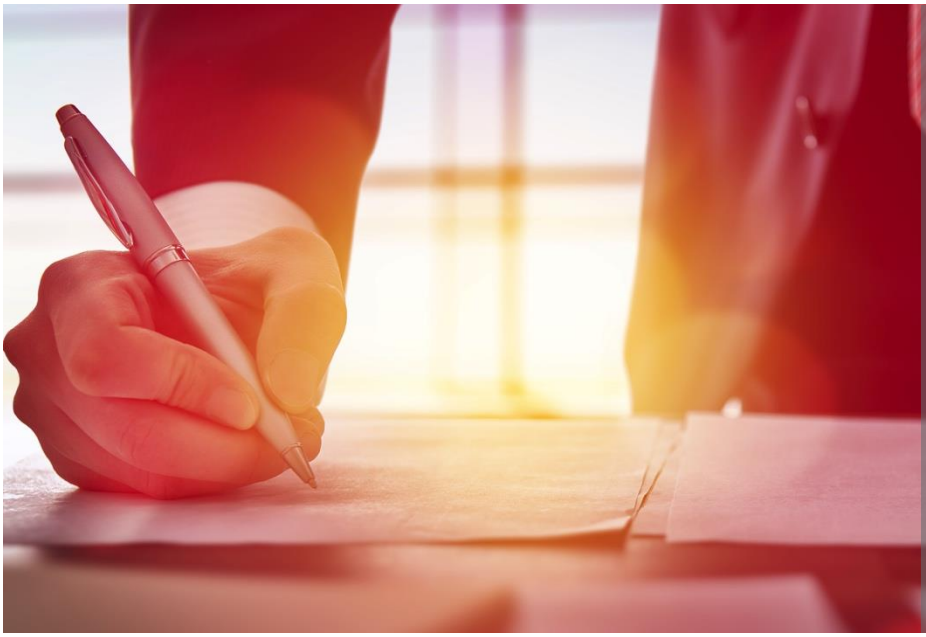

GSG Hukuk

Aylık KVK Bülteni

Ekim 2018

Bu sayıda

1 Güncel Haberler

2 Makale

Güncel Haberler:

Amazon Çalışanlarının Veri Satışı İddialarını Araştırıyor

Amazon, çalışanlarının veri brokerlarına veri sattığına ilişkin iddialar karşısında iç soruşturma başlattı. İddialara göre, Çin'deki Amazon çalışanları, veri brokerlarına ve tedarikçilere 80 ila 2.000 Amerikan Doları arasında değişen tutarlar üzerinden veri satışında bulundu.
Amozon şirketi, şirket içi politikalarının ihlali sebebiyle çalışanlarına yönelik kapsamlı bir iç soruşturma başlattığını doğruladı. Dünya çapında yarım milyondan fazla çalışanı bulunan Amazon'un kaç çalışanının hukuka aykırı şekilde veri satıcılığı yaptığı ve şirketin durumu fark ettikten sonra ilgili veri koruma kurumuna bildirimde bulunup bulunmadığı bilinmiyor. Çeşitli raporlara göre, Amazon yetkililerinin skandal karşısında bir zarar ile karşılaşması halinde çalışanlarına karşı para ve cezai yaptırım için dava açmaya hazırlandığı tahmin ediliyor. Amazon şirketinin Amerika'da da çalışan ihlallerini araştırdığı belirtiliyor.

Uber'e Sanal Saldırıyı Bildirmediği İçin 148milyon USD Ceza Verildi

Bilgisayar korsanları, 2016 yılının başlarında 57 milyon Uber sürücüsünün kişisel verilerine ulaşmış ve sürücülerin isimler, e-posta adresleri, telefon numaraları ve ehliyet bilgi ve numaralarına ulaşmıştı. Saldırının farkına varan şirket, korsanlara verileri silmeleri taahhüdü karşılığında 100.000 Amerikan Doları teklif etti. Uber Şirketine, saldırıyı takriben emniyet birimlerinin ilgili birimlerine ihbarda bulunmak yerine korsanlarla anlaşmaya çalışmış olması sebebiyle soruşturma açıldı. Şirket, Amerika Birleşik Devletleri'nin her bir eyaletini temsil eden 50 savcının açmış olduğu soruşturma sonrasında uzlaşmaya giderek 148 milyon Amerikan Doları tutarındaki cezayı ödemeyi kabul etti.

Facebook Kullanıcı Verilerine Saldırı

Facebook, Eylül ayı içerisinde kullanıcılarının verilerini hedefleyen yeni bir siber saldırıya maruz kaldığını açıkladı. Şirket'ten yapılan açıklamaya göre, saldırının nerden ve kim tarafından yapıldığı ve hedeflenen kullanıcıların neye göre sınıflandırıldığı hususları hala bilinmezliğini korurken, saldırganların 50 milyon civarında kullanıcının verilerini hedeflediği ancak verilere ulaşıp ulaşamadığı henüz bilinmemekte. İddialara göre saldırganlar, kullanıcı hesaplarına erişim kazanmak ve potansiyel olarak bunları kontrol altına almak için Facebook'un kodundaki bir özellikten faydalandılar. Saldırının, başarıya ulaşmış olması ihtimalinde, Cambridge Analytica skandalından daha büyük bir skandalı beraberinde getirebileceği iddia ediliyor.

Boost Finance Ltd. Şirketine 90bin GBP Ceza Verildi

ICO (Information Commissioner Office) , Londra merkezli pazarlama şirketi olan Boost Finance Ltd Şirketini 90.000 İngiliz Sterlini idari para cezasına hükmetti. Şirket'in, Ocak-Eylül 2017 döneminde üçüncü kişi ve müşterilere 4 milyondan fazla pazarlamaya ilişkin mail atmış olduğu ve bu maillerin birçoğunda abonelikten çıkma (unsubscription) seçeneğinin yer almamış olması Kurul'un kararında önem arz etti. Ayrıca aboneliğe onay veren kullanıcıların Şirket'in iştirakleri ve grup şirketlerinden gelecek pazarlama bildirimlerine ilişkin onay verdiği ve Boost Finance Ltd. tüzel kişiliğine yönelik herhangi bir abonelik elde etmemesi Kurul'un kararına esas teşkil eden husus olarak belirtildi.

Güncel Haberler:

ICO Heathrow Airport Ltd. Şirketine 120bin GBP Ceza Verdi

ICO (Information Commissioner Office), ağında depoladığı kişisel verilerin korunmasına yönelik yeterli önlemleri almaması sebebi ile Heathrow Airport Ltd. şirketine 120.000 İngiliz Sterlini idari para cezası kesti. Para cezasına esas teşkil eden olay kamuya açık bir alanda bir USB bellek bulunmasıyla gerçekleşti. Heathrow Airport çalışanına ait olan bu taşınabilir belleğin şifresiz bir şekilde kullanıma açık olması ağır bir güvenlik ihlali olarak kabul edildi. Belleğin içeriğindeki belgeleri görüntüleyen vatandaş sonrasında belleği ulusal medya kuruluşuna iletti ve bellekteki veriler burada kopyalandıktan sonra Şirket yetkililerine iletildi. Veri güvenliği açığı sonrasında ICO'nun gerçekleştirmiş olduğu inceleme sonucunda Şirket'in kişisel verilerin korunması politikasında ciddi gedikler olduğu ve veri koruma bakımından yeterli ve gerekli önlemleri almadığı görüldü. Şirket, taşınabilir bellek olayının ve ICO incelemesinin GDPR'ın yürürlüğe giriş tarihinden gerçekleşmiş olması sebebiyle en üst sınırdan ceza almaktan kıl payı kurtuldu.

Facebook Video-Chat Cihazı Gizlilik Endişeleriyle Karşılandı

Facebook, video konferans özelliği sağlayan yeni bir cihazı geçtiğimiz günlerde piyasaya sürdü. Kamera, ekran, mikrofon ve hoparlörden oluşan ve taşınabilir olan bu aygıt, kullanıcılara kolayca video konferans yapma özelliği sağlıyor. Facebook tarafından yapılan açıklamaya göre aygıt 140 derecelik geniş açılı kamera lensi içerecek ve bu lens oda içindeki kullanıcıları takip edebilme ve yüz tanıma sistemi bulunmasa dahi farklı kullanıcıları ayırt edebilme ve odaklanabilme özelliklerine sahip. Ancak Facebook'un piyasaya sürmüş olduğu bu yeni aygıt akıllara güvenlik ve gizlilik sorunlarını getirdi. Zira Facebook'un Cambridge Analytica skandalına ilişkin zihinler hala tazeliğini korurken video konferans yapabilme özelliğine sahip olan bu aygıtın mikrofon ve kamera aracılığı ile konuşma, görüntü ve ses kayıtlarının alınabileceği noktasında kamuoyunda ciddi bir şüphe devam etmekte. Zuckerberg ise bu eleştirilere cevaben güvenlik sistemlerinin derinlemesine bir şekilde kurulduğunu, tüm konuşmaların kriptolandığını ve kimsenin konuşma ve içeriklerinin dinlenmeyeceği ve kayıt altına alınmayacağı ifade etti. Ayrıca yapılan açıklamalarda aygıtta yer alan kamera ve mikrofonun kapatma ve açma özelliklerinin olduğu ve bu açma/kapama tuşu aracılığı ile kullanıcıların bu özellikleri devre dışı bırakabileceğinin altı çizilmiştir. Facebook tarafından piyasaya sürülen video konferans özelliği içeren taşınabilir bu aygıt kullanıcılara kolayca video konferans yapma özelliği sağlıyor. Ancak aygıtın piyasaya sürülmesi ile beraberinde gelen veri güvenliği ve gizlilik ile ilgili endişeler kesin olarak ortadan kaldırılmış değil. Facebook'un Cambridge Analytica sızıntısı dikkate alındığında Facebook'un bu aygıt aracılığı ile kullanıcıların verilerini toplayıp toplamayacağı ve veri güvenliği sisteminin belirtildiği şekilde güçlü olup olmadığı hususları ise hala belirsizliğini korumaktadır.

ICO Bupa Insurance Services Ltd'ye 175 bin GBP Ceza Verdi

ICO, sigorta hizmeti sunan Bupa Insurance Services Ltd ("Bupa") adlı şirkete yönelik 175.000 Pound tutarında para cezası öngördü. 2017 yılı içerisinde Bupa'nın çalışanlarından birinin 547.000 adet müşterinin kişisel verilerini şahsi email hesabına yollamak kaydıyla ele geçirdikten sonra bunları karanlık ağda satmaya yeltendi. Bupa'nın iş ortaklarından birinin durumu fark etmesi üzerine Şirket'in ihlalden haberdar olduğu öğrenildi. ICO'nun incelemesi sonucunda Şirket'in gerekli tedbir ve önlemleri alma konusunda yetersiz kaldığı ve verilerin tutulduğu sistem üzerinde düzenli olarak monitörleme yapmadığı anlaşıldı.

Güncel Haberler:

Hindistan'daki Aadhaar Yasası Veri Koruma Yasasına Karşı

Aadhaar, Hindistan'da ikamet eden gerçek kişilerin biyometrik ve demografik verilerini işlemek kaydıyla ortaya çıkan 12 haneli bir rakamdır. Bu rakamın temel veriliş amacı, devletin ülke sakinlerine çeşitli yardımlarını sağlaması sırasında sistematiğin oturtulabilmesidir. Ülkede 2016 yılında yürürlüğü giren Aadhaar Yasası ise Aadhaar numarasının kullanımına ilişkin usul ve esasları düzenlemektedir. Aadhaar Yasası yürürlüğe girmesiyle beraber gizlilik ve veri koruması noktalarında birçok eleştirinin odak noktası oldu. Hindistan Yüksek Mahkemesi'nin düzenlemeye ilişkin Eylül ayı içerisinde vermiş olduğu kararda ise düzenlemenin bazı maddelerinin tadil edilmek kaydıyla yürürlükte kalmasının uygun olduğu yönündedir. Yüksek Mahkeme'nin düzeltilmesini öngördüğü önemli hususlardan biri ise özel şirketlerin sözleşme ilişkisi içerisine girerken müşterilerinden Aadhaar numaralarını talep edebilme hakkına yönelik 57 numaralı maddedeki hükümdür.

Ayrıca Temmuz 2018 tarihinde açıklanan veriler uyarınca Hindistan'da ikamet eden 1,2 milyardan fazla insanın Aadhaar numarası aldığını göstermektedir. Depolanan veriler Hindistan devleti birimlerinden olan UIDAI'da depolanmaktadır. 1,2 milyardan fazla insanın hassas nitelikli verilerini depolayan UIDAI'nin veri güvenliği bakımından halihazırda sahip olduğu teknik ve idari tedbirler ise otoriteler tarafından ciddi şekilde eleştiri konusu olmaktadır. Nitekim yapılan teknik testlerde ilgili kurumun tam anlamıyla sızıntıya engel olabilecek mekanizmaları monte etmediği ve herhangi bir saldırı durumunda birçok insanın verilerinin çalınabileceği görüşü ağırlık kazanmaktadır.

KVK Makalesi:

Dış Kaynak Hizmeti için Veri Paylaşım Sözleşmesi İmzalanmalı mı?

Günümüzde birçok firma, çeşitli hizmet sağlayıcıları ile anlaşarak faaliyetlerini yürütmek adına dış kaynaklardan destek almaktadır. **Outsourcing** kavramı ile ifade edilebilecek dış kaynak hizmet kullanımındaki temel amaçlar mali ve operasyonel anlamda yarar sağlamak, verim elde etmek ya da giderleri azaltmak olarak gösterilebilir. Ancak outsourcing hizmeti, gerek hizmeti alan gerekse de hizmeti sağlayan bakımından kişisel verilerin korunmasına ilişkin düzenlemeler ve uygulamalar ışığında hukuki olarak değerlendirilmelidir. Nitekim taraflar dış kaynak hizmeti aldıkları şirketlerin gerekli hukuki, idari ve teknik tedbirleri aldığından emin olmalıdır.

Bu bağlamda öncelikli olarak değerlendirilmesi gereken husus veri aktarımına ilişkindir. Dışarıdan hizmet alan şirket, hizmetin gerçekleştirilmesi adına müşterilerinin, çalışanlarının veya üçüncü kişilerinin verilerini outsourcing şirketine aktarabilmektedir. Her ne kadar bu aktarım outsourcing faaliyetine esas teşkil eden sözleşmenin kapsamında olsa da bir veri transferinin söz konusu olduğu açıktır. Veri transferine ilişkin taraflar arasında bir veri aktarım sözleşmesi yapılmalı ve veri aktarımından kaynaklanabilecek riskler iki taraf için de asgari düzeye indirilmelidir.

Bir diğer önem teşkil eden husus ise outsourcing hizmetinin taraflarının hangisinin veri sorumlusu ve veri işleyen sıfatını haiz olacağına yöneliktir. Burada dikkat edilmesi gereken husus outsourcing faaliyetini gerçekleştirmek adına yapılacak veri transferinin amacı ve kapsamına ilişkindir. Veri işleyen, ***veri sorumlusu olan gerçek veya tüzel kişinin verdiği yetkiye dayanarak onun adına kişisel verileri işleyen*** taraftır. Bu durumda örneğin, veri sorumlusu olan şirketler, verilerini depolanması ve saklanması adına bir dış kaynak oluşturma yoluna gittiği takdirde bu hususta verileri güvenli bir şekilde koruma ve depolama yükümlülüğü altında olan taraf hizmet sağlayıcı olacaktır ve veri işleyen sıfatını haiz olacaktır. Böylece dış kaynak hizmeti sağlayıcısı, herhangi bir veri işleyenin alması gereken idari ve teknik tedbirleri dikkate almak durumunda kalacaktır. Ancak belirtmek gerekir ki, veri işleyenin bu durumlarda kendi çalışanlarına karşı veri sorumluluğu sıfatı ise devam edecektir.

Ancak her outsourcing hizmeti durumunda bir veri paylaşım sözleşmesi imzalanması gerekli olmalı mıdır? Eğer taraflar B2B bir hizmet ilişkisi içindeyse ve bir tarafın karşı taraf ile paylaştığı kişisel veri sadece kendi çalışanlarına ilişkin iletişim detayları (isim – soyad, e-mail, telefon) ile sınırlıysa yine de bu kişisel verilerin korunmasına ilişkin bir veri paylaşım sözleşmesi imzalanmalı mıdır? Örneğin otomotiv sektöründe üretim yapan bir şirketin ürettiği malın tedarikçisi firma ile paylaştığı kişisel veri, bu işi yürüten çalışanların e-mail imzalarının altında bulunan iletişim verileri ile sınırlı olacaktır. Bu durumda sadece bu iletişim verilerinin korunmasına ilişkin her tedarikçi ile veri paylaşım sözleşmesi imzalanması oldukça ciddi bir iş yükü doğurmaktadır.

Kanaatimizce sadece bu tür iletişim verisi paylaşılan, şirketlerin özel nitelikli kişisel veri işlenen bir alanda faaliyet göstermediği ve alınan hizmetin içeriğinde başka bir kişisel veri paylaşımı olmayan durumlarda veri paylaşım sözleşmesi imzalanması zaruri olmamalıdır. Veri paylaşım sözleşmesinin hizmetin niteliği itibariyle kişisel verilerin işlenmesini gerektiren hizmetler için aranması gerektiği görüşündeyiz. Bu kapsamda ilerleyen günlerde bir Kurul kararı yayınlanması uygulamayı rahatlatacaktır. Nitekim uygulamada tamamen B2B faaliyet yürütülen taraflar arasında veri paylaşım sözleşmesi imzalanmakta ve bu durum özellikle avukatların iş yükünü oldukça fazla meşgul etmektedir.

Kısaltmalar

ICO	Information Commissioner's Office
GDPR	General Data Protection Regulation
Kurum	Kişisel Verileri Koruma Kurumu
Kurul	Kişisel Verileri Koruma Kurulu
KVKK	Kişisel Verileri Koruma Kanunu
m.	Madde
Örn.	Örnek

GSG Hukuk

Aylık Kişisel Verilerin Korunması Hukuku Bülteni

Ekim 2018

www.gsghukuk.com

KVKK kapsamında yerine getirmeniz gereken hukuki yükümlülükler hakkında daha detaylı bilgi almak için bizimle iletişime geçin

Süleyman Seba Cad.
No :48 BJK Plaza B Blok
K:4 Akaretler
Beşiktaş - İstanbul

+90 212 326 68 68

+90 212 326 68 69

info@gsghukuk.com

Nilgün Serdar Şimşek, LL.M.
Ortak, Avukat
T: +90 (212) 326 63 68
nilgun.simsek@gsghukuk.com

Rıza Eroğlu
Kıdemli Müdür
T: +90 (212) 326 64 61
riza.eroglu@gsghukuk.com

İpek Okucu Taftalı
Müdür, Avukat
T: +90 (212) 326 60 68
ipek.okucu@gsghukuk.com

© 2018 Gündüz Şimşek Gago Avukatlık Ortaklığı. Tüm hakları saklıdır.

Bu dokümanda “GSG Avukatlık Ortaklığı” veya “GSG Hukuk” ibaresi, Gündüz Şimşek Gago Avukatlık Ortaklığı’nı ifade etmektedir.