



KVK BÜLTENİ

Nazalı Avukatlık Ortaklığı olarak, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında gündeme gelen konular ve yenilikler hakkında hazırladığımız KVK Bültenimizdir.

İçindekiler

Duyurular	Sf. 1
GDPR	Sf. 3
Ulusal ve Uluslararası Kararlar	Sf. 6

DUYURULAR

- Yurt Dışına Veri Aktarımına İlişkin Esaslar Hakkında Duyuru
- Veri Sorumlularının Uygun Güvenlik Düzeyini Temin Etmeleri Hakkında Duyuru
- Veri İhlali Bildirimi Hakkında Kamuoyu Duyurusu
- Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) Yürürlüğe Girmesi Hakkında Duyuru

▪ Yurt Dışına Veri Aktarımına İlişkin Esaslar Hakkında Duyuru

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("Kanun") 9. maddesi uyarınca; kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunmaması halinde, veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri gerektiği öngörülmüş olup, Kişisel Verileri Koruma Kurumu ("Kurum") tarafından yayınlanan Yurt Dışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar belirlenmiştir. Kurum tarafından yayınlanan metinde, ikili bir ayırım benimsenerek konu, Veri Sorumlusundan Veri İşleyene Aktarım ve Veri Sorumlusundan Veri Sorumlusuna Aktarım olarak iki ayrı başlık altında incelenmiştir.

▪ Veri Sorumlularının Uygun Güvenlik Düzeyini Temin Etmeleri Hakkında Duyuru

Veri sorumlusu nezdinde, buldukları pozisyon ve görev itibarıyla kişisel verilere erişime yetkisi olanlar tarafından yetkilerini aşarak ve işleme amacı dışında söz konusu verilerin işlendiği hususunda Kurula intikal eden ihbar ve şikâyetlere ilişkin yapılan değerlendirme sonucunda uygulamada yaşanan problemlerin önüne geçilebilmesi amacıyla Kurulun yaptığı değerlendirmeler neticesinde "31.05.2018 karar tarihli ve 2018/63 karar numaralı Kurul Kararı" 04.07.2018 tarihli Resmi Gazete'de yayımlanmıştır. Kurul kararında, kişisel verilerin işleme amacı dışında işlenmesi ve üçüncü kişilerle paylaşılması durumunda önlem alınması gerekliliğinden ve bu önlemleri almakla yükümlü kişilerin bilgilendirilmesinden söz edilmiştir. Veri sorumluları, Karar doğrultusunda ilgili verileri kanuna uygun olarak muhafaza etmek ve güvenlik düzeyini temin etmekle yükümlüdür.



▪ Veri İhlali Bildirimi Hakkında Kamuoyu Duyurusu

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12. maddesinin (5) numaralı fıkrasında öngörüldüğü üzere; veri sorumluları tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından



KAMUOYU DUYURUSU (VERİ İHLALI BİLDİRİMİ)

elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kişisel Verileri Koruma Kurulu'na ("Kurul") bildirmekle yükümlüdür ve Kurul, gerekli gördüğü durumlarda, söz konusu ihlali, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilecektir.

Anılan düzenleme çerçevesinde 29.06.2018 tarihinde Kurul'un sitesinde yayımlanan "Kamuoyu Bildirisi (Veri İhlali Bildirimi)" ile Ticketmaster UK ("Ticketmaster İngiltere") adına Biletix Bilet Dağıtım Basım ve Tic. A.Ş. ("Biletix A.Ş.") tarafından 28.06.2018 tarihinde yapılan kötü niyetli yazılım tespiti ve ihlal bildirimi hakkında bilgi verilmiş ve söz konusu ihlal durumu hakkında değerlendirmeler yapılmıştır.

▪ Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) Yürürlüğe Girmesi Hakkında Duyuru



Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) 25 Mayıs 2018 tarihinde yürürlüğe girmesiyle, Avrupa Birliği'nin yıllardır yürürlükte olan 95/46/EC sayılı Veri Koruma Direktifi mülga olmuş ve bunun neticesinde kişisel verilerin korunması alanında köklü değişiklikler meydana gelmiştir. GDPR ile veri koruma hukukuna kazandırılan yeni kavram ve düzenlemeler ile mevzuata uyum sağlanması şartları ağırlaştırılırken, uygulama alanı da genişletilerek bazı hallerde Avrupa Birliği üyesi olmayan ülkelerde bulunan veri sorumlularının da ilgili düzenlemelere uyumlu hale gelmesi gerekliliği ortaya çıkmıştır.

GDPR



1.GDPR Kapsamında İlgili Kişinin Başvuru ve Şikayet Hakkı

GDPR Kapsamında Şirketlere ve Otoritelere Yapılan Başvurular Arttı

GDPR'a Aykırılık Durumunda Otoriteler Tarafından Verilebilecek Cezalar

GDPR Kapsamında Veri Süjesinin Başvuru ve Şikayet Hakkı

- Veri Süjesinin Başvuru/Erişim Hakkı ("*right of access*") Nedir?

Veri sorumlusuna başvurarak; kendileriyle ilgili kişisel verilerin işlenip işlenmediğini öğrenmek, işlenmişse bunları talep etmek, verinin muhtevasının eksik veya yanlış olması halinde bunların düzeltilmesini, hukuka aykırı olması halinde ise silinmesini, yok edilmesini ve buna göre yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini ve verilerin kanuna aykırı olarak işlenmesi sebebiyle zararlarının giderilmesini talep etme hakkı, veri süjesinin başvuru hakkıdır.

- Veri Süjesinin Şikayet Hakkı ("*right to complaint*") Nedir?

Veri süjesi; veri sorumlusuna yapmış olduğu başvurunun kanun kapsamında öngörülen süre zarfında cevaplanmamış olması, reddedilmesi, verilen cevabın yetersiz bulunması sebebiyle, hakkının yerine getirilmesini, şikayet hakkı kapsamında, kurulan otoritelerden talep edebilmektedir. Bu hak, veri süjesinin mahkemeler nezdinde dava açma hakkına halel getirmemektedir.



GDPR Kapsamında Şirketlere ve Otoritelere Yapılan Başvurular Arttı

Kişisel verilerin korunması alanına önceki düzenlemelere nazaran daha ağır usul ve esaslar getiren GDPR'ın yürürlüğe girmesinin üzerinden henüz 1,5 ay geçmiş olmasına rağmen oluşan yoğunluk ve şimdiden gerçekleştirilen fazla sayıda başvuru sebebiyle, şirketler ve otoriteler, ilgili prosedürleri yerine getirmekte ve süreci yürütmekte zorlanmaktadır.

GDPR ile bireylere tanınan haklar doğrultusunda veri s jeleri tarafından kiřisel verilerinin nasıl ve ne amala kullanıldığını öğrenmek, kendileriyle paylaşılmasını saėlamak yahut kiřisel verilerinin silinmesini talep etmek adına řirketlere ve otoritelere yapılan bařvurular sıklasmış olup; řirketler ve otoriteler söz konusu bařvuruları yanıtlayarak kanuni yüküml l klerini yerine getirebilmek amacıyla yoğun bir alıřma iine girmiřtir.

▪ řirketlere Yapılan Bařvurular

Geniř m řteri aėına sahip global řirketler, faaliyetleri daha k  k aplı olan řirketlere kıyasla daha yoğun řekilde bařvuru almaktadır. İřledikleri kiřisel verilerin niteliėi gereėi teknoloji řirketleri, medya grupları, perakendeciler ve bankalar söz konusu bařvuruların cevaplanabilmesi iin ciddi bir alıřma y r tmektedirler. Finans řirketleri gibi yoğun kiřisel veri iřlemesinin söz konusu olduėu řirketler de GDPR ile getirilen usul ve esaslar ile olduka aėır bir y k altına girmiř bulunmaktadır.

WH Ireland gibi uzun yıllardır faaliyet g steren řirketler bug ne kadar ok fazla kiřisel veri iřlemiř olmaları sebebiyle, mevzuata uyum s recinde diėerlerine oranla ok daha sıkı bir alıřma y r tmekte olup, ilgili s rete ok vakit kaybettiklerini dile getirmektedirler. řirketin İcra Kurulu Bařkanı Richard Killingbeck, sadece fiziken tutulmuş 5.000 kartonu ařkın kiřisel verinin bulunması ve g n y z ne ıkartılması iin birok personelin sadece bu iře memur edildiėini ve hala konu kapsamındaki eksikliklerini gideremediklerini ifade etmektedir.

Bireylerin, kiřisel verilerine iliřkin řirketlere yaptıėı bařvuruların bu denli yoğunluk g stermesinin ardında ise Cambridge Analytica skandalının olduėu belirtilmektedir. İngiltere’de kurulu Monzo Bank’ın Hukuk ve Compliance B l m  Sorumlusu Frances Coyle, insanların řirketlerde bulunan verilerinin 3. kiřilerle paylaşılıp paylaşılmadıėını merak ettiėini ve bu nedenle bařvuruların bu kadar yoğunlařtıėını dile getiriyor.

The L.A. Times, the Chicago Times ve unroll.me (*maillere d řen spamleri engelleyen bir mail uygulaması řirketi*) gibi b y k kuruluřlar ise GDPR’a uyum saėlamak ve bařvurularla muhatap olmaksızın Avrupa’daki faaliyetlerini askıya alma yolunu seerek, řimdilik Avrupa’daki hizmetlerini durdurma kararı almıřlardır.

▪ Otoritelere Yapılan Bařvurular

Britanya Veri Komisyonu Ofisi’nden (*“Ofis”*) yapılan aıklamaya g re GDPR’ın y r rl ėe girmesinden itibaren řimdiye kadar Ofis’e 1000’i ařkın Őikayet bařvurusunda bulunulmuş ve bu Őikayetlerin incelenmesi sonucu birok veri ihlali tespit edilmiş bulunmaktadır. Ofis nezdinde y r t len alıřmalar ve GDPR h k mleri gereėi de Dixons Carphone ve Ticketmaster gibi İngiliz firmalar, sistemlerinde meydana gelen ihlalleri kamuoyunun bilgisine sunmak adına bildirimlerde bulunmuřtur. Bu y n yle bireylerin otoritelere yaptıkları bařvuruların sonu doėurmaya bařladıėı d ř n lebilir.

İrlanda Veri Koruma Komisyonu’na ise GDPR’ın y r rl ėe girmesinden bu yana 500’ n  zerinde veri ihlali ve 300’ n  zerinde Őikayet bildirimi yapılmıřtır. ek Cumhuriyeti ve Fransa’da da bařvuru yoğunluėu konusunda herhangi bir farklılık bulunmayıp, iki  lkede yer alan otoritelere GDPR’ın y r rl ėe girmesinin ardından bug ne kadar 400’ n  zerinde veri ihlali ve Őikayet bildirimi ulařmış durumdadır.

Bařvuruların yoğunluėunun artarak mı yoksa azalarak mı s receėi konusunda bir fikir beyan etmek řu an iin m mk n olmamakla birlikte, -her ne kadar bireylerde kiřisel veriler konusunda bir farkındalık bilinci oluřsa

da-, otoritelerin ve şirketlerin konu üzerinde kazandığı tecrübeler mutad prosedürler oluşmasına zemin hazırlayabilecek ve başvurulardaki yoğunluğun azalması sonucunu doğurabilecektir¹.

▪ **GDPR'a Aykırılık Durumunda Otoriteler Tarafından Verilebilecek Cezalar**

GDPR'a uyum sağlamamanın 20 milyon Euro, yahut şirketin yıllık gelirinin %4'üne (ya da fazlasına) tekabül edebilecek sert maddi yaptırımları olabilecektir.

Oliver Wyman²'in tahminine göre kanunun yürürlükte olacağı ilk yıl, uyum sağlamayan şirketler üzerinden AB 6 milyon € gibi bir gelir elde edebilecektir.

Cevabı belirli olmayan en büyük soru ise cezaların nasıl tatbik edileceği sorunudur. Örneğin, uyum sağlamayan şirketlere kesilecek tüm ceza miktarları aynı mı olacaktır yoksa ihlalin büyüklüğü oranında cezanın miktarı değişecek midir? Bu yöndeki görüş birliği ise otoritelerin mevzuata uyum sağlamamış şirketlerin üzerine hızlıca giderek böylesi sorulara karşın şirketleri bilgilendirecek ilke kararlar vereceği ve uygulamayı yönlendireceği üzerinedir.

AB üye ülkelerince oluşturulan komisyonlar GDPR ihlallerini soruşturacak ve ihlalleri ortadan kaldırmak adına karar verebileceklerdir. Uyarı cezası, ilgili ihlalin düzeltilmesi adına karar alma, GDPR'a uyum sağlanması kararı alınması ve veri işleme aktivitelerinin durdurulmasına yönelik tedbirler alma, komisyonlarca alınabilecek bazı aksiyonlardır. Bunların yanında pek tabii ki komisyon para cezaları da verebilecektir.

Komisyonların ceza verirken göz önünde bulunduracağı hususlar ise; ihlalin sürekliliği, ortaya çıkan zararın boyutu, ihmalin büyüklüğü, veri sahibinin zararı azaltmak için gösterdiği çaba, önceki ihlaller, davalı şirketin komisyonla yaptığı iş birliği ve zararın boyutunu etkileyen başkaca faktörler olacaktır.

Şirketlerin cezalandırılması için komisyonlara kişiler tarafından yapılacak başvurular yahut şikayetler sonrasında denetleyici kurumun denetçileri şirketlerin yönetmeliğe uyum sağlayıp sağlamadığını denetleyecekler ve bunun ardından kararlarını vereceklerdir.

¹ Ayrıntılı bilgi için bkz. <https://www.ft.com/content/31d9286a-7bac-11e8-8e67-1e1a0846c475>

² Ayrıntılı bilgi için bkz. <http://www.oliverwyman.com/our-expertise/hubs/gdpr.html>

ULUSAL VE ULUSLARARASI KARARLAR



Yargıtay 12. Ceza Dairesi Kararı : "*Kişisel Verinin Tanımı ve Yorumlanması*"

1.IP Adresi Kişisel Veri Olarak Değerlendirilebilir mi?

■ Yargıtay 12. Ceza Dairesi Kararı : "*Kişisel Verinin Tanımı ve Yorumlanması*"

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda "*kişisel veri*" kavramının tanımı yapılmış ancak Kanun kapsamında korunan kişisel verilerin hangileri olduğu ya da bunun tespiti sürecinde nasıl bir yorum yapılması gerektiği yönünde bir açıklamaya yer verilmemiştir. Yargıtay 12. Ceza Dairesi'nin 2017/12083 E. ve 2018/2539 K. no.lu kararında³ kişisel verilerin tanımlanması ve yorumlanmasına ilişkin esaslar değerlendirilmiştir.

Söz konusu karara göre 5237 sayılı Türk Ceza Kanunu'nun ("*TCK*") 136. maddesinde düzenlenen "*Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme*" suçunun konusunu oluşturan "*kişisel veri*" kavramından ne anlaşılması gerektiği hususu açıklanmış ve kişinin yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı "*nüfus bilgileri, adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilgi*"nin kişisel veri olarak kabul edilmesi gerektiği değerlendirilmiştir.

Ne var ki; bu yönde bir yorumun, kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun uygulama alanını amaçlanandan fazla genişleterek uygulamada bir belirsizlik yaratacağı ve kişisel verilerin işlenmesi ve aktarılmasını içeren her türlü eylemin suç sayılması riskini ortaya çıkaracağı yönündeki endişeler belirtilerek; TCK m. 136'nın uygulanmasında somut olayın özelliklerinin dikkate alınması ve suça konu olayda herhangi bir hukuka uygunluk nedeninin olup olmadığının değerlendirilmesinin, sanığın gerçekleştirdiği eylem ile hukuka aykırı hareket ettiğinin bilincinde olup olmadığı yönünde tespitlerin gerçekleştirilmesinin gerektiği de karar içerisinde belirtilmiştir.

³ Karar için bkz. <http://www.kazanci.com/kho2/ibb/files/dsp.php?fn=12cd-2017-12083.htm&kw=%60E.2017/12083%60#fm>

▪ IP Adresi Kişisel Veri Olarak Değerlendirilebilir mi?

95/46/EC sayılı AB Veri Koruma Direktifi, (“*Direktif*”) veri süjesini belirleyen yahut belirlenebilir kılan verilerin işlenmesi özelinde uygulanmakta ve direktifin uygulama alanı dahilindeki her kişinin/kurumun, bünyesinde barındırdığı kişisel verileri direktifin öngördüğü şekilde işlemeye özen göstermek durumunda bırakılmaktaydı. 25 Mayıs 2018’de yürürlüğe giren GDPR ile artık bu özen borcu, veri sorumluları üzerine bırakılan bir yükümlülüğe dönüşmüştür.

GDPR, veri sorumlularını işledikleri kişisel veriler dolayısı ile sorumlu tutmakta olup, veri sorumlularına mevzuata uyum sağma şartı getirmiştir. Uyum sağlamayan şirketler ise, yalnızca ihlalin meydana geldiği bölgede değil, dünya çapında elde ettikleri yıllık gelirlerinin %4’üne varan miktarlarda ceza ile karşı karşıya kalabileceklerdir. Herhangi bir ihlal halinde söz konusu sorumluluktan kurtulmanın en kolay şekli ise; şirket tarafından işlenen ihlal konusu verinin kişisel veri olmadığı ileri sürülmesi ve ispatlanması olacaktır.

Avrupa Birliği Adalet Divanı’nın (“*Divan*”) işbu kararı bu anlamda büyük önem teşkil etmektedir. Zira Divan, kararında kişilere ait IP adreslerinin kişisel veri sayılıp sayılmayacağı özelinde kişisel veri kavramının tanımı kapsamlı olarak ele almıştır. Divan “*Breyer⁴*” davası olarak bilinen yargılamada kurum ve kuruluşların pratiğini değiştirecek bir karara imza atarak⁵, her ne kadar IP adresi bilgilerinin kişileri doğrudan doğruya belirlemeyeceğini ya da belirlenebilir kılmayacağını ifade etmiş olsa da, dinamik IP adresi bilgilerinin kişisel veri olarak nitelendirilmesi gerektiğine hükmetmiştir.

Breyer davasındaki sorular, Divan’a Alman Mahkemelerince yönlendirilmiştir. Avrupa Birliği içinde uygulanan mevzuatın farklı yorumlamalar sonucu farklı uygulamalar göstermemesi adına kurulan Divan bu yargılamada, Alman Mahkemeleri tarafından yöneltilen “*kişilere ait IP adresleri Kişisel Veri niteliğinde midir?*” sorusunu cevaplandırmıştır.

Mahkeme dosyasından bilindiği kadarıyla Alman Federal kurumları, meydana gelebilecek siber saldırıları önlemek ve olası bir soruşturma faaliyetinde kullanmak adına web sitelerine giren her kullanıcının, bağlantı sona erdikten sonra dahi, hangi siteye giriş sağladığı, ne zaman giriş sağladığı, transfer ettiği data miktarı, arama alanlarına yazdıkları ve IP adresleri bilgilerini depolamaktadır. Breyer ise Alman Mahkemelerine yaptığı başvuruda bu verilerinin kullanılmasını engellemek adına verilerin imha edilmesi talebinde bulunmuştur. Talep karşısında kişilere ait IP adreslerinin kişisel veri olup olmadığı noktasında Alman Mahkemeleri kesin bir kanıya ulaşamamış, lakin değerlendirmelerinde kimi bilgisayarların geçici IP’leri bulunurken, kimi bilgisayarların da kalıcı IP adresleri bulunduğu ifade edilmiştir. Ayrıca salt IP adresine sahip olmanın kişiyi belirlenebilir kılmaya muktedir olmadığını belirten Mahkeme, sorunun çözümünü Divan’a bırakmıştır.

Divan konuyu değerlendirirken Alman hukuku uyarınca ilgili cezai prosedürlerin kişilerin internet bilgisini tutan diğer kurumlar tarafından da yürütülebileceğini ve bu yüzden kişilere ait IP adreslerinin depolanmaması gerektiğini söyleyerek, üçüncü bir kişi aracılığı ile de olsa, kişiyi belirlenebilir kılmaya muktedir geçici/kalıcı IP adreslerinin yasal düzenlemeler uyarınca kişisel veri olarak kabul edilmesi gerektiğinin altını çizmiştir.

⁴ Patrick Breyer v. Bundesrepublik Deutschland.

⁵ ECLI:EU:C:2016:779; 19.10.2016

EKİBİMİZ



Ersin Nazalı

Yönetici Ortak,
Avukat, Yeminli Mali Müşavir
enazali@nazali.av.tr



Hatice Zümbül

Kıdemli Avukat
hzumbul@nazali.av.tr

Bu bültende yer verilen açıklamalarımız, hukuki görüş ve tavsiye niteliğinde olmayıp, konuya ilişkin genel bilgiler içermektedir; bu sebeple belirtilen konularda bir aksiyon almadan önce, bir uzmana danışmanızı tavsiye ederiz. NAZALI'ya işbu dokümanın içeriğinden kaynaklanan veya içeriğine ilişkin olarak ortaya çıkan sonuçlardan dolayı herhangi bir sorumluluk iddiasında bulunulamaz.

Bu yazı hakkında daha fazla bilgi almak için lütfen Av. Ersin Nazalı ve Av. Hatice Zümbül ile irtibata geçiniz.



İSTANBUL OFİS

19 Mayıs Cad. Dr. İsmet Öztürk Sok.
No: 3 Elit Residence Kat 10/23 - 29/60
Şişli 34360 İstanbul, Türkiye

Tel : +90 212 380 0640

Faks : +90 212 217 1890

ANKARA OFİS

Kızılırmak Mah. 1450 Sok. Ankara Ticaret
Merkezi (ATM) B Blok No: 1/29 Kat 5
Karakusunlar, Çankaya, Ankara, Türkiye

Tel : +90 312 286 1006

Faks : +90 312 286 1007

İZMİR OFİS

Adalet Mah. Manas Bulvarı Folkart
Towers B Kule No: 47/2209
Bayraklı, İzmir, Türkiye

Tel : +90 232 290 0998

Faks : +90 232 290 0999

BURSA OFİS

Odunluk Mah. Akademi Cad. Zeno
Center C Blok No: 2/14 Kat 3
Nilüfer, Bursa, Türkiye

Tel : +90 224 441 19 50

Faks : +90 224 441 19 51

