12 Mart 2018

# VERİ GÜVENLİĞİ REHBERİ'NE DAİR NOTLAR

7 Nisan 2016 tarihinde yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 sayılı Kanun) uygulanmasına yönelik olarak, Kişisel Verileri Koruma Kurulu (Kurul) tarafından çeşitli rehberler ve açıklama/bilgilendirme metinleri yayımlanmaktadır. Son dönemde oldukça aktif şekilde faaliyet gösteren ve iki ilke kararı da yayımlayan Kurul, son olarak veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapma yükümlülüğü kapsamında Veri Güvenliği Rehberi'ni (Rehber) yayımlamıştır. Bu yazıda Kurul'un ilke kararları ve diğer ülkelerden örneklerle Rehber'e dair açıklamalara yer verilecektir.

Kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla yayımlanan Rehber'in veri sorumlusunun veri güvenliğini sağlama yükümlülükleri bakımından önümüzdeki süreçte oldukça aydınlatıcı nitelikte olacağı söylenebilecektir. Bilindiği üzere 6698 sayılı Kanun'un 12. maddesinde veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerine yer verilmiş ve 18. maddede veri güvenliğine ilişkin yükümlülüklerini yerine getirmeyenler hakkında **15.000 TL**'den **1.000.000 TL**'ye kadar idari para cezası verilebileceği hüküm altına alınmıştır.

Hatırlanacağı üzere Kurul ilk ilke kararlarından olan 21.12.2017 tarih ve 2017/62 sayılı ilke kararında veri güvenliğinin sağlanmasına ilişkin olarak veri sorumlusunun yükümlülüklerini hatırlatarak, **gerekli teknik ve idari tedbirleri almaması halinde Kanun'un 18. maddesi çerçevesinde cezalandırılacağını** belirtmişti. Veri güvenliğinin sağlanması bakımından yurtdışındaki uygulamalar incelendiğinde ise yakın zamanda Fransa Ulusal Bilişim ve Özgürlükler Komisyonu (CNIL) (Komisyon) tarafından verilen karar dikkat çekmektedir. Kararda elektronik şirketi olarak faaliyet gösteren Darty'nin satış sonrası hizmetlerine ilişkin olarak internet sitesinde güvenlik açığı olduğu şeklindeki bir şikâyet üzerine Komisyon tarafından başlatılan incelemede; başvuru formuna ilişkin linkteki açık sebebiyle, satış sonrası hizmet talebi için form dolduran Darty müşterilerinin diğer müşterilerin isim, soy isim, e-posta adresi ve telefon numarası gibi bilgilerine kolaylıkla ulaşılabildiği tespit edilmiş ve Darty'e **100.000 Avro para cezası** verilmiştir[1].

Veri güvenliği ihlali halinde; 6698 sayılı Kanun'da yer alan idari para cezası, Kurul'un ilke kararı ile yaptırım uygulayacağına dair sinyaller vermesi ve yurt dışındaki uygulamalar birlikte değerlendirildiğinde veri güvenliğinin önümüzdeki süreçte büyük öneme sahip olacağı söylenebilecektir. Bu sebeple veri güvenliğinin sağlanması bakımından oldukça yol gösterici ve açıklayıcı nitelikteki Rehber'deki tedbirlerin özenle yerine getirilmesi önemlidir.

[1] Komisyon kararına ilişkin yazımız için bkz. http://www.ari.av.tr/wp-content/uploads/Fransa-Bilisim-Komisyonu-Darty-Karari.pdf

ARI AVUKATLIK BÜROSU

Rehber'de veri güvenliğine ilişkin tedbirlere ikili bir ayrım yapılarak yer verilmiştir. Rehber'in ilk bölümünde "idari tedbirler"e ilişkin açıklamalara yer verilirken, ikinci bölümünde "teknik tedbirler" açıklanmıştır. Gerek idari gerek teknik tedbirler elde edilen kişisel verilerin güvenli bir şekilde saklanmasına yönelik olup, tek bir sefer değil sürekli olarak uygulanması ve iç işleyişte çalışma düzeninin bir parçası haline getirilmesi gereken tedbirler olması dolayısıyla oldukça önemlidir. Tedbirlere ilişkin açıklamalar aşağıdaki şekilde özetlenebilecektir:

## 1. İDARİ TEDBİRLER

Genel olarak şirketin iç işleyişi ile ilgili olan idari tedbirler; kişisel veri işleme envanteri hazırlanması, kurumsal politikalar hazırlanması (Erişim, bilgi güvenliği, kullanım, saklama, imha vb), sözleşmeler (veri sorumlusu ile veri sorumlusu, veri sorumlusu ile veri işleyen arasında), gizlilik taahhütnameleri, kurum içi periyodik ve/veya rastgele denetimler, risk analizleri, iş sözleşmesi hükümleri, disiplin yönetmeliğine Kanun'a uygun hükümler eklenmesi, kurumsal iletişim (kriz yönetimi, Kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.), eğitim ve farkındalık faaliyetleri (özellikle bilgi güvenliği ve kanun hakkında), Veri Sorumluları Sicil Bilgi Sistemine bildirim olarak sayılmaktadır. Rehber'de yer verilen idari tedbirlere daha yakından bakıldığında dikkat çeken hususlara aşağıda yer verilmiştir.

**1- Mevcut risk ve tehditlerin belirlenmesi gerekmektedir:**

- Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından, işlenen tüm kişisel verilerin -özel nitelikli verilerin belirtilmesi suretiyle- neler olduğunun, mahiyeti gereği hangi gizlilik seviyesini gerektirdiği, verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.
- Risklerin belirlenmesi ve önceliğinin saptanmasından sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.

**2- Çalışanlara eğitimler verilmeli ve kişisel veri güvenliği konusunda farkındalıklarının yaratılmasına yönelik çalışmalar yapılmalıdır:**

- Kişisel verilerin güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin saldırılar bakımından çalışanların sınırlı da olsa ilk müdahaleyi yapabilecek ölçüde bilgi sahibi olmaları önem taşımaktadır. Bu nedenle çalışanlara kişisel veri ve veri güvenliği konusunda eğitim verilmesi gerekmektedir.
- Diğer taraftan kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında çalışanların eğitim almaları, farkındalıklarının geliştirilmesi ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından önemlidir.
- Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır.

ARŞİV KİTLİK BÜROSU

- Çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik anlaşmalarını imzalamaları istenebilir. Çalışanların güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci de mutlaka olmalıdır.
- Kişisel veri güvenliğine ilişkin politika ve prosedürlerde önemli değişikliklerin meydana gelmesi halinde; yapılacak yeni eğitimlerle bu değişikliklerin, çalışanların bilgisine sunulması ve kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerinin güncel tutulması sağlanmalıdır.

**3- Kişisel Veri Güvenliği Politikaları ve Prosedürleri Belirlenmelidir:**

- Veri güvenliğine yönelik risklerin belirlenebilmesi ve istikrarlı bir şekilde önlem alınabilmesi için kişisel veri güvenliğine yönelik bir politika hazırlanması gerekmektedir.
- Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılmalı, yapılan kontroller belgelenmeli, geliştirilmesi gereken hususlar belirlenmeli ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmelidir. Ayrıca, politika ve prosedürler ile her kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmelidir.

**4- Kişisel veriler mümkün olduğunca azaltılmalıdır:**

- Kişisel veriler doğru ve güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidirler.
- Uzun süredir faaliyet gösteren veri sorumluları tarafından toplanan kişisel verilerin bir kısmı zamanla doğru olmayan, güncelliğini yitirmiş ve herhangi bir amaca hizmet etmeyen veriler haline gelebilmektedir. Bunun önüne geçebilmek için, veri sorumlularınca işleme amaçları bakımından anılan kişisel verilere hala ihtiyaç olup olmadığının değerlendirilmesi ve kişisel verilerin doğru yerde muhafaza edildiğinden emin olunması gerekmektedir.
- Sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi tavsiye edilmektedir. İhtiyaç duyulmayan kişisel verilerin ise "Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliği"ne uygun ve güvenli bir şekilde imha edilmesi gerekmektedir.

**5- Veri İşleyenler ile ilişkiler planlı yürütülmelidir:**

- Bilgi teknolojileri ihtiyaçlarının karşılanması için veri işleyenlerden hizmet alınması durumunda, veri işleyen tarafından gerekli güvenlik seviyesinin sağlandığından emin olunmalıdır. Veri işleyen kişiler, en az veri sorumluları tarafından alınan güvenlik seviyesini sağlamalı ve bu durum veri sorumlusu tarafından kontrol edilmelidir.
- Veri işleyen ile veri sorumlusu arasında düzenlenecek olan sözleşmeye ilişkin dikkat edilmesi gereken hususlar şu şekilde sıralanabilecektir:
  - Veri sorumlusu ile veri işleyen arasında yazılı bir sözleşme olmalıdır.
  - Sözleşmede, veri işleyenin veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilecek veri işleme amaç ve kapsamına göre hareket edeceğine ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde davranılacağına ilişkin hükümler yer almalıdır.

ARI AVUKATLIK BÜROSU

- Veri işleyen, sözleşme ile Kişisel Veri Saklama ve İmha Politikasına uygun davranacağını taahhüt etmelidir.
- Veri işleyenin işlediği kişisel veriler bakımından süresiz sır saklama yükümlülüğüne tabi olacağı sözleşmede yer almalıdır.
- Herhangi bir veri ihlali olması halinde, veri işleyenin bu durumu derhal veri sorumlusuna bildireceği veri işleyenin yükümlülüğü olarak sözleşme de yer almalıdır.
- Sözleşmede, veri sorumlusu tarafından veri işleyene aktarılan kişisel veri kategori ve türlerinin de ayrı bir maddede belirtilmiş olması, veri işleyenin veri güvenliğini sağlama yükümlülüğünü yerine getirmesi açısından faydalı olacaktır.

## 2. TEKNİK TEDBİRLER

Rehber'in ikinci bölümünde veri güvenliğine ilişkin teknik tedbirler yer almaktadır. Siber güvenliğin sağlanması, kişisel veri güvenliğinin takibi, kişisel veri içeren ortamların güvenliğinin sağlanması, kişisel verilerin bulutta depolanması, bilgi teknolojileri sistemleri tedariği, geliştirme ve bakımı, kişisel verilerin yedeklenmesi kapsamında yetki matrisi, yetki kontrol, erişim logları, kullanıcı hesap yönetimi, ağ güvenliği, uygulama güvenliği, şifreleme, sızma testi, saldırı tespit ve önleme sistemleri, log kayıtları, veri maskeleme, veri kaybı, önleme yazılımları, yedekleme güvenlik duvarları, güncel anti-virüs sistemleri, silme, yok etme veya anonim hale getirme, anahtar yöntemi alınabilecek teknik tedbirlerdendir. Rehber'de belirtilen bu tedbirler alınması zorunlu tedbirler olmayıp Kanun'un uygulanmasında yol göstermek amacıyla örnek vermek suretiyle sayılmıştır.

Alınabilecek teknik tedbirlerden bazıları aşağıda detaylı şekilde açıklanmış olup, diğer teknik tedbirlere ilişkin ayrıntılı bilgiye http://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf adresinden ulaşılabilecektir.

### 1- Siber Güvenliğin Sağlanması:

- Güvenlik duvarı ve ağ geçidi oluşturulmalıdır.
- Bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıklarının bulunması sebebiyle kullanılmayan yazılım ve servislerin cihazlardan kaldırılması öncelikle tercih edilebilecek bir yöntem olabilecektir.
- Yazılım ve donanımlar güncel tutulmalı, düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi gerekmektedir.
- Kişisel veri içeren sistemlere erişimin de sınırlı olması gerekmektedir. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalı ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmalıdır.
- Erişim yetki ve kontrol matrisi oluşturulmalı ve ayrı bir erişim politika ve prosedürleri oluşturarak veri sorumlusu organizasyonu içinde bu politika ve prosedürlerin uygulamaya alınması önerilmektedir.
- Güçlü şifre ve parola kullanımının yanı sıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişikleri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da

ARAVUKATLIK BÜROSU

girişlerin kapatılması gibi yöntemlerle erişimin sınırlandırılması gerekmektedir.

- Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır.
- Veri sorumluları tarafından, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi de kişisel veri güvenliğinin sağlanması için önemlidir.

**2- Kişisel Veri Güvenliğinin Takibi:**

- Veri sorumlusu sistemlerinin hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalması halinde bu durumun kısa süre içerisinde fark edilebilmesi ve müdahale edilebilmesi için;

  a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,

  b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,

  c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),

  ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,

  d) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması, gerekmektedir.
- Güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zafiyetlere karşı korunması için düzenli olarak zafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir.

**3- Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması:**

- Kişisel veriler, veri sorumlularının yerleşkelerinde yer alan cihazlarda ya da kâğıt ortamında saklanıyor ise, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması gerekmektedir. Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınması önemlidir.
- Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılması veya bileşenlerin ayrılması sağlanabilecektir.
- Veri sorumlusunun yerleşkesi dışında kalan ve veri sorumlusunun sorumluluğunda bulunan kişisel veriler için de aynı önlemlerin alınması gerekmektedir.
- Elektronik posta ya da posta ile aktarılacak kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmesi gerekmektedir. Ayrıca çalışanların şahsi elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bunlar için de yeterli güvenlik tedbirleri alınmalıdır.
- Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kâğıt ortamındaki evraklar, sunucular, yedekleme cihazları,

ARŞİVLİK BÜROSU

CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler de alınmalıdır.

- Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı şifreleme yöntemleri kullanılmalı ve şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanarak, yetkisiz erişim önlenmelidir. Benzer şekilde, kişisel veri içeren kâğıt ortamındaki evraklar da kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmalı, söz konusu evraklara yetkisiz erişim önlenmelidir.

**4- Kişisel Verilerin Bulutta Depolanması:**

- Bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin yeterli ve uygun olup olmadığı veri sorumlusunca değerlendirilmelidir.
- Bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması gerekmektedir.
- Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyalarının da yok edilmesi gerekir.

**3. SONUÇ**

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun hayatımıza girmesi birçok önemli değişikliği beraberinde getirmektedir. Kanun'u uygulayacak olan Kurul'un çalışmaya başlaması ile birlikte, uygulamaya dair çıkarılan yönetmelik ve kılavuzlar veri sorumlusu olarak kabul edilen şirketlerin kişisel verilerin korunmasına adına almaları gerekli tedbirleri ortaya çıkarmaktadır. Şirketlere yönelik idari para cezalarının yanı sıra bireylere yönelik hapis cezaları da öngörmesi nedeniyle veri güvenliğine uyumun gerek şirketler gerekse kişiler için son derece önemli olduğu ve bu nedenle konuya hassasiyet gösterilmesi gerektiği açıktır.

*Arı Avukatlık Bürosu*

ARI AVUKATLIK BÜROSU

ARI Avukatlık Bürosu

Atatürk Mah. Ataşehir Bul.
42 Ada Gardenya 7/1 Blok Kat:11 No:68
34758 Ataşehir/İSTANBUL
Tel/Faks: +90 (216) 455 09 81/455 46 05
e-posta: info@ari.av.tr
Url: www.ari.av.tr