Building a better working world

Kuzey YMM ve Bağımsız Denetim A.Ş.
Eski Büyükdere Cad.
Orjin Maslak No:27
Maslak, Sarıyer 34398
İstanbul - Turkey

Tel: +90 212 315 3000
Fax: +90 212 234 1067
ey.com
Ticaret Sicil No : 479919
Mersis No: 0-6010-2772-0400010

Avrupa Birliği Genel Veri Koruma Yönergesi ve Türkiye'de Kişisel Verilerin Korunması Kanunu karşılaştırması

Ceylan Necipoğlu

1. Giriş

Kişisel verilerin korunması ile bireylerin verileri üzerinde daha iyi kontrol sağlaması ve Avrupa Birliği genelinde yüksek düzeyde veri koruması oluşturmayı amaçlayan Avrupa Birliği ('AB') Genel Veri Koruma Yönetmeliği (General Data Protection Regulation-GDPR) uzun süren çalışmalar sonucunda ve 95/46/EC sayılı AB Veri Koruma Direktifini yürürlükten kaldırarak Avrupa Parlamentosu tarafından kabul edilmiştir. 1995 yılında yayınlanan eski çerçeve 95/46/EC sayılı Yönerge, internet henüz emeklemeye başladığında yürürlüğe konulmuş iken getirilen yeni regülasyon; sosyal medya, internet bankacılığı, global transferler ve akıllı telefonların dijitalleştirdiği yeni dünyada vatandaşların kendi verileri üzerinde kontrolünü artırıyor. Bu regülasyon sonrasında Avrupalı vatandaşların verilerini işleyen firmaların yeni düzenlemedeki kurallar çerçevesinde hazırlıklara başlaması gerekmekte olup kişisel veri kanunu olan ülkeler kanunlarını 2 yıl içinde yeni düzenlemeye uydurmalı, ilgili kanunları olmayanlar ise bu düzenlemeye uygun bir kanun çıkarmalıdırlar.

2. 6698 sayılı Kişisel Verilerin Korunması Kanunu

Kişisel verilerin korunması, gerçek kişilere ait olan ve onların belirlenebilir olmasını sağlayan kişiye özgü ve özel bilgilerin hukuki anlamda koruma altına alınmasını ifade eder. Kişisel veri ise kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olup, kişinin "adı, soyadı, doğum tarihi ve doğum yeri, telefon numarası, motorlu taşıt plakası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri" gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri olarak kabul edilmektedir.

Kişisel verilerin işlenmesi

Kişisel verilerin işlenmesi, kişisel verilerin tamamen veya kısmen otomatik olan ya da olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olup bu işlemlerin gerçekleştirilebilmesi için uyulması gereken temel ilkeler Kanun'da gösterilmiştir. Kanun'a göre, sayılan temel ilkelere uygun olmak şartıyla kişisel veriler kural olarak ancak ilgili kişinin açık rızası olması koşuluyla işlenebilecektir. Bununla birlikte Kanun'da sayılan istisnalardan birinin varlığı halinde açık rıza olmaksızın da kişisel verilerin işlenmesi mümkün olabilecektir.

Veri sorumlusu ve veri işleyen

Kanun'da veri sorumlusu ve veri işleyen olarak birbirinden ayrı kavramlara yer verilmiştir. Veri sorumlusu veri kayıt sisteminin bir birim, kurum ya da temsilci bünyesinde kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanırken veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmıştır.

Kişisel verilerin yetkisiz kişilerin eline geçmesi durumunda sorumlunun belirlenmesi amacıyla veri sorumlusu ve veri işleyen arasındaki ayrımın doğru şekilde yapılması gerekecektir. Kanunda öngörülen idari para cezalarının ve ilgili kişinin dava edeceği muhatabının belirlenmesi ancak bu ayrım sayesinde mümkün olabilecektir.

3. GDPR ile getirilen yenilikler

Veri Koruma Memuru

Yeni hukuki düzenleme uyarınca Veri Koruma Memuru ('VKM') pek çok organizasyon için GDPR hükümlerine uyum sürecinin merkezinde yer almaktadır. GDPR hükümleri uyarınca veri sorumluları ve veri işleyenler için bir VKM belirlenmesi zorunlu hâle gelmiştir. VKM'nin temel görevleri; tabiatları, kapsamları ve amaçları gereği veri sahiplerinin düzenli ve sistematik gözlemini gerektiren veri işleme operasyonlarının yürütülmesi veya büyük çapta özel nitelikli verilerin cezai yaptırım ve suçlamalarla ilgili kişisel verilerin işlenmesi şeklinde belirlenmiştir.

Denetimler

Veri işleyen, veri sorumlusu tarafından veya veri sorumlusu tarafından yetkilendirilmiş başka bir denetçi tarafından yürütülen soruşturmalarda, teftişlere katkıda bulunma yükümlülüğü altındadır. VKM, ilgili denetimler dâhil olmak üzere, GDPR, diğer AB veya üye devlet veri koruma şartları ve veri sorumlusu veya veri işleyenin kişisel verilerin korunmasına dair politikalarıyla uyumunu takip etme yükümlülüğü altındadır.

Veri koruma etki değerlendirmesi

Veri sorumlusu, veri işleme biçiminin gerçek kişilerin hak ve özgürlükleri açısından yüksek risk teşkil eden hâllerde bir etki değerlendirmesi yürütmelidir. Bunlara örnek olarak; gerçek kişilerle ilgili kişisel yönlerin, fişleme de dâhil olmak üzere otomatikleştirilmiş işlemeye dayalı olarak sistematik ve yaygın bir değerlendirmeye tâbi tutulması, büyük çapta özel nitelikli kişisel veri veya cezai hüküm ve suçlamalar hakkında işleme yapılması, halka açık bir alanın sistematik şekilde ve büyük çapta gözlemlenmesi verilebilir. Veri sorumlusu, mahremiyet/gizlilik etki değerlendirmesi yürütmek için VKM'nin görüşünü almalıdır. Değerlendirme en azından öngörülen işleme faaliyetlerinin sistematik bir tarifini ve veri sorumlusunun meşru menfaatleri de dâhil olmak üzere işlemenin amaçlarını, amaçlar doğrultusunda işleme faaliyetlerinin gerekliliğinin ve ölçülülüğünün değerlendirmesini, veri sahiplerinin hak ve özgürlerine karşı riskleri ve güvenceler, güvenlik tedbirleri ve kişisel verilerin korunmasını temin edecek diğer mekanizmalar da dâhil, risklerin bertaraf edilmesi ve veri sahiplerinin ve diğer kişilerin haklarını meşru menfaatlerini göz önünde tutarak GDPR ile uyumluluğun sağlanması için gerekli tedbirleri içermelidir.

Önceden istişare

Koruma etki değerlendirmesi ile işlemenin, veri sorumlusu tarafından riskin azaltılması için alınması gereken tedbirlerin yokluğunda yüksek risk yaratacağının anlaşıldığı durumlarda veri sorumlusu denetim kuruluna önceden danışmalıdır.

Çerez kullanımı

GDPR altında çerez kullanımına dair herhangi bir özel şart bulunmamaktadır. Yine de, GDPR'nin 30. beyan maddesinde çerez belirleyicilerin, bilhassa münhasır belirleyicilerle ve sunuculardan alınan bilgilerle birleştirildiğinde, gerçek kişilerin profilini oluşturmada ve kimliklerini belirlemede kullanmak için izler bırakabileceğine dikkat çekilmektedir.

Rehber Denetleme Kurulu

Rehber Denetleme Kurulu (RDK), özetle sınır ötesi veri işleme faaliyetlerin idaresinde birinci sorumluluğa sahip yetkili merci olarak tanımlanabilir ve GDPR'nin devletlerarası uygulamada işbirliği ve tutarlılık hedeflerinin gerçekleştirilmesi için oluşturulmuş bir kurumdur. RDK iki kilit kavramdan oluşmaktadır: "Sınır ötesi veri işleme" ve "Ciddi etki".

Dosyalama gereklilikleri

Her bir veri sorumlusu, sorumluluğu altındaki işleme faaliyetlerinin bir kaydını tutmak zorundadır. Kayıtlar; sorumlunun ismi ve iletişim detayları ve varsa birlikte sorumlu, veri sorumlusunun temsilcisi ve VKM, işlemenin amacı, veri sahibi kategorilerinin ve kişisel verilerin tarifi, üçüncü ülkeler de dâhil olmak üzere kişisel verilerin ifşa edildiği alıcıların kategorileri, var ise üçüncü bir ülkeye yapılan kişisel veri aktarımları, mümkün ise farklı kategorilerden verilerin silinmesi için öngörülen zaman sınırları ve teknik ve organizasyonel güvenlik tedbirlerinin genel bir tarifidir.

4. GDPR ve KVKK karşılaştırması

6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun (KVKK) ile büyük oranda Avrupa Birliği müktesebatı ile uyumlu şekilde kişisel verilerin korunması olgusu Türk mevzuatında da ihdas edilmiş ise de AB müktesebatı ile bazı farklılıkları bulunmaktadır.

Uygulanabilirlik kapsamı

GDPR, AB içerisinde yer alan veri sorumlularının veya veri işleyenlerin kuruluşları tarafından yürütülen tüm işleme faaliyetlerine, işleme faaliyeti AB içerisinde yer almayan veri sorumlusu veya veri işleyici kuruluşları tarafından yürütülüyor ise işleme faaliyetlerinin AB içerisinde yer alan veri sahiplerine mal veya hizmet sunumuyla ilgili olması halinde veya işleme faaliyetlerinin AB içerisinde yer alan veri sahiplerinin hareketlerini,

hareketlerin AB içerisinde bulunması kaydıyla, gözlemlemeye yönelik olması halinde uygulanır. KVKK ise kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanmaktadır.

İlgili kişinin hakları

GDPR çerçevesinde ilgili kişinin hakları erişim hakkı, düzeltme hakkı, unutulma hakkı, işlemenin kısıtlanması hakkı, itiraz etme hakkı ve veri taşınabilirliği hakkı olarak sayılmış iken, KVKK'da sayılan haklar; kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, Kanun'da sayılan kişisel verilerin işlenmesini gerektiren sebeplerinin ortadan kalkması halinde kişisel verilerin silinmesini veya yok edilmesini isteme, kişisel verilerin silinmesinin veya yok edilmesinin talep edilmesi halinde yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme şeklindedir.

İdari para cezaları

GDPR, kişisel verilerin işlenmesi sırasında düzenleme ihlâl edilirse veri konusunun düzenleyici kuruma şikâyette bulunma hakkı olmalıdır. İhlalin çeşidine bağlı olarak, GDPR şu maddi yaptırımları uygulayacaktır:

10.000.000 Avro'ya kadar (veya küresel cironun % 2'si): Bu yaptırım; çocuğun rızasının alındığı durumlarda buna uyulmaması, veri koruma ilkelerinin uygulanmaması, veri denetleyicisi adına hareket eden veri işleyicisinin işleme sürecinde koşulların uygulanmaması, işlenen verilerin kayıtlarını tutma yükümlülüğünün uygulanmaması, kuruma itaatsizlik, güvenlik önlemlerine uyulmaması, kuruma bildirim eksikliği ve veri sahibinin ihlali, veri koruma memurunun atanmaması ve benzeri durumlarda uygulanır.

20.000.000 Avro'ya kadar (veya küresel cironun %4'si): Bu yaptırım; işleme operasyonlarına hakim ilkelere uyulmaması, kanuna aykırı işleme, veri sahibinin haklarına ihlal, AB dışındaki transferlerin gerekliliklerine uymama durumlarında uygulanır.

İdari para cezalarına karar verilirken ve cezanın miktarı belirlenirken ihlâlin özellikleri (tabiatı, büyüklüğü, süresi, veri sorumlusu tarafından alınan aksiyonlar vs.), veri işleme faaliyetinin özellikleri ve diğer ağırlaştırıcı ve hafifletici etkenler başta olmak üzere birçok etken hesaba katılmalıdır.

KVKK, aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar, veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar, kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar, Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para verileceğini düzenlemiştir.

Suçlar ve hapis cezaları ise; kişisel verilerin hukuka aykırı olarak kaydedilmesi halinde 1 yıldan 3 yıla kadar, özel nitelikli kişisel verilerin hukuka aykırı olarak kaydedilmesi halinde 1,5 yıldan 4 yıla kadar, kişisel verileri hukuka aykırı olarak verme veya geçirme halinde 2 yıldan 4 yıla kadar, kişisel verileri yok etmeme halinde 1 yıldan 2 yıla kadar şeklinde düzenlenmiştir.

5. Sonuç

Avrupa'daki sürece baktığımızda; 1981'de bilgisayarlar ile yapılan işlem sayısı artınca Kişisel Veriler Sözleşmesi hazırlandı, 1995'te internetin yayılmaya başlaması ile birlikte bir çerçeve hazırlandı ve 2016'da sosyal medyanın gelişmesi etkisi ile GDPR yürürlüğe konulmuş oldu. 1995 bir çerçeveydi ve ülkeler kendi düzenlemelerini bu çerçeve içinde istedikleri gibi hazırlıyorlardı ancak 2016 uyulması gereken bir düzenleme ve ülkelerin buna uyma zorunluluğu bulunmaktadır. 7 Nisan 2016'da yürürlüğe giren KVKK ise 1995 çerçevesine uygun hazırlanmış olsa da, bu Kanun'un yasalaşması ile AB Uyum Kriterleri normlarından biri gerçekleşmiş olup, AB üyeliği yolunda bir adım olarak görülmektedir.