Avrupa Birliği ‘Genel Veri Koruma Yönetmeliği’nin Temel Esasları

1. Genel Veri Koruma Yönetmeliği: giriş

Genel Veri Koruma Yönetmeliği (General Data Protection Regulation-GDPR), dünyadaki en katı gizlilik ve güvenlik düzenlemesidir. Bu Yönetmelik, Avrupa Birliği (AB) tarafından hazırlanmış ve kabul edilmiş olmasına rağmen, AB’deki insanları hedefledikleri veya bunlarla ilgili verileri topladıkları sürece her yerde kuruluşlara yükümlülükler getirmektedir. Anılan Yönetmelik, 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. GDPR, gizlilik ve güvenlik standartlarını ihlal edenlere on milyonlarca avroya varan ağır para cezaları uygulayacaktır.

GDPR ile Avrupa, daha fazla insanın kişisel verilerini bulut hizmetlerine emanet ettiği ve ihlallerin günlük olarak gerçekleştiği bir zamanda veri gizliliği ve güvenliği konusundaki kararlı duruşunun sinyallerini vermektedir. Düzenlemenin kendisi büyük, geniş kapsamlı ve ayrıntılara oldukça açık olduğundan, GDPR uyumluluğunu özellikle küçük ve orta ölçekli işletmeler (KOBİ; small and medium-sized enterprises-SMEs) için göz korkutucu bir olasılık haline getirmektedir.

Özel hayatın gizliliği hakkı, esasen 1950 tarihli Avrupa İnsan Hakları Sözleşmesi’nin (European Convention on Human Rights) bir parçası olup, *“Herkesin özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkı vardır.”* AB bu temelden hareketle bu hakkın korunmasını mevzuat yoluyla sağlamaya çalışmıştır.

Teknoloji ilerledikçe ve İnternet icat edildiğinde, AB modern korumalara olan ihtiyacı fark etmiştir. Böylece 1995 yılında, her üye devletin kendi uygulama yasasını temel aldığı minimum veri gizliliği ve güvenlik standartlarını belirleyen Avrupa Veri Koruma Direktifini (European Data Protection Directive) çıkarmıştır. Ancak İnternet, bugün olduğu gibi Hoover verilerine dönüşmeye başlamış ve 1994 yılında ilk simge reklam (banner ad) çevrimiçi olarak yayınlanmıştır. 2000 yılında, finansal kurumların çoğu çevrimiçi bankacılık hizmetini sunmuş, 2006 yılında da Facebook halka açılmıştır. 2011’de bir Google kullanıcısı, elektronik postalarını (e-posta) taradığı için şirkete dava açmıştır. Bundan iki ay sonra, Avrupa’nın veri koruma makamı, AB’nin *“kişisel verilerin korunması konusunda kapsamlı bir yaklaşıma”* ihtiyacı olduğunu ilan etmiş ve 1995 tarihli direktifi güncelleme çalışmaları başlamıştır.

GDPR, Avrupa Parlamentosu’ndan geçtikten sonra 2016 yılında yürürlüğe girdi ve 25 Mayıs 2018 tarihi itibarıyla tüm kuruluşların uyumlu olması zorunlu oldu.

2. GDPR: kapsam, cezalar ve temel tanımlar

İlk olarak, AB vatandaşları veya sakinlerinin kişisel verileri işlendiğinde veya bu kişilere mal veya hizmet sunulduğunda, AB'de olunmasa bile GDPR hükümleri geçerlidir.

İkincisi, GDPR'yi ihlal etmenin cezaları çok yüksektir. En fazla 20 milyon avro veya küresel gelirin %4'ü (hangisi daha yüksekse) olan iki aşamalı ceza vardır, ayrıca veri özneleri zararlar için tazminat talep etme hakkına sahiptir.

GDPR, bir dizi yasal kavramı uzun uzadıya tanımlamaktadır. Aşağıda en önemli olanlardan bazıları verilmiştir:

- **Kişisel veriler (Personal data):** Kişisel veriler, kimliği doğrudan veya dolaylı olarak belirlenebilen bir kişiyle ilgili her türlü bilgidir. İsimler ve e-posta adresleri açıkça kişisel verilerdir. Konum bilgileri, etnik köken, cinsiyet, biyometrik veriler, dini inançlar, web çerezleri ve siyasi görüşler de kişisel veriler olabilir. Birinin kimliğini belirlemek nispeten kolaysa, takma adlı veriler de tanımın kapsamına girebilir.
- **Veri işleme (Data processing):** Otomatik veya manuel olsun, veriler üzerinde gerçekleştirilen herhangi bir işlemdir. Metinde belirtilen örnekler arasında toplama, kaydetme, düzenleme, yapılandırma, depolama, kullanma, silme… yani temelde her şey sayılabilir.
- **Veri konusu (Data subject):** Verileri işlenen kişidir. Bunlar müşteriler veya site ziyaretçileridir.
- **Veri denetleyicisi (Data controller):** Kişisel verilerin neden ve nasıl işleneceğine karar veren kişidir. Kuruluşta verileri işleyen bir şirket sahibi veya çalışanıdır.
- **Veri işlemcisi (Data processor):** Bir veri denetleyicisi adına kişisel verileri işleyen üçüncü taraftır. GDPR'nin bu kişi ve kuruluşlar için özel kuralları vardır. Tresorit gibi bulut sunucularını veya Proton Mail gibi e-posta servis sağlayıcılarını içerebilirler.

3. Veri koruma ilkeleri

Veriler işleniyorsa, bunun Madde 5.1-2'de belirtilen yedi koruma ve hesap verebilirlik ilkesine göre yapılması gerekir:

1. **Yasallık, adalet ve şeffaflık (lawfulness, fairness and transparency):** İşleme, veri sahibi için yasal, adil ve şeffaf olmalıdır.
2. **Amaç sınırlaması (purpose limitation):** Veriler toplandığında veri sahibine açıkça belirtilen meşru amaçlar için işlenmelidir.
3. **Asgari veri (data minimization):** Belirtilen amaçlar için yalnızca kesinlikle gerekli olduğu kadar veri toplanmalı ve işlenmelidir.
4. **Doğruluk (accuracy):** Kişisel veriler doğru ve güncel tutulmalıdır.

5. **Depolama sınırlaması (storage limitation):** Kişisel tanımlayıcı verileri yalnızca belirtilen amaç için gerekli olduğu sürece saklanabilmelidir.
6. **Bütünlük ve gizlilik (integrity and confidentiality):** İşleme, uygun güvenlik, bütünlük ve gizliliği sağlayacak şekilde yapılmalıdır (örneğin şifreleme kullanılarak).
7. **Hesap verebilirlik (accountability):** Veri denetleyicisi, GDPR'nin tüm bu ilkelere uygunluğunu gösterebilmekten sorumludur.

4. Hesap verebilirlik

GDPR, veri denetleyicilerinin GDPR uyumlu olduklarını kanıtlayabilmeleri gerektiğini söylemektedir. Bu, gerçeklerden sonra yapılabilecek bir şey değildir: GDPR ile uyumlu olduğu düşünülüyor ancak nasıl olduğu gösterilemiyorsa, o zaman GDPR uyumlu değildir. Bunu yapmanın yolları arasında:

- Ekibe veri koruma sorumluluklarının belirlenmesi.
- Toplanılan verilere, nasıl kullanıldığına, nerede saklandığına, hangi çalışanın bundan sorumlu olduğuna vb. ilişkin ayrıntılı belgelerin saklanması.
- Personelin eğitilmesi ve teknik ve organizasyonel güvenlik önlemlerinin uygulanması.
- Verileri işlemek üzere sözleşme yapılan üçüncü taraflarla Veri İşleme sözleşmeleri imzalanması.

5. Veri güvenliği

"Uygun teknik ve organizasyonel önlemleri" uygulayarak verilerin güvenli bir şekilde işlenmesi gerekir. Teknik önlemler, çalışanların kişisel verilerin depolandığı hesaplarda iki faktörlü kimlik doğrulama (two-factor authentication) kullanmasını zorunlu kılmaktan uçtan uca şifreleme (end-to-end encryption) kullanan bulut sağlayıcılarıyla yapılan sözleşmelere kadar her şeyi ifade eder. Kurumsal önlemler, personel eğitimleri, çalışan el kitabına bir veri gizliliği politikası eklemek veya kişisel verilere erişimi yalnızca kuruluşta buna ihtiyacı olan çalışanlarla sınırlamak gibi şeylerdir. Bir veri ihlali varsa, veri sahiplerine bildirmek veya ceza almak için 72 saat vardır. (Verileri bir saldırgan için kullanışsız hale getirmek için şifreleme gibi teknolojik güvenlik önlemleri kullanılırsa, bu bildirim yükümlülüğünden feragat edilebilir.)

6. Tasarım ve varsayılan olarak veri koruması

Bir kuruluşta yapılan her şey, "tasarım gereği ve varsayılan olarak" (by design and by default) veri korumayı dikkate almalıdır. Pratik olarak bu, herhangi bir yeni ürün veya faaliyetin tasarımında veri koruma ilkelerini göz önünde bulundurmanız gerektiği anlamına gelir. GDPR, bu ilkeyi Madde 25'te

kapsamaktadır. Örneğin, bir şirket için yeni bir uygulama başlatıldığını varsayalım. Uygulamanın kullanıcılardan hangi kişisel verileri toplayabileceğinin düşünülmesi, ardından veri miktarını en aza indirmenin yollarının ve bunların en son teknolojiyle nasıl güvence altına alınacağının düşünülmesi gerekir.

7. Verileri işlemeye izin verilmesi

GDPR madde 6, kişi verilerinin işlenmesinin yasal olduğu durumları listelemektedir. Aşağıdakilerden biriyle haklı çıkarılmadığı sürece, birinin kişisel verilerine dokunmak dahi düşünülmemelidir (toplanmamalı, saklanmamalı, reklamcılara satılmamalı):

1. Veri sahibi, verileri işlemek için ***özel ve net bir onay*** (***açık rıza***; unambiguous consent) vermiştir (Örneğin, pazarlama e-posta listesine kayıt olundu).
2. Veri sahibinin taraf olduğu ***bir sözleşmeyi akdetmeye*** (to enter into a contract) ***hazırlanmak*** için işleme gereklidir. (Örneğin, mülkü müstakbel bir kiracıya kiralamadan önce bir geçmiş kontrolünün yapılması gerekir).
3. ***Yasal bir yükümlülüğe uymak*** (to comply with a legal obligation) için işlenmesi gerekir (Örneğin, ülkedeki mahkemeden bir emir alınırsa).
4. ***Birinin hayatının kurtarılması*** (to save somebody's life) için verilerin işlenmesi gerekir (Örneğin, bunun ne zaman geçerli olduğu muhtemelen bilinir).
5. ***Kamu yararına bir görevi yerine getirmek*** (to perform a task in the public interest) veya bazı resmi işlevleri yerine getirmek için işleme gereklidir. (Örneğin özel bir çöp toplama şirketiyse).
6. Birinin kişisel verilerini işlemek için ***meşru/yasal bir menfaatin*** (legitimate interest) var olması gerekir. Bu, en esnek yasal dayanaktır, ancak "veri sahibinin temel hak ve özgürlükleri", özellikle bir çocuğun verileriyse, her zaman çıkarları geçersiz kılar (Burada bir örnek vermek zordur, çünkü dava için göz önünde bulundurulması gereken çeşitli faktörler vardır.).

Veri işlemenin yasal dayanağı belirlendikten sonra, bu temelin belgelenmesi ve veri sahibinin bilgilendirilmesi gerekir (şeffaflık/transparency). Daha sonra gerekçe değiştirilmeye karar verilirse, iyi bir nedenin olması, bu nedenin belgelenmesi ve ilgili kişiye bildirilmesi şarttır.

8. Razı olmak (consent)

Bir veri sahibinin bilgilerini işlemek için rızasını neyin oluşturduğuna dair katı yeni kurallar vardır. Rıza *"özgürce verilmiş, özellikli, bilgilendirilmiş ve açık olmalıdır"* (freely given, specific, informed and unambiguous). Muvafakat talepleri *"diğer hususlardan açıkça ayırt edilebilir"* (clearly distinguishable from the other matters) olmalı ve *"açık ve sade bir dille"* (clear and plain language)

sunulmalıdır. Veri sahipleri, daha önce verdikleri onayı istedikleri zaman geri çekebilir ve onların kararına saygı gösterilmesi gerekir. İşlemenin yasal dayanağı diğer gerekçelerden biriyle değiştirilemez. 13 yaşından küçük çocuklar ancak ebeveynlerinin izniyle onay verebilirler. Belgeli rıza kanıtının saklanması gerekir.

9. Veri koruma görevlileri

Popüler inanışın aksine, her veri denetleyicisinin veya işlemcisinin bir Veri Koruma Görevlisi (Data Protection Officer-DPO) olarak atanması gerekmez. Bir DPO olarak atanmak için üç koşul vardır:

1. Yargı yetkisine sahip bir mahkeme dışında bir kamu makamı olmalıdır.
2. Temel faaliyetler, insanların sistematik ve düzenli olarak büyük ölçekte izlenmesini gerektirmektedir (örneğin Google).
3. Temel faaliyetler, GDPR'nin 9'uncu maddesinde listelenen özel veri kategorilerinin veya Madde 10'da belirtilen cezai hükümler ve suçlar ile ilgili verilerin büyük ölçekli işlenmesi olmalıdır (örneğin, tıbbi bir ofis).

Zorunlu olunmasa bile bir DPO atama da seçilebilir. Bu rolde birinin olmasının faydaları vardır. Temel görevleri, GDPR'yi ve bunun kuruluş için nasıl uygulandığını anlamak, kuruluştaki kişilere sorumlulukları hakkında tavsiyelerde bulunmak, veri koruma eğitimleri yürütmek, denetimler yapmak ve GDPR uyumluluğunu izlemek ve düzenleyicilerle bağlantı kurmaktır.

10. İnsanların gizlilik hakları (People's privacy rights)

Bir veri denetleyicisi ve/veya bir veri işlemcisi, interneti kullanan bir kişi olarak, aynı zamanda bir veri öznesidir. GDPR, bireylere kuruluşlara ödünç verdikleri veriler üzerinde daha fazla kontrol sağlamayı amaçlayan, veri sahipleri için bir dizi yeni gizlilik hakkı tanımaktadır. Bir kuruluş olarak, GDPR'ye uyumlu olduğundan emin olmak için bu hakların anlaşılması önemlidir. Aşağıda, veri konularının gizlilik haklarının bir özeti bulunmaktadır:

- Bilgilendirilme hakkı (right to be informed),
- Erişim hakkı (right of access),
- Düzeltme hakkı (right to rectification),
- Silme hakkı (right to erasure),
- İşlemeyi kısıtlama hakkı (right to restrict processing),
- Veri taşınabilirliği hakkı (right to data portability),
- İtiraz hakkı (right to object),
- Otomatik karar verme ve profil oluşturma ile ilgili haklar (rights in relation to automated decision making and profiling).