
SANS SECURITY AWARENESS

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

# Genel Veri Koruma Yönetmeliği

## Giriş

Genel Veri Koruma Yönetmeliği ya da GDPR (General Data Protection Regulation) olarak adlandırılan yeni yönetmeliği belki duymuşsunuzdur. Bu yönetmelik Avrupa Birliği tarafından oluşturulmuş olup 25 Mayıs 2018'de yürürlüğe girecektir. Bu yönetmelik Avrupa Birliği'nde yerleşmiş olan kişilerin kişisel bilgilerini kullanan her şirket için geçerli olacaktır, bu şirket dünyanın neresinde olursa olsun. GDPR, şirketlerden Avrupa Birliği'nde yerleşmiş olan kişilerin kişisel verilerin güvenliği ve gizliliğini sağlamalarını talep eder. GDPR uyumlu olmak için anahtar prensiplerin anlaşılması ve uygulanması gerekmektedir.

İnsanlar gizlilik hakkına sahiptirler. Şirketler, topladıkları ve işledikleri kişisel verileri sınırlandırarak ve toplanan bu verileri koruyarak bu gizliliğe saygı duymak zorundadırlar. Gizlilik yaptırımları her türlü veri için geçerlidir, tek başına ya da başka veriler ile birlikte kullanılarak Avrupa Birliği'nde yaşayan kişilerin kimliğini tespit etmeyi sağlayan bir veri. Bu veri, adresi passport numarası, ehliyet numarası, finansal detaylar, biyometrik bilgileri, sendika üyelikleri, sağlık bilgileri, lokasyon verisi ya da cinsiyet, din, politik yönelimi gibi veriler olabilir. Bu yönetmelik, yaşayan bir birey olan 'gerçek kişi'lere uygulanır. Takip edilmesi gereken bazı temel ilkeler şunlardır:

**Bireylerin kişisel verileri yasalara uygun, adil ve şeffaf bir şekilde işlenecektir.**

**Bireylere hangi verilerin hangi amaçla toplandığı bilgisi verilecektir.**

**Kişisel veriler belirgin, açık ve yasalara uygun amaçlarla toplanacaktır. Bu veriler, bu amaçlarla çelişen başka bir amaçla kullanılamaz.**

**Kişisel veriler sadece gerektiği sürece tutulacak ve işlenecektir, bu süreden daha uzun tutulmayacaktır.**

**Kişisel veriler güncel ve hatasız bir şekilde saklanmalıdır.**

**Bireyler, saklanan verilerin bir kopyasını alma hakkına sahiptir ya da artık kullanılmayan ya da bazı durumlarda silinmiş olan verileri isteyebilirler.**

**Şirketler, tesadüfi ya da yasadışı tahriplere, kayıplara, değişikliklere veya ifşalara karşı kişisel verilerin korunması için uygun güvenlik önlemleri almalıdır.**

**Ayrıca şirketler, kişisel verileri kullanan tüm çalışanlarının verilerin güvenliğinin sağlanması ve korunması ile ilgili uygun bir şekilde eğitim aldıklarından emin olmalıdır.**

Kişisel verilerin güvenliğini sağlayan koruma önlemleri, verilerin hassaslığına uygun bir koruma seviyesinin sağlandığını garanti altına almalıdır. Veriler çoğaldıkça bununla birlikte gelen riskler arttığından, bu verileri korumak için alınacak önlemler için gereken çaba ve harcamalar da artmalıdır. Bu önlemler, düzenli bir şekilde gözden geçirilmeli ve uygun bir şekilde güncellenmelidir. Gizlilik ve güvenlik öenmleri ile ilgili iyi dokümante edilmiş kayıtlar, gereksinimler ile uyumluluğunuzu göstermenize yardımcı olur. Bununla beraber şirketler, kişisel verilerin Avrupa Birliği içindeki ya da dışındaki üçüncü şahıslara aktarılırken güvenliğini sağlamak için kontratlar ve gerekli özenin gösterildiğine dair alınan inceleme ve tespitler gibi hukuken önlem almak zorundadırlar. Son olarak, kişisel veri ihlali durumlarında, şirketler bunun farkına vardıktan 72 saat içerisinde bu ihlali rapor etmelidirler. Şirketlerin GDPR ile uyumluluğunu sağlayamadıkları takdirde genel hasılatlarının %4'ü kadarı ile cezalandırılacaklardır, ki bu da GDPR'yi dünyadaki finansal olarak en masraflı yönetmeliklerden biri yapar.

## Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

## Konuk Yazar

**Brian Honan**, *Dublin Irlanda'da bağımsız bir siber güvenlik ve veri koruma şirketi olan BH danışmanlığın yönetim kurulu başkanıdır. Brian, Europol Siber Suçlar Merkezinin özel danışmanı olarak görev almaktadır. Irlanda'nın ilk Bilgisayar Acil Mühadale Takımının (Computer Emergency Response Team) kurucusudur. Ayrıca birçok yenilikçi güvenlik şirketinin danışma kurulunda bulunmaktadır. Brian'a* www.linkedin.com/in/brianhonan *ulaşabilirsiniz ya da* @brianhonan *ile Twitter'da takip edebilirsiniz.*

## Kaynaklar

| | |
|---|---|
| Bireyler ve Şirketler için GDPR'ye Giriş: | http://gdprandyou.ie |
| GDPR Düzenlemeleri: | https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679 |
| OUCH! Çevirileri ve Arşivleri: | https://www.sans.org/u/D88 |