Siber Güvenlik Toplantıları:
Stratejik Veriyi Güvende Tutmak

Kişisel Veri İşlemek İçin Alınması Gereken Tedbir ve Önlemler

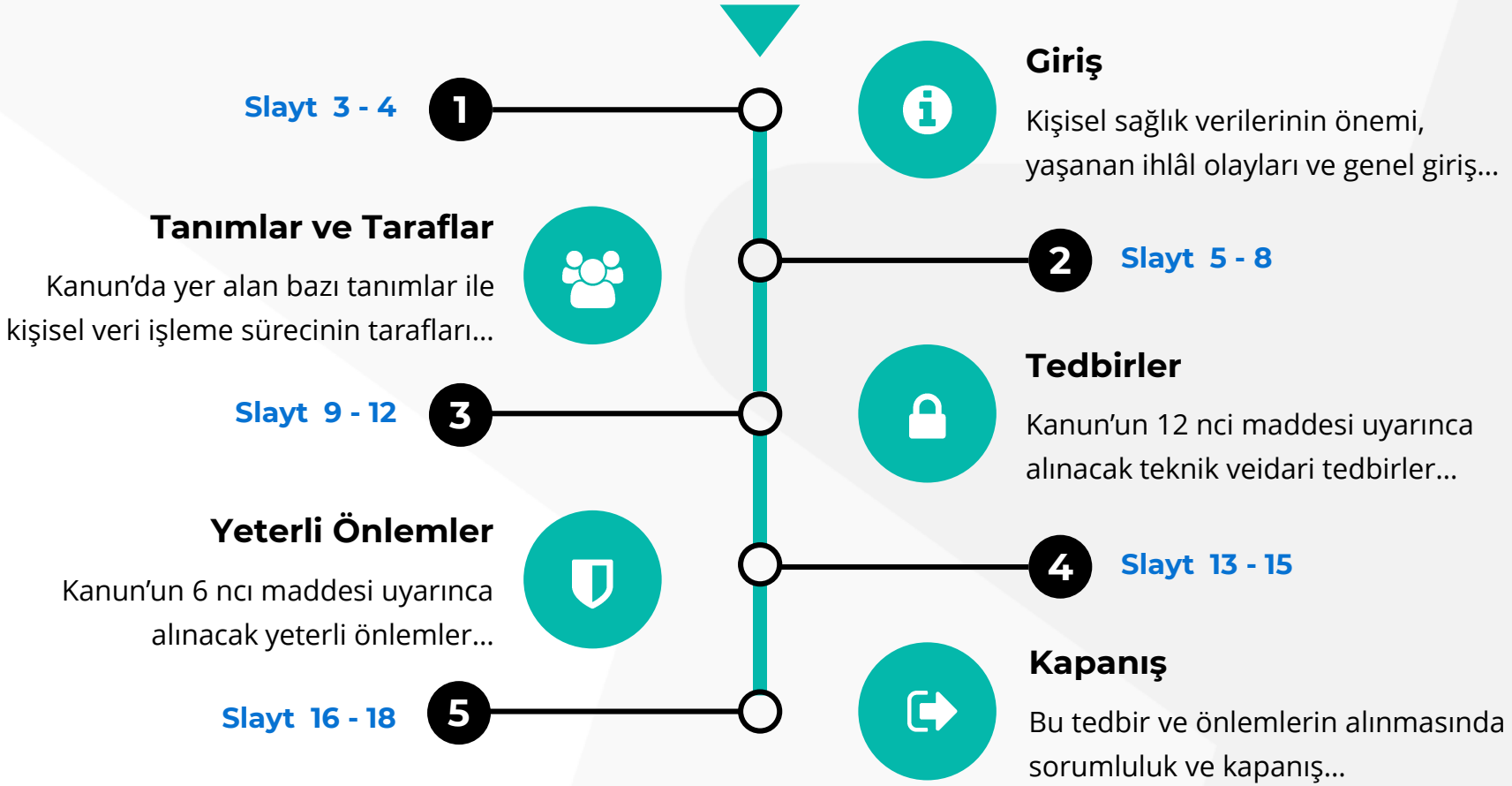
T.C. Sağlık Bakanlığı

Av. Ahmet Esad BERKTAŞ (LL.M)

Bilişim Hukuku Danışmanı
Sağlık Bilgi Sistemleri Genel Müdürlüğü

Sunum Plânı

Sunumda üzerinde durulacak başlıklar



Giriş

Sağlık verilerinin önemi, maliyeti ve önemli ihlâller

Yapılan araştırmalar, siber saldırganların kişisel sağlık verilerini daha fazla hedef aldığını ortaya koymaktadır. Bu verilerin, nitelikleri gereği kara borsada daha yüksek fiyatlara alıcı bulduğu belirtilmektedir.

Kişisel Sağlık Verilerinin İhlâli

Sağlığa ilişkin veriler gereği gibi korunuyor mu?

Siber korsanların sağlık verilerine rağbeti yüksek. (1)

Kişisel sağlık verisi, diğer verilerden daha değerli. (2)

Karaborsada kişisel sağlık verisinin karşılığı fazla. (3)

ABD'de 2012 – 2016 yıllarında milyonlarca ihlâl. (4)

Yalnızca 2018 yılında çok sayıda veri ihlâli oldu. (5)

Büyük tesislerin tamamına yakınında ihlâl oluyor. (6)

İhlâl edilen bu verilerin maliyeti çok büyük. (7)

(1) BakerHostetler: Is Your Organization Compromise Ready? | (2) Reuters: Your medical record is worth more to hackers than your credit card | (3) Aberdeen Group | (4-5) U.S. Department of Health & Human Services - Office for Civil Rights | (6) PwC: Top Health Industry Issues of 2016 | (7) Ponemon Institute: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data & Accenture: The $300 Billion Attack

Tanımlar ve Taraflar

Kişisel veriye ilişkin tanımlar, veri işleme süreci tarafları

Hangi verinin kişisel veri olduğu ve hangi verinin anonim veri olduğuna ilişkin yanlış değerlendirmeler yapılabildiği görülmektedir. Benzer bir karmaşa veri işleme sürecinin taraflarıyla ilgili olarak da yaşanmaktadır, özellikle kişisel veri işleyen herkesin “veri işleyen” olduğu düşünülmektedir.

Tanımlar

Kişisel Verilerin Korunması Kanunu'nda tanımlar

Tanımlar

Madde 3 – Bu Kanunun uygulanmasında:

Kişisel veri: **Kimliği belirli veya belirlenebilir** gerçek kişiye ilişkin her türlü bilgi,

Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi **veriler üzerinde gerçekleştirilen her türlü işlem**,

Anonim hale getirme: Kişisel verilerin, **başka verilerle eşleştirilerek dahi** hiçbir surette kimliği belirli veya belirlenebilir bir **gerçek kişiyle ilişkilendirilemeyecek** hâle getirilmesi,

Kanun’da Veri Tasnifi

Kişisel Verilerin Korunması Kanunu’nda kişisel verilerin tasnifi

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri, özel nitelikli kişisel veridir.

Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgilerdir.

Kanun’da Taraflar

Kişisel Verilerin Korunması Kanunu’nda taraflar

İLGİLİ KİŞİ

Kişisel **verisi işlenen** gerçek kişidir.

VERİ İŞLEYEN

Veri sorumlusunun **verdiği yetki**ye dayanarak **onun adına** kişisel verileri işleyen gerçek veya tüzel kişidir.

VERİ SORUMLUSU

Kişisel **verilerin işleme amaçlarını** ve vasıtalarını **belirleyen**, veri kayıt **sisteminin kurulmasından ve yönetilmesinden sorumlu olan** gerçek veya tüzel kişidir.

Tedbirler

Alınması gereken teknik ve idari tedbirler

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin birinci fıkrasında; kişisel verilerin hukuka aykırı işlenmesi ile bu verilere hukuka aykırı erişilmesini önlemek ve ayrıca verilerin muhafazasını sağlamak amacıyla veri sorumlusuna gerekli teknik ve idari tedbirleri alma yükümlülüğü getirilmiştir. Veri işleme sürecinde "veri isleyen" sıatını haiz bir tarafın varlığı halinde, her iki tarafın müşterek sorumluluğu bulunmaktadır.

Teknik Tedbirler

Kişisel Veri Güvenliği Rehberi'nde yer alan teknik tedbirler

Yetki matrisi

Hangi düzeyde yetkili olan kullanıcının hangi verilere erişebileceği tanımlanmalı.

Yetki kontrol

Verilere erişmek isteyen kullanıcının o yetkiye sahip olup olmadığı kontrol edilmeli.

Erişim logları

Verilere erişen kullanıcıların log kaydı tutulmalı. Bunların zaman damgalı olması gerektiği belirtilmiyor.

Kullanıcı hesap yönetimi

Kullanıcıların hesapları ve yetkileri teknik açıdan iyi kontrol edilebilmeli. İşten ayrılışta hesap kapatılmalı.

Ağ güvenliği

Kullanıcıların kendi aralarındaki kapalı ağın ve internete çıktıkları ağın güvenliği sağlanmalı.

Uygulama güvenliği

Kullanılan uygulamaların güvenliği sağlanmalı, veri ihlâline sebebiyet verebilecek hususlar önlenmeli.

Şifreleme

Sunucularda tutulan kişisel veriler uluslararası kabul gören standartlar kullanılarak şifrelenmeli.

Sızma testi

Makûl aralıklarla periyodik olarak sızma testleri yapılmalı, güvenlik zafiyetleri tespit edilerek kapatılmalı.

Saldırı tespit ve önleme sistemi

Saldırıların hem tespit edilmesi (IDS) hem de önlenmesi (IPS) noktasında gerekli sistemler kullanılmalı.

Teknik Tedbirler

Kişisel Veri Güvenliği Rehberi'nde yer alan teknik tedbirler

Veri maskeleme

Kimliksizleştirme (data masking, de-identification, pseudonymisation vb.) yöntemleri kullanılmalı.

Güvenlik duvarları

Kullanılan ağa dışarıdan yapılabilecek saldırılara karşı gerekli sistemler (Firewall) kurgulanmalı.

Anahtar yönetimi

Şifrelenen verilerin anahtarı, yalnızca yetkili kişilerin erişebileceği ortamlarda saklanılmalı.

Veri kaybı önleme yazılımları

Sisteme izinsiz yapılan müdahale sonucunda veri kaybını önleyecek sistemler (DLP) kullanılmalı.

Güncel antivirus sistemleri

Antivirüs sistemleri kullanılmalı ve bu sistemlerin veritabanları devamlı güncel tutulmalı.

Yedekleme

Kişisel verilerin periyodik olarak yedekleri alınmalı, tüm verilerin kaybına imkân verilmemeli.

Verileri imha etme

İlgili envanter ve politikalar çerçevesinde zamanı gelen veriler imha edilmeli.

İdari Tedbirler

Kişisel Veri Güvenliği Rehberi'nde yer alan idari tedbirler

Kişisel veri işleme envanteri

Sicile (VERBİS) kayıt yükümlülüğü olan veri sorumluları tarafından hazırlanmalı.

Kurumsal politikalar

Kişisel verilere erişim, bilgi güvenliği, verilerin kullanımı, saklanması, imhası gibi politikalar hazırlanmalı.

Sözleşmeler

Veri sorumlusu ile veri sorumlusu arasında veya veri sorumlusu ile veri işleyen arasında sözleşme yapılmalı.

Gizlilik taahhütnameleri

Kişisel verilere erişenlerle gizlilik sözleşmeleri imzalanmalı, amaç dışı kullanım engellenmeli.

Periyodik ve rastgele denetimler

Veri sorumlusu tarafından periyodik ve rastgele denetimler yapılmalı, tespit edilen açıklar giderilmeli.

Risk analizleri

Kişisel veri ihlâline sebep olabilecek riskler analiz edilmeli, riskler için DÖF açılmalı ve takip edilmeli.

Sözleşme revizyonu

Çalışanlara imzalatılan sözleşmeler ve kurum içi düzenlemeler, 6698 s. Kanun kapsamında revize edilmeli.

Kurumsal iletişim

Kriz yönetimi, itibar yönetimi, ihlâl halinde ilgili kişileri ve KVKK'yı bilgilendirme süreçleri belirlenmeli.

Eğitim ve farkındalık

Konuya ilişkin eğitimler düzenlenmeli, farkındalık faaliyetleri gerçekleştirilmeli.

Yeterli Önlemler

Özel nitelikli verilerin niteliği gereği özel önlemler

Veri koruma yasalarında kişisel veri ile özel nitelikli (hassas) kişisel veri ayrımı yapılmasının doğal bir yansıması olarak, KVKK m. 6/4'te de ifade edildiği üzere özel nitelikli kişisel verilerin işlenmesi için alınması gereken bir takım ilave önlemler bulunmaktadır. Bu önlemler, Kişisel Verileri Koruma Kurulu tarafından 2018/10 sayılı Karar ile belirlenmiştir.

Yeterli Önlemler

Kişisel Verileri Koruma Kurulunun 2018/10 sayılı Kararı

Veri işleme sürecinde yer alan çalışanlara yönelik;

- Veri koruma mevzuatına yönelik **eğitim verilmeli**,
- **Gizlilik sözleşmesi** yapılmalı,
- Kullanıcıların **yetki kapsamları ve süreleri** net tanımlanmalı,
- Periyodik olarak **yetki kontrolleri** gerçekleştirilmeli,
- Görev değişikliği/işten ayrılma halinde yetkiler hemen kaldırılmalı, **envanter iade alınmalı**.

Veriler elektronik ortamda işleniyorsa;

- **Kriptografi**k yöntemlerle muhafaza edilmeli,
- **Anahtarlar güvenli ve farklı ortamda** tutulmalı,
- Tüm hareketlerin **güvenli log kayıtları** alınmalı,
- Sunucu ve uygulamalar **düzenli güncellenmeli, güvenlik testi** yapılmalı, kayıtlar tutulmalı,
- Uzaktan erişim varsa **iki kademeli kimlik doğrulama** kullanılmalı,

Yeterli Önlemler

Kişisel Verileri Koruma Kurulunun 2018/10 sayılı Kararı

Veriler fiziksel ortamda işleniyorsa;

- Yeterli önlemler (**elektrik kaçağı, yangın, su baskını, hırsızlık vs.**) alınmalı.
- **Fiziksel güvenlik** sağlanarak, yetkisiz giriş ve çıkışlar engellenmeli.

Özel ve ayrı bir politika;

- Sistemli, kuralları net, yönetilebilir ve sürdürülebilir, **ayrı bir politika ve prosedür** belirlenmeli.

Veriler aktarılacaksa;

- **Eposta:** Şifreli olarak kurumsal eposta ile veya KEP kullanılarak.
- **Taşınabilir ortamlar:** Veriler şifrelenmeli, anahtar farklı ortamda tutulmalı.
- **Sunucular arası:** VPN kurularak veya sFTP yöntemiyle aktarılmalı.
- **Kağıt ortam:** Yeterli önlemler (çalınma, kaybolmaya karşı vs.) alınmalı, gizli belge olarak gönderilmeli.

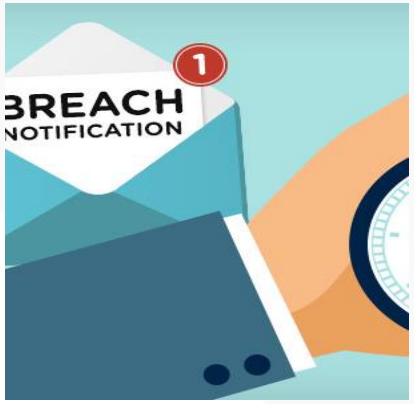
Kapanış

Stratejik sağlık verisini güvende tutmanın önemi

Sağlık verisi stratejik bir veridir. Ülkelerin sağlık bütçelerine bakıldığında, bu verilerin ekonomik açıdan önemi anlaşılmaktadır. Sağlık verilerinin milli güvenliğe ilişkin değeri ise parayla ölçülemeyecek düzeydedir.

İdari Yaptırımlar

Kişisel Verileri Koruma Kurulunun 2018/10 sayılı Kararı



1. (...) müşterinin verilerinin yer aldığı belgenin aynı isimli farklı bir kişiye gönderilmesi; müşteriye ait verilerin kişisel amaçlarla sorgulanması (...)

2. (...) veri sorumlusunun ihlâl bildirimini ilgili kişilere 17 ay, Kurula ise 10 aylık gecikmeyle bildirilmesi (...)

3. (...) şirketler topluluğu bünyesinde yer alan şirketler arasında (aynı veritabanı) veri aktarımı gerçekleştirilmesinin, üçüncü kişiye veri aktarımı olarak değerlendirildiği (...)

4. (...) sağlık raporunun, hekimler tarafından mobil kullanılan bir uygulamadaki ekran görüntüsünün başka bir cihazla çekilmesi ve sosyal medyada paylaşılması (...)

Beni dinlediğiniz için

TEŞEKKÜR EDERİM!

Av. Ahmet Esad BERKTAŞ (LL.M)
Bilişim Hukuku Danışmanı, Sağlık Bakanlığı

aesadberktas