KİŞİSEL VERİ GÜVENLİĞİNE

İLİŞKİN TEKNİK

TEDBİRLER REHBERİ

ETİTAY ENERJİ TELEKOMUNİKASYON İLETİSİM TEKNOLOJİ VE ATIK YÖNETİMİ GRUP ANONİM ŞİRKETİ

**İÇİNDEKİLER**

1. [GİRİŞ 3](#_bookmark0)
   1. [Amaç ve Dayanak 3](#_bookmark1)
   2. [Kapsam 3](#_bookmark2)
   3. [Tanımlar 4](#_bookmark3)
2. [KİŞİSEL VERİLERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER 4](#_bookmark4)
   1. [Siber Güvenliğin Sağlanması 4](#_bookmark5)
   2. [Kişisel Veri Güvenliğinin Takibi 6](#_bookmark6)
   3. [Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması 7](#_bookmark7)
   4. [Kişisel Verilerin Bulutta Depolanması 8](#_bookmark8)
   5. [Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakımı 9](#_bookmark9)
   6. [Kişisel Verilerin Yedeklenmesi 10](#_bookmark10)
3. [KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER](#_bookmark11)

[KAPSAMINDAKİ ÖZET TABLOLAR 11](#_bookmark11)

* 1. [Asgari Teknik Tedbirler 11](#_bookmark12)
  2. [Tavsiye Edilen Teknik Tedbirler 13](#_bookmark13)

# GİRİŞ

# AMAÇ VE DAYANAK

Kişisel Verileri Koruma Kanunu’nun 12. maddesinin birinci fıkrasında;

*“Veri sorumlusu;*

1. *Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
2. *Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
3. *Kişisel verilerin muhafazasını sağlamak*

*amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.”*

hükmü yer almaktadır.

Bu kapsamda, kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla Teknik Tedbirler Rehberi (“Rehber”) hazırlanmıştır.

# KAPSAM

Veri kayıt sistemlerinde kişisel veri güvenliğine ilişkin çeşitli riskler ortaya çıkabilmektedir. Bu risklerin önüne geçilebilmesi için gerekli zaman, kaynak ve uzmanlığın sağlanarak uygun teknik ve idari tedbirlerin alınması gerekmektedir. Bu tedbirler, her zaman yüksek maliyet gerektirmemekte olup, söz konusu tedbirlerin masrafsız ya da düşük maliyetli olarak alınması veya halihazırda sistemlerde mevcut olması da mümkündür.

Rehber, kişisel verilerin hukuka aykırı olarak işlenmesi ile kişisel verilere hukuka aykırı olarak erişilmesinin önüne geçilerek kişisel verilerin muhafazasının sağlanması ve bireylerin temel hak ve özgürlüklerinin korunmasının temini için veri sorumlularına yol göstermesi amacıyla hazırlanmış olup rehberde, alınabilecek teknik ve idari tedbirlere yer verilmiştir.

Rehberin;

**Birinci bölümü** giriş bölümü olup bu bölümde, rehberin hazırlanmasının amacına, dayanağına ve rehberin kapsamına ve tanımlara,

**İkinci bölümde,** kişisel veri güvenliğine ilişkin teknik tedbirlere,

**Üçüncü bölümde** ise incelenmesinin uygun olacağı faydalı olacağı değerlendirilen dokümanlara yer verilmiştir.

# TANIMLAR

Rehberde yer alan,

**Güvenli giriş katmanı (SSL):** Sunucu ile istemci arasında akan verinin güvenliğini ve bütünlüğünü mümkün kılan sertifikayı, İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

**İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

**Kanun:** 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

**Kayıt ortamı:** Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,

**Kişisel veri saklama ve imha politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı,

**Veri kaybı/sızıntısı önleme (DLP):** Kişisel verilerin, yanlışlıkla ya da kötü niyetli kişilerce kurum dışına çıkarılmasına engel olan ya da engel olmadan işlemi raporlamaya yarayan güvenlik yazılımını,

**Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini, ifade eder.

Bu Rehberde yer almayan tanımlar için Kanundaki tanımlara başvurulabilir.

# KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER

# Siber Güvenliğin Sağlanması

Kişisel veri güvenliğinin sağlanması için tek bir siber güvenlik ürünü kullanımı ile tam güvenliğin sağlanabileceği görüşü her zaman doğru değildir. Çünkü tehditler her geçen gün boyut ve nitelik değiştirerek etki alanlarını genişletmektedirler.

Bu kapsamda tavsiye edilen yaklaşım, birçok prensip dahilinde tamamlayıcı niteliğe sahip ve düzenli olarak kontrol edilen birtakım tedbirlerin uygulanmasıdır.

Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında alınabilecek öncelikli tedbirler, güvenlik duvarı ve ağ geçididir. Bunlar, internet gibi ortamlardan gelen saldırılara karşı ilk savunma hattı olacaktır.

İyi yapılandırılmış bir güvenlik duvarı, kullanılmakta olan ağa derinlemesine nüfuz etmeden önce, gerçekleşen ihlalleri durdurabilir. İnternet ağ geçidi ise çalışanların, kişisel veri güvenliği bakımından tehdit teşkil eden internet sitelerine veya online servislere erişimini önleyebilir.

Bununla birlikte hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerekmektedir. Ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta olup, kullanılmayan yazılım ve servislerin cihazlardan kaldırılması potansiyel güvenlik açıklarının azalmasını sağlamaya yardımcı olacaktır. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir.

Diğer önemli unsurlardan biri de yama yönetimi ve yazılım güncellemeleri olup yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi de olası güvenlik açıklarının kapatılması için gereklidir.

Ayrıca, 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. Söz konusu şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmalıdır.

Buna bağlı olarak veri sorumlularının, erişim yetki ve kontrol matrisi oluşturmaları 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 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.

# Kişisel Veri Güvenliğinin Takibi

Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir.

Bu durumun önüne geçebilmek için;

* + 1. Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,
    2. Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,
    3. Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),

**ç)** Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,

* + 1. Çalışanların sistem ve servislerdeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması, gerekmektedir.

Söz konusu raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir.

Ayrıca 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.

Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanmalıdır.

# Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Kişisel veriler, veri sorumlularının yerleşkelerinde yer alan cihazlarda ya da kağıt ortamında saklanıyor ise, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması suretiyle korunması 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 sınırlandırılabilir veya bileşenlerin ayrılması sağlanabilir. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.

Aynı seviyedeki önlemlerin veri sorumlusu yerleşkesi dışında yer alan ve veri sorumlusuna ait kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınması gerekmektedir.

Kişisel veri güvenliği ihlalleri sıklıkla kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) çalınması ve kaybolması gibi nedenlerle ortaya çıksa da 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 mutlaka yeterli güvenlik tedbirleri alınmalıdır.

Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, 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 erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması kişisel veri güvenliğinin sağlanmasına yardımcı olacaktır. Bu kapsamda şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanmalı ve yetkisiz erişim önlenmelidir. Benzer şekilde, kişisel veri içeren kağıt ortamındaki evraklar da kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmalı, söz konusu evraklara yetkisiz erişim önlenmelidir.

Bunlarla birlikte şifreleme farklı farklı formlarda kullanılan ve bu formlara göre farklı şartlar sağlayan bir güvenlik sağlama aracıdır. Bu kapsamda, tam disk şifrelemesiyle cihazın tümü şifrelenebilir ya da cihazda bulunan bir dosya şifrelenebilir. Bazı yazılımlar ise verilerde değişiklik yapılmasına izin vermemek için şifre koruması sunmakla birlikte bu yazılımlar kişisel verinin yetkisiz kişiler tarafından okunmasını durdurmaz. Bu nedenle hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunmalı ve bu amaçla uluslararası kabul gören şifreleme programlarının kullanımı tercih edilmelidir. Tercih edilen şifreleme yönteminin asimetrik şifreleme yöntemi olması halinde, anahtar yönetimi süreçlerine önem gösterilmelidir.

# Kişisel Verilerin Bulutta Depolanması

Kişisel verilerin bulutta depolanması, hukuka aykırı işlemenin ve erişimin önlenmesi ile

hukuka uygun muhafaza yükümlülüğü olan veri sorumlusunun kendi bilgi teknolojileri sistemi ağından ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olduğundan, bu durum birtakım riskleri beraberinde getirmektedir.

Bu nedenle, bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının veri sorumlusunca değerlendirilmesi gerekmektedir.

Bu kapsamda, 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 önerilmektedir.

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.

# Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakımı

Veri sorumlusu tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır.

Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır.

Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi gibi işlemler yapılması gerekir. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

# Kişisel Verilerin Yedeklenmesi

Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir.

Ayrıca kötü amaçlı yazılımlar da halihazırdaki verilere erişime engel olabilmektedir. Örneğin elektronik cihazlardaki kişisel verileri içeren dosyaları kilitleyen ve bunların açılabilmesi için veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlar olabilir. Bu tür kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi önerilmektedir.

Öte yandan, yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmalı, veri seti yedekleri mutlaka ağ dışında tutulmalıdır. Aksi halde, veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınabilecektir. Bu nedenle tüm yedeklerin fiziksel güvenliğinin de sağlandığından emin olunmalıdır.

# KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER KAPSAMINDAKİ ÖZET TABLOLAR

Veri sorumlularının; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin hukuka uygun olarak muhafazasını sağlamak amacıyla alabilecekleri teknik ve idari tedbirleri gösteren tablolar aşağıda verilmiştir.

Teknik ve idari tedbirler belirlenirken, kişisel verilerin niteliği ve muhafaza edildiği ortam göz önünde bulundurulur.

# Asgari Teknik Tedbirler

Tablo 1’de veri sorumluları tarafından alınması beklenen asgari teknik tedbirler gösterilmiştir.

|  |
| --- |
| **Asgari Teknik Tedbirler** |
| 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 Yönetimi |

Tablo 1. Asgari Teknik Tedbirler

# Tavsiye Edilen Teknik Tedbirler

Tablo 2’de veri sorumluları tarafından alınması tavsiye edilen teknik tedbirler gösterilmiştir.

|  |
| --- |
| **Tavsiye Edilen Teknik Tedbirler** |
| Ağ güvenliği ve uygulama güvenliği sağlanmaktadır. |
| Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır. |
| Çalışanlar için yetki matrisi oluşturulmuştur. |
| Erişim logları düzenli olarak tutulmaktadır. |
| Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır. |
| Güncel anti-virüs sistemleri kullanılmaktadır. |
| Güvenlik duvarları kullanılmaktadır. |
| Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır. |
| Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır. |
| Kişisel veri içeren ortamların güvenliği sağlanmaktadır. |
| Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır. |
| Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır. |
| Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır. |
| Mevcut risk ve tehditler belirlenmiştir. |
| Saldırı tespit ve önleme sistemleri kullanılmaktadır. |
| Sızma testi uygulanmaktadır. |
| Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir. |
| Şifreleme yapılmaktadır. |

|  |
| --- |
| Veri kaybı önleme yazılımları kullanılmaktadır. |

Tablo 2. Tavsiye Edilen Teknik Tedbirler