KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİ GÜVENLİĞİ REHBERİ (Teknik ve İdari Tedbirler)

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİ GÜVENLİĞİ REHBERİ (Teknik ve İdari Tedbirler)

KİŞİSEL VERİ GÜVENLİĞİ REHBERİ (Teknik ve İdari Tedbirler)

KVKK Yayınları
ISBN : 978-975-19-6834-0
Ocak 2018, Ankara

Kişisel Verileri Koruma Kurumu
Adres: Nasuh Akar Mahallesi Ziyabey Caddesi 1407. Sokak No: 6
Balgat/Çankaya/ANKARA/ TÜRKİYE
Telefon: +90 312 216 50 50
Web: www.kvkk.gov.tr

KİŞİSEL VERİLER
TEKNİK TEDBİR
HUKUK
VERİ GÜVENLİĞİ
İDARİ TEDBİR
YÖNETMELİK
6698
VERİ SORUMLUSU
KANUN
MEVZUAT
KARARTMA
VERİ GÜVENLİĞİ

ÖZET

Bu Rehber; 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla veri sorumlularının alması gereken teknik ve idari tedbirlere ilişkin başlıca yöntemleri ayrı ayrı bölümler halinde açıklamaktadır.

ABSTRACT

This Guide, in accordance with Law 6698 on Protection of Personal Data (“Law No. 6698”), explains in different sections the major methods of the technical and administrative measures that data controllers should take in order to prevent unlawful processing of personal data and unlawful access to personal data as well as to ensure the retention of personal data.

ANAHTAR KELİMELER:

Kişisel veri, kişisel veri güvenliği, teknik ve idari tedbirler.

KEY WORDS:

Personal data, personal data security, technical and administrative measures.

İÇİNDEKİLER

1.GİRİŞ

1.1. Amaç ve Dayanak

Kanunun 12 nci maddesinin birinci fıkrasında;

“Veri sorumlusu;
a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) 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 ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla Kişisel Verileri Koruma Kurulu (“Kurul”) tarafından Kişisel Veri Güvenliği Rehberi (“Rehber”) hazırlanmıştır.

1.2. 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 idari tedbirlere,

Üçüncü bölümde, kişisel veri güvenliğine ilişkin teknik tedbirlere,

Dördüncü bölümde, ikinci ve üçüncü bölümde bahsedilen tedbirler kapsamında oluşturulan özet tablolara,

Beşinci bölümde ise rehber hazırlanırken faydalanılan kaynaklar ve incelenmesinin uygun olacağı değerlendirilen dokümanlara

yer verilmiştir.

1.3. Tanımlar

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.

2. KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN İDARİ TEDBİRLER

2.1. Mevcut Risk ve Tehditlerin Belirlenmesi

Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.

Bu riskler belirlenirken;

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,
- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği

dikkate alınmalıdır.

Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.

2.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin, çalışanların sınırlı bilgileri olsa dahi ilk müdahaleyi yapmaları, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır.

Kişisel veri güvenliğini ihlal etmeye yönelik saldırıların yanısıra, kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlallerindendir. Bu ihlaller, kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerinin kullanılması suretiyle kötü amaçlı yazılım içeren elektronik posta ekinin açılması veya elektronik postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin erişimine açılması şeklinde de ortaya çıkabilmektedir.

Bu nedenle çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.

Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır.

Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken “Yasaklanmadıkça Her Şey Serbesttir” prensibi değil, “İzin Verilmedikçe Her Şey Yasaktır” prensibine uygun hareket edilmesine dikkat edilmelidir.

Öte yandan, çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik anlaşmalarını imzalamaları istenebilir. Çalışanların güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci de mutlaka olmalıdır.

Kişisel veri güvenliğine ilişkin politika ve prosedürlerde önemli değişikliklerin meydana gelmesi halinde; yapılacak yeni eğitimlerle bu değişikliklerin, çalışanların bilgisine sunulması ve kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerinin güncel tutulması sağlanmalıdır.

2.3. Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi

Kişisel veri güvenliğine ilişkin iyi bir politika hazırlanması, bu kapsamdaki risklerin önceden belirlenebilmesini ve istikrarlı bir şekilde önlem alınmasını sağlayacaktır.

Kişisel veri güvenliğine ilişkin belirlenecek doğru ve tutarlı politika ve prosedürler, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Veri sorumlularınca politika ve prosedürler iyi bir şekilde ve zamanında hazırlanamadığında, sorunlu alanlar belirlenemediğinde veya mevcut güvenlik önlemleri kullanılamadığında kişisel veri güvenlik seviyesi yeteri kadar sağlanamamaktadır.

Bu kapsamda alınacak tedbirlerin önceden belirlendiği iyi bir olay yönetimi, çalışanlar üzerinde ortaya çıkabilecek baskıyı azaltacaktır. Bu nedenle veri sorumlularının, veri kayıt sistemlerinde hangi kişisel verilerin bulunduğundan ve mevcut güvenlik önlemlerini inceleyerek diğer yasal yükümlülüklerle uyumlu hareket edildiğinden emin olması gerekmektedir.

Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılmalı, yapılan kontroller belgelenmeli, geliştirilmesi gereken hususlar belirlenmeli ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmelidir.

Ayrıca, her kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmelidir.

2.4. Kişisel Verilerin Mümkün Olduğunca Azaltılması

Kanunun 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler, gerektiğinde doğru ve güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Ancak, özellikle uzun süredir faaliyet gösteren veri sorumluları, çok fazla miktarda kişisel veri toplamakta olduğundan söz konusu kişisel verilerin bir kısmı zamanla doğru olmayan, güncelliğini yitirmiş ve herhangi bir amaca hizmet etmeyen veriler haline gelebilmektedir. Bunun önüne geçebilmek için, veri sorumlularınca işleme amaçları bakımından anılan kişisel verilere hala ihtiyaç olup olmadığının değerlendirilmesi ve kişisel verilerin doğru yerde muhafaza edildiğinden emin olunması gerekmektedir.

Bunun yanında, yetkisiz erişimin önüne geçilebilmesi için kişisel veri işleme amaçlarına uygun olmasına rağmen, veri sorumlularının sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi tavsiye edilmekte ve ihtiyaç duyulmayan kişisel verilerin ise kişisel veri saklama ve imha politikası ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve güvenli bir şekilde imha edilmesi gerekmektedir.

2.5. Veri İşleyenler ile İlişkilerin Yönetimi

Bazı veri sorumluları, bilgi teknolojileri ihtiyaçlarını karşılamak için veri işleyenlerden hizmet almaktadırlar. Veri sorumlularının, hizmet alırken söz konusu veri işleyenlerin kişisel veriler konusunda en az kendileri tarafından sağlanan güvenlik seviyesinin

sağlandığından emin olmaları gerekmektedir. Zira Kanunun 12 nci maddesinin ikinci fıkrası gereği veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusuyla müştereken sorumludur.

Veri işleyen ile imzalanan sözleşmenin yazılı olması, veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde hareket edeceğine ilişkin hüküm içermesi ve Kişisel Veri Saklama ve İmha Politikasına uygun olması önerilmektedir.

Veri işleyenin, işlediği kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tabi olacağının da bu sözleşmede yer alması önem taşımaktadır.

Yine söz konusu sözleşmede herhangi bir veri ihlali olması durumunda, veri işleyenin bu durumu derhal veri sorumlusuna bildirmekle yükümlü olduğunun öngörülmesi de, veri sorumlusunun bu ihlali derhal Kişisel Verileri Koruma Kurulu'na ve ilgili kişiye bildirme yükümlülüğünü yerine getirmesi açısından faydalı olacaktır.

Ayrıca; taraflar arasındaki sözleşmenin niteliği buna elverdiği ölçüde, veri sorumlusu tarafından veri işleyene aktarılan kişisel veri kategori ve türlerinin de ayrı bir maddede belirtilmiş olması, veri işleyenin veri güvenliğini sağlama yükümlüğünü yerine getirmesi açısından faydalı olacaktır.

Bununla birlikte veri sorumlusu, kişisel veri içeren sistem üzerinde gerekli denetimleri yapar veya yaptırır, denetim sonucunda ortaya çıkan raporları ve hizmet sağlayıcıyı yerinde inceleyebilir.

3. KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER

3.1. 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 yanısıra, 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.

3.2. 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;

a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,
b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,
c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),
ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,
d) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini 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 zaafiyetlere karşı korunması için düzenli olarak zaafiyet 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.

3.3. 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.

3.4. 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.

3.5. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

Veri sorumlusu tarafından yeni sistemlerin tedariği, 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.

3.6. 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.

4. KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK ve İDARİ 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.

4.1. Teknik Tedbirler Özet Tablosu

Tablo 4.1'de veri sorumluları tarafından alınabilecek teknik tedbirler gösterilmiştir.

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 4.1. Teknik tedbirler

4.2. İdari Tedbirler Özet Tablosu

Tablo 4.2'de veri sorumluları tarafından alınabilecek idari tedbirler gösterilmiştir.

İdari Tedbirler
Kişisel Veri İşleme Envanteri Hazırlanması
Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında)
Gizlilik Taahhütnameleri
Kurum İçi Periyodik ve/veya Rastgele Denetimler
Risk Analizleri
İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

Tablo 4.2. İdari tedbirler

5. REHBER HAZIRLANIRKEN FAYDALANILAN KAYNAKLAR ve İNCELENMESİNİN UYGUN OLACAĞI DEĞERLENDİRİLEN DOKÜMANLAR

Aşağıdaki dokümanların da okunup gözden geçirilmesi Kurul tarafından tavsiye edilmektedir.

AHA	American Hospital Association, Cybersecurity and Hospitals, 2013, bkz. http://www.aha.org/content/13/ahaprimer-cyberandhosp.pdf
Article 29	29. Madde Avrupa Veri Koruma Grubu, Advice paper on special categories of data ("sensitive data").
Baskerville/ Im/	R.L. Baskerville, G.P.Im, A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error", SIGMIS Database, vol.36, 2005.
Brown/Marsden	I. Brown, C. T. Marsden, Regulating Code: Good Governance and Better Regulation in theInformation Age, The MIT Press, 2013
BS10012:2009	British Standart, Data protection – Specification for a personal information management system
BSI C5	Federal Office for Information Security, Cloud Computing Compliance Controls Catalogue (C5), criteria to assess the information security of cloud services v 1.0
Castells	M. Castells, Ağ Toplumunun Yükselişi, Birinci Cilt, çev. E. Kılıç, İstanbul Bilgi Yayınları, 2005
CES	Cyber Essentials Scheme, Requirements for basic technical protection from cyber attacks,
Desmedt	Y. Desmedt, Man-in-the-Middle Attack, Encyclopedia of Cryptography and Security, 2011

Directive 95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Oficial Journal of the European Communities of 23 Kasım 1995, No L. 281, s. 31.

Directive 2002/58/EC Directive 2002/58/EC of the European Parliament and of the Council of 12 Temmuz 2002 concerning the processing of personal data and protection of privacy in the electronic communications sector OJ L201/37

ENISA The European Union Agency for Network and Information Security, Hardware Threat Landscape and Good Practice Guide, Şubat 2017, bkz. https://www.enisa.europa.eu/publications/ hardware-threat-landscape

ENISA The European Union Agency for Network and Information Security, Cyber Security and Resilience for Smart Hospitals, Kasım 2016, bkz. https:// www.enisa.europa.eu/publications/ cyber-security-and-resilience-for-smart-hospitals

ENISA European Union Agency for Network and Information Security, Cyber Security and Resilience of Intelligent Public Transport, Good practices and recommendations, 2016, bkz. https://www. enisa .europa.eu/ publications/good-practices-recommendations

ENISA Guidelines for SMEs on the security of personal data processing, 27 Ocak 2017, bkz. https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ENISA Algorithms, key size and parameters report 2014, 21 Kasım 2014, https://www.enisa.europa.eu/publications/algorithms- key- size-and-parameters-report-2014

Gunter O.Gunter, The Phishing Guide-Understanding and Preventing Phishing Attacks.

Gürses B. Gürses, Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği, Sorunlar ve Çözüm Önerileri, BTK İdari Uzmanlık Tezi (2013)

Gürses/ Danezis S. Gürses, G Danezis, A Critical Review of Ten Years of Privacy Technology, UK, 2012

Hilbert M. Hilbert, Big Data for Development: From Information- to Knowledge Societies, United Nations ECLAC, 2013

ICO Information Commisioner's Office, Encryption Guide, https://ico.org.uk/media/for-organisations/encryption-1-0.pdf

ICO Information Commisioner's Office, A Practical Guide to IT Security,bkz. https://ico.org.uk/media/for-organisations/ documents/1575 /it_security_ practical_guide.pdf

ISO/IEC International Standarts of Organizations, Information technology - Security techniques - Information security management systems – Requirements

ISO/IEC International Standarts of Organizations, Information technology - Security techniques, Code of practice for information security controls

Küzeci E. Küzeci, Kişisel Verilerin Korunması, Turhan Kitabevi, 2010

NIS The Directive on security of network and information systems (NIS Directive), European Commission, Temmuz 2016, bkz. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv: OJ. L_.2016.194.01.0001.01. ENG&toc=OJ:L:2016:194:TOC

NIST National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, v 1.0,

NIST National Institute of Standards and Technology, Guidelines for Smart Grid Cyber Security, 2010, bkz. https://www.nist. gov/ sites/default/ files/ documents/smartgrid/nistir-7628_total.pdf

Ok K. OK, Bilgi ve Bilgi Yönetimine Giriş, 1. Baskı, Papatya Yayıncılık Eğitim, İstanbul, Ekim 2013

Özdemir H. Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayıncılık, 2009

Şimşek O. Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Basım, 2008

TBD Türkiye Bilişim Derneği, Bilişim Sistemleri Güvenliği El Kitabı, v 1.0, Ankara, Mayıs 2006

UDHB T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planı, bkz. http://www.udhb.gov.tr/ doc/ siberg/2016-2019guvenlik.pdf

Vural/Sağıroğlu Y. Vural, Ş. Sağıroğlu, Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, Bildiriler Kitabı Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 2007

Yılmaz H.Yılmaz, TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi, Denetişim 2014-2015, http://dergipark.gov.tr/download/article-file/208742

Weingart S. Weingart, Physical security devices for computer subsystems: A survey of attacks and defenses, Cryptographic Hardware and Embedded Systems - CHES 2000, s. 45-68

Wolfe/ Gunasekara/ Bogue

N. Wolfe, L. Gunasekara, Z. Bogue, Crunching Digital Data can help the World, 2011, bkz. http://edition.cnn.com/2011/OPINION/02/02/wolfe.gunasekara.bogue.data/index.html?_s=PM:0 PINION