KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

Genel Müdürlük: Sümer Mahallesi 2482/2 Sokak
No: 4/1 İç Kapı No:9 Skycity B Blok
Merkezefendi/DENİZLİ
bilgi@deosgb.com.tr
www.deosgb.com.tr / 444 76 89

İçindekiler

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 alınması gereken teknik ve idari tedbirler konusunda alınması gereken önlemleri tanımlamak amacıyla bu politika hazırlanmıştır.

1.2 Kapsam

Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Şirket'in sahip olduğu ya da Şirketimizce yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3 Kısaltmalar ve Tanımlar

Alıcı Grubu: *Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.*

Açık Rıza: *Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.*

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

Çalışan: *Kişisel Verileri Koruma Şirket personeli.*

EBYS: *Elektronik Belge Yönetim Sistemi*

Elektronik Ortam: *Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, eriştirilebildiği ve yazılabildiği ortamlar.*

Elektronik Olmayan Ortam: *Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.*

Hizmet Sağlayıcı: *Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.*

İlgili Kişi: *Kişisel verisi işlenen gerçek kişi.*

İlgili Kullanıcı: *Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler.*

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

Kanun: *6698 Sayılı Kişisel Verilerin Korunması Kanunu.*

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 ortam.*

Kişisel Veri: *Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.*

Kişisel Veri İşleme Envanteri: *Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.*

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

Özel Nitelikli Kişisel Veri: *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.*

Periyodik İmha: *Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.*

Politika: *Kişisel Verileri Saklama ve İmha Politikası*

Veri İşleyen: *Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.*

Veri Kayıt Sistemi: *Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.*

Veri Sorumlusu: *Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.*

Veri Sorumluları Sicil Bilgi Sistemi: *Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.*

VERBİS: *Veri Sorumluları Sicil Bilgi Sistemi*

Yönetmelik: *28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.*

Güvenli giriş katmanı (SSL): *Sunucu ile istemci arasında akan verinin güvenliğini ve bütünlüğünü mümkün kılan sertifika.*

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 yazılımı.*

Veri kayıt sistemi: *Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.*

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.

Tüm çalışanların 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.

Her bir kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmelidir.

2.3. 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, 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, 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 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.

2.4. Veri İşleyenler ile İlişkilerin Yönetimi

Hizmet alınan veri işleyenlerin kişisel veriler konusunda sağladığı güvenlik seviyesinin yeterli olduğundan emin olunmalıdır. 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 gereklidir.

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

Ayrıca; taraflar arasındaki sözleşmenin niteliği buna elverdiği ölçüde, 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 kişisel veri içeren sistem üzerinde gerekli denetimler düzenli olarak yapılmalı veya yaptırılmalıdır, denetim sonucunda ortaya çıkan raporlar ve hizmet sağlayıcı yerinde incelenebilir.

3. KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER

3.1. Siber Güvenliğin Sağlanması

Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında öncelikli olarak güvenlik duvarı ve ağ geçidi tedbiri alınmalıdır. Güvenlik duvarının iyi yapılandırılması, kullanılmakta olan ağa derinlemesine nüfuz etmeden önce, gerçekleşen ihlalleri durdurması açısından çok önemlidir.

Çalışanların kişisel veri güvenliği bakımından tehdit teşkil eden internet sitelerine veya online servislere erişimini önleyebilmek için İnternet ağ geçidi kullanılmalıdır.

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 öncelikli olarak tercih edilmelidir.

Diğer önemli unsurlardan biri de yama yönetimi ve yazılım güncellemeleridir. 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 erişim sınırlı olmalıdır. 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. 17 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

Sistemlere içeriden veya dışarıdan gelen saldırılar ve siber suçlar veya kötü amaçlı yazılımlara maruz kalma durumunda, müdahale için geç kalmadan;

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

Şirket yerleşkelerinde yer alan cihazlarda ya da kağıt ortamında saklanan kişisel verilerin, 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 sınırlandırılmalı veya bileşenlerin ayrılması sağlanmalıdır.

Kullanılmakta olan ağın sadece belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.

Aynı seviyedeki önlemlerin şirket yerleşkesi dışında yer alan 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 tutulmalı, 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 kapsamında şirkete ait 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 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 gerekmektedir.

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

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 yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi gerekir.

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

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 bulundurulmalıdır.

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