ERZURUM BÜYÜKŞEHİR BELEDİYESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI

VERİ AKTARIM GÜVENLİĞİ POLİTİKASI

(Versiyon 1.0)

2022

Doküman Detayları

Hazırlanma Tarihi	12.12.2022	**Yayın**	Final
Hazırlayan	Olcay Ozan DİKBAŞ – Ersin YILDIZ		
Doküman Numarası	EBB-POL-02		

Revizyon Geçmişi

Revizyon Tarihi	Önceki Revizyon Tarihi	Yapılan Değişikliklerin Özeti
12.12.2022		İlk Yayın

Onay

Onaylayan	İmza	Görevi	Tarih	Versiyon
Zafer AYNALI		Genel Sekreter	12.12.2022	1.0
Murat ALTUNDAĞ		Genel Sekreter Yardımcısı	12.12.2022	1.0
Serkan ÇEKİÇ		Bilgi İşlem Daire Başkanı	12.12.2022	1.0

1. AMAÇ VE KAPSAM

Kurumumuz faaliyetlerinin yürütülmesinde hem elektronik ortamda hem de kâğıt ortamında büyük kapsamlı veri depolamaktadır. İşbu Politika metni, depolanan verilerin korunması için geçerli olacak prosedürleri düzenlemek ve kişisel verilerin Kurum nezdinde ve Kurum dışına güvenli bir şekilde aktarılabilmesini temin etmektir.

İşbu Politika Kurumumuz bünyesinde kişisel verileri ve özel nitelikli kişisel verileri işleyen ve görevleri gereği Kurum paydaşlarına aktarması gereken aşağıdaki tüm kişi grupları için geçerli olacaktır:

- Çalışanlar
- Kurumumuzun ortak faaliyet yürüttüğü tedarikçiler ve üstlenici firmalar
- Stajyerler

Çalışanlarımız bu Politikayı Bilgi ve İletişim Teknolojilerinin Kullanımı Politikası ile birlikte ele almalıdırlar.

2. GEÇERLİ KANUN

6698 sayılı Kişisel verilerin Korunması Kanunu ve ilgili idari düzenlemeler.

3. ÖZEL NİTELİKLİ VERİLER

İşbu Politikanın amaçları bakımından özel nitelikli veriler aşağıdaki veri kategorilerini içermektedir:

- 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.
- Kurumumuz ile ilgili gizli veriler
- Mallar, hizmetler ve ürünlerle ilgili olarak akdedilen sözleşmelerde gizli veri olarak tanımlanan tüm veriler
- Kurumumuzun müşterileri ve tedarikçileri ile ilgili gizli kalması gereken veriler.

İşlenen herhangi bir verinin özel nitelikli veri olup olmadığı yönünde şüphe içerisinde kalan her çalışan bu hususu istihdam edildiği ilgili Departman Sorumlusuna bildirerek talimatları doğrultusunda hareket etmelidir.

4. VERİ AKTARIMLARINDA GÖZ ÖÜNDE BULUNDURULMASI GEREKEN HUSUSLAR

4.1. Kişisel veriler ve özel nitelikli kişisel verileri aktarırken her çalışan veri aktarımının yetkilendirilmesi için ilgili Departman Sorumlusunun görüş ve talimatlarına başvurmalıdır.

4.2. Özel nitelikli kişisel veriler ve diğer kişisel veriler Şirketimizin yasal

faaliyetlerinin gerektiği gibi yürütülebilmesi için kesinlikle gerekli olduğu ölçüde aktarılmalıdır. Buna göre her bir veri aktarımından önce veri aktarımının gerekli olup olmadığı önceden mütalaa edilmelidir.

4.3. Üçüncü taraflarla iletişim kurulurken ilgililerle veri paylaşımı sözleşmeleri, kişisel verilerin korunması hususunda ek protokoller imzalanıp imzalanmadığı göz önünde bulundurulmalıdır. Ayrıca kullanılması ön görülen veri aktarımı metotları hakkında bir hüküm bulunup bulunmadığı kontrol edilmeli var ise ön görülen yöntemlerin kullanılmasına özen gösterilmelidir.

4.4. Belirlenen amaç için gerekli olanın ötesinde bilgi sağlanıp sağlanmadığı her zaman kontrol edilmelidir. Örneğin bir belgenin yalnızca bir bölümü ya da belirli bir parçası talep edilmekte ise belge ya da çizelgenin tamamı gönderilmemelidir.

4.5. Kişisel veriler ve özel nitelikli kişisel verileri ihtiva eden bilgilerin aktarıldığı tüm durumlarda alıcı tarafın kimliği ve veriye erişim yetkisi açık bir şekilde tanımlanmalıdır.

5. VERİ AKTARIM YÖNTEMLERİ

Veri aktarım yöntemleri belirlenmeden önce aşağıdaki hususların göz önüne alınması gerekir:

- Aktarılacak bilginin özellikleri, hassasiyet durumu, gizlilik seviyesi ya da muhtemel değeri
- Aktarılacak verinin boyutu
- Veri aktarımı yapılırken meydana gelecek kayıpların neticesinde ilgili kişilerin maruz kalması muhtemel olan kayıplar ya da sıkıntılar
- Veri kayıplarının Şirketimiz açısından doğuracağı sonuçlar.
- Belirlenen amaç için gerekli olanın ötesinde bilgi ve belge aktarılmamalıdır. Gerekli olmayan tüm veriler aktarım yapılmadan önce karartılmalı ya da gerekli olduğu durumlarda tamamen çıkarılmalıdır.

5.1. Elektronik Posta ile veri Transferleri

- Kişisel veri ihtiva edebilecek şifrelenmemiş hassas verilerin aktarımı için elektronik posta iletişimi kullanılmamalıdır. Çalışanlarımızın elektronik postanın büyük çaplı veri eklemek ve aktarmak için dizayn edilmediği konusunda bilinçli olması gerekir.
- Çalışanlarımızın mümkün ve uygulanabilir olduğu her durumda özel nitelikli verilerin aktarımında alternatif güvenli yöntemleri kullanmayı tercih etmelidir. Uygun bir alternatifin bulunamadığı durumlarda ekstra güvenlik düzeyleri kullanılmalıdır. Örneğin şifreleme kullanımı ya da gönderilmek istenen özel nitelikli verilere erişim için şifre ve kullanıcı adı istenmesi gibi. Kullanıcı adı ve şifreler aktarılırken posta, belirlenen numaralara yapılacak telefon araması ya da SMS mesajı gibi alternatif yöntemler kullanılmalıdır.
- Elektronik posta mesajlarında alıcının doğru kişi olmadığı durumlarda yanlışlıkla veri aktarımı yapılan alıcının yasal sorumlulukları ve gelen elektronik posta iletisi ile ilgili ne yapması gerektiği hususunda açık talimatlara yer verilmelidir.

- Uygulanabilir olduğu durumlarda gönderilen bilgiler kapalı eklentiler içerisinde gönderilmelidir.
- Elektronik postanın konu satırında ya da buna eşlik eden mesaj bölümünde hangi bilginin yerleştirildiğine özen gösterilmelidir. Dosya ismi ya da konu satırında eklentilerin tüm içeriği ya da özel nitelikli kişisel veriler ifşa edilmemelidir.
- Elektronik postalar, uygun gizlilik ve güvenlik bilgilerinin gösterilebilmesi için Kurum tarafından sağlanan e-mail adresi kullanılarak aktarılmalıdır.

52. Kurum İçi Portal

- Kaldırılabilir ortama veri kopyalama ya da aktarma yapması gereken ya da gönderilecek verinin miktarının çok fazla olduğu kullanıcılar Kurumun IT Destek Ekibinden yardım almalıdır.
- Portala IT Destek Ekibinden önceden izin alınmaksızın dosya gezgini kullanılmak suretiyle erişilmemelidir.
- Portala veri yüklenirken dosya adlarının uygun bir şekilde isimlendirildiği ve doğru konumlarda depolandığından emin olunmalıdır. Portala yüklenmesi gereken özel nitelikli veriler herkesin erişebileceği konumlarda depolanmamalıdır.
- Kurumun kullandığı ağa veri yüklenirken uygun prosedürler takip edilerek güvenli portal kullanılmaya özen gösterilmelidir.
- Çevrimiçi eğitim kaynaklarına aktarılacak her bir veri şifre korumalı doküman ya da şifrelendirilmiş zip dosyası kullanılarak şifrelenmelidir.

53. Çıkarılabilir Veri Depolama Araçları (hafıza kartı, USB sürücü vb.)

- USB taşınabilir bellek gibi çıkarılabilir ortamlar vasıtasıyla aktarılan her veri şifrelenmelidir. Şifrelenen taşınabilir depolama araçları güçlü şifreler kullanılarak korunmalıdır. Eğer şifrenin kendisinin üçüncü bir tarafa bildirilmesi gerekiyorsa ilgili bilgi posta, telefon ya da SMS mesajı gibi alternatif yöntemler kullanılarak aktarılmalıdır.
- Kaldırılabilir ortama veri kopyalama ya da aktarma yapması gereken ya da gönderilecek verinin miktarının çok fazla olduğu kullanıcılar Kurumun IT Destek Ekibinden yardım almalıdır.
- Kullanılan kaldırılabilir ortamların zilyetliği açık bir şekilde tanımlanmalıdır. Kaldırılabilir ortam veri aktarımı yapıldıktan sonra sahibine iade edilmeli ve aktarılan veriler kullanıldıktan sonra veri depolama cihazından silinmelidir.
- Alıcının doğru kişi olmadığı durumlarda yanlışlıkla veri aktarımı yapılan alıcının yasal sorumlulukları ve gelen elektronik posta iletisi ile ilgili ne yapması gerektiği hususunda açık talimatlara yer verilmelidir
- Dosya adı ve ilişik mesajlarda şifreli dosyanın içeriği hakkında bilgi ifşa edilmememledir.
- Gönderici uygun bir zamanda veri aktarımının başarı ile gerçekleştirilip gerçekleştirilmediğini çek etmeli ve bunun için teslim alma belgesi düzenlenmelidir. Dosyanın alındığını teyit eden elektronik posta mesajları bu

amaç için uygun olabilir.

- Yaşanan olumsuzluklar sıralı amirlere bildirilmeli ve kaybolan ya da bozulmuş veriler hakkında derhal Veri Koruma Sorumlusu/İrtibat Görevlisine bilgi verilmelidir.

5.4. Telefon Görüşmeleri

Telefon görüşmeleri takip edilebildiğinden, kulak misafiri olabileceğinden veya kesilebileceğinden (kasıtlı veya kazara), aşağıdaki hususlara özen gösterilmelidir:

- Alıcının kimliğini ve yetkisini onaylamadığınız sürece kişisel veriler telefonla aktarılmamalı veya tartışılmamalıdır.
- Telesekreter kullanırken hassas veya gizli mesajlar bırakmayın veya herhangi bir kişisel veri eklemeyin. Yalnızca bir iletişim aracı sağlayın ve alıcının sizinle kişisel olarak konuşmasını bekleyin.
- Kendinize bırakılan sesli telefon mesajlarını dinlerken, başkalarının kulak misafiri olma riski taşıyan açık alanlarda ses kaydını açmamaya dikkat edin.

5.5. Posta ve Kurye Vasıtasıyla Veri Aktarımları

- Hafıza kardı ya da CD gibi fiziki ortamlarda taşınacak olan veri aktarımlarında güvenli posta hizmetleri kullanılmalıdır. Birinci ya da ikinci sınıf posta yerine özel teslimat ve taahhütlü posta hizmeti tercih edilmelidir. PTT harici posta kullanılacaksa teslimat sonrası imzalı teslimat yöntemini kullanan güvenli kurye hizmeti sunan firmalar tercih edilmelidir.
- Alıcı açık bir şekilde posta gönderi kısmında belirtilmeli ve fiziki ortamın kırılma ya da zarar görmemesi için güvenli bir şekilde paketlenmesi sağlanmalıdır.
- Alıcılar öncesinden bilgilendirilerek aktarılacak verileri ne zaman almaları gerektiği hususunda önceden bilgi sahibi olmalıdır. Alıcı veri ulaşır ulaşmaz güvenli bir şekilde teslim alındığını belirtmelidir. Veri aktarımından sorumlu olan gönderici verinin güvenli bir şekilde ulaştığını teyit etmekle mükelleftir.

5.6. Elden Teslimat

Belgelerin elden teslim edilmesi ve alınması onaylanan aktarım yöntemleri içerisindedir. Bir kişinin aktarılacak verileri teslim alması planlanmışsa kimliği önceden belirlenmeli ve teslimatta uygun kimlik teyit yöntemleri kullanılarak alıcının kastedilen kişi olduğu doğrulanmalıdır.

6. Kayıp Veriler

Her bir çalışan herhangi bir verinin kaybolduğunu tespit ettiğinde derhal sıralı amirini ve veri Koruma Sorumlusu/İrtibat Görevlisini konudan haberdar etmeli ve Kişisel Veri İhlali Müdahale Planında belirtilen işlemler gecikmeksizin yerine getirilmelidir.

Yetkisiz kullanıcıların özel nitelikli verilere erişim sağladığından şüphe ediliyorsa gecikmeksizin kolluk kuvvetlerine bilgi verilmelidir.

7. Veri Aktarımı Konularında İhmal Gösterilmesi

İşbu Politika kapsamında vazedilen hususlara riayet göstermek noktasında ihmal sergileyen çalışanlar görevde ağır ihmal göstermiş sayılarak iş akitleri feshedilebilir. Kişisel veri ihlali durumları Kurumumuzun itibar kaybına ve ağır para cezalarına maruz kalmasına neden olabilecektir.

Bu nedenle çalışanlarımızın özel nitelikli veriler aktarılırken azami özen göstermeleri zaruridir. İhmal ve kusurlu davranış olarak değerlendirilebilecek filler: yetki almaksızın veri aktarımı yapılması, verinin uygun şekilde şifrelenmemesi, sıkıştırılarak şifre koruması kullanılmaması, taahhütlü ya da sigortalı posta hizmetlerinin kullanılmaması vb.dir.