İÇİNDEKİLER

1. **Amaç**
2. **Tanımlar**
3. **Kapsam**
4. **Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Önlemlere Dair Esaslar**
5. **Diğer Güvenlik Önlemleri**
6. **Diğer Hukuki Düzenlemeler**
7. **İhlalin Bildirimi**
8. **Uygulama**
9. **Saklama**

1. Amaç

İşbu Özel Nitelikli Kişisel Verilerin İşlenmesi ve Korunması Politikası (Politika), şirketimizin belirlemiş olduğu, özel nitelikli kişisel verilerin işlenmesinde alınması gerekli önlemlere dair yürürlükteki mevzuata uyumunu temin etmeye yönelik prensipleri düzenlemektedir.

2. Tanımlar

İşbu Politika'da kullanılan terimler kendilerine aşağıda atfedilen anlamları haiz olacaklardır. Burada yer almayan tanımlar Kanun ve ikincil düzenlemelerde tanımlandıkları şekilde kullanılacaktır.

İki Kademeli Kimlik Doğrulama	Kişinin kullanıcı adı ve şifresi ile, dışarıdan ayrı bir kimlik doğrulama sisteminin (cep telefonu, kişisel soru, kriptografik anahtar vb.) birleşiminden oluşan doğrulama sistemini ifade eder.
Kayıtlı Elektronik Posta (KEP)	Elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukukî delil sağlayan, elektronik postanın nitelikli şeklini ifade eder.
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ifade eder.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
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 işlemi ifade eder.
Özel Nitelikli Kişisel Veri (ÖNKV)	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 verileridir.
SFTP	Kriptografik ağ protokolü SSH kullanarak dosya transferi yapan bir dosya aktarım protokolüdür.
Sanal Özel Ağ (VPN)	Sanal ağ uzantısı oluşturarak internet ya da başka bir açık ağ üzerinden özel bir ağa fiziksel olarak bağlıymışçasına o ağ üzerinden veri alışverişinde bulunmayı sağlayan bağlantı çeşidini ifade eder.
Sızma Testi	Bilişim sistemlerine mümkün olabilecek her yolun denenerek sızılmaya çalışma işlemlerini ifade eder.
Güvenli Ortam *(Secure vault)*	Hareketsiz değerli verinin okunmaya, değiştirilmeye ve taşınmaya karşı korunması amacıyla oluşturulmuş yazılım alanıdır.
Şirket	Veri Sorumlusu'nu ifade eder.
Uçtan Uca Şifreleme	Gönderilen iletinin şifrelenerek iletinin sadece gönderen ve gönderilen tarafça okunulmasını sağlayan şifreleme metotlarını ifade eder.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, Veri Kayıt Sistemi'nin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Veri Sorumlusu İrtibat Kişisi	Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanun'a dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla sicile kayıt esnasında bildirilen gerçek kişiyi ifade eder.
Veri Yetkilisi	Veri Sorumlusu tarafından atanan ve Kanun'a uygun olarak Şirket kişisel veri envanterini oluşturan, güncel tutan ve gerekli değişiklikleri Veri Sorumlusu İrtibat Kisisine ileten sirket calısanını ifade eder.
Yetki Matrisi	Kişisel verilerin yer aldığı sistemlerde kullanıcıların erişim, kayıt oluşturma, görüntüleme, değiştirme gibi yetkilere sahip olup olmadıklarını gösteren bir matristir.

3. Kapsam

Kanun'un 12. maddesi uyarınca Şirket, veri sorumlusu olarak, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Ayrıca, Kişisel Verileri Koruma Kurulu'nun (Kurul) "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı (özel nitelikli kişisel verilere dair karar) uyarınca, kişisel verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması gerekmektedir.

İşbu Politika, Kanun ve özel nitelikli kişisel verilere dair ilke kararı uyarınca Şirket'in özel nitelikli kişisel verilerin işlenmesinde alması gereken önlemlere dair düzenlemeleri kapsar.

4. Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Önlemlere Dair Esaslar

4.1. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ve fiziki ortamlar envanterde belirtilir. Özel nitelikli kişisel veriler yüksek risk içeren kişisel veriler olarak sınıflandırılır.

4.2. Özel nitelikli kişisel verilere erişim Şirket çalışanları ve alt-işveren çalışanları ile kısıtlıdır. Kanun'da öngörülen hukuki sebeplerin bulunması hali hariç, Şirket dışından hizmet sağlayıcılarına veya çalışanlarına özel nitelikli kişisel veri erişimi verilemez.

4.3. Şirket çalışanlarının, kişisel verilerin ve özel nitelikli kişisel verilerin gizliliğine “Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikasını” imzalamış olmaları ve Kanun ve buna ikincil mevzuat ile özel nitelikli kişisel verilerin güvenliği konularında Şirket'in belirleyeceği eğitimi almış olmaları zorunludur. Şirket çalışanlarının farkındalığını arttırmak amacıyla Şirket bünyesinde kişisel verilerin korunmasına yönelik aktiviteler düzenler.

4.4. Özel nitelikli kişisel verilerin gizliliğine dair, tüm çalışanların uyması gereken prensipleri de içeren ve Şirket tarafından “Kişisel Verilerin Korunması ve İşlenmesi Politikası” ile “Kişisel Veri Saklama ve İmha Politikası” yayınlanmıştır. Bunlarla birlikte, özel nitelikli kişisel verilerin gizliliğine dair uyulması gereken ana politika işbu politikadır.

4.5. Elektronik ortamda muhafaza edilen özel nitelikli kişisel veriler için,

4.5.1. Özel nitelikli kişisel verilerin kayıt edildiği kayıt ortamlarında kullanılacak kriptografik şifreleme metotları veya şifreleme sistemi içeren veri kayıt sistemi kullanılır.

4.5.2. Özel nitelikli kişisel verilerin aktarımlarında kullanılacak şifreleme yöntemleri en azından Uçtan Uca Şifreleme koruması içeren e-posta sistemlerinin kullanılması veya kurulumu sağlanır.

4.5.3. Kriptografik anahtarlar güvenli ortamda *(secure vault)* tutulur.

4.5.4. Veriler üzerinde gerçekleştirilen hareketlerin işlem kayıtları loglanır, zaman damgasıyla imzalanır ve güvenli ortamda erişim kontrolleri uygulanarak saklanır.

4.5.5. Üreticilerin yayınladığı güvenlik güncellemeleri veri sistemlerine uygulanır.

4.5.6. Verilerin bulunduğu ortamlara ait güvenlik testleri yılda 1 kez yapılır ve test sonuçlarının kayıt altına alınması sağlanır.

4.5.7. Verilere erişim için erişim yetki kontrol metotları uygulanır. Bu metotlar "Bilgi Sistemleri Erişim Kontrol Yönetim Politikasına" göre takip edilir.

4.6. Fiziksel ortamda işlenen, muhafaza edilen ve/veya erişilen ÖNKV için,

4.6.1. Özel nitelikli kişisel verilerin bulunduğu ortamlar ve nitelikleri her bir bölüm tarafından kişisel veri envanterinde belirlenir.

4.6.2. Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre gerekli önlemlerin alındığından emin olunması gereklidir.

4.6.3. Şirket, herhangi bir veri ihlali durumunda kanuni yükümlülüklerin yerine getirilebilmesi ve bu konudaki düzenlemelere uygun hareket edilebilmesi amacıyla "Kriz Müdahale Prosedürünü" işletmektedir.

4.6.4. Özel nitelikli kişisel verilerin bulunduğu tüm fiziksel ortamların güvenliğinin sağlanması için tüm ortamlara giriş çıkışlar kartlı sistem, şifreli sistem, parmak izi tarama, kilitli dolapta tutma vb. yöntemler ile kontrol altında tutulur ve yetkisiz giriş ve çıkışların engellenmesi sağlanır.

4.7. Özel nitelikli kişisel verilerin aktarımında, aşağıda belirlenen aktarım yöntemleri uygulanır. Aktarım ancak özel nitelikli kişisel veri aktarmaya yetkili çalışanlar tarafından yapılır.

Aktarım yolu	**Aktarım yöntemi**
E-posta yoluyla aktarım	Şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılır.
Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarım	Kriptografik yöntemlerle şifrelenir ve kriptografik anahtar farklı ortamda tutulur
Farklı fiziksel ortamlardaki sunucular arasında aktarım	Sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımının gerçekleştirilir.
Kâğıt ortamı yoluyla aktarım	Verilerin evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı belirlenen önlemlere uyulur ve evrak "ÇOK GİZLİ" kaydıyla ilgiliye gönderilir.

4.8. Çalışanların özel nitelikli kişisel verilere dair tüm yetkileri (erişim ve varsa aktarım yetkisi dahil) görevlerinin sona erdiği an itibariyle kaldırılır. Bu kapsamda, erişimin sona erdirilmiş olduğuna, yetkilerin kaldırıldığına, fiziki ortamda tutulan evrakların yetkililere teslim edildiğine dair kayıtları tutulur ve bu kişilerin kullanımına verilen şirket envanterindeki her unsur geri alınır.

5. Diğer Güvenlik Önlemleri

Alınacak diğer güvenlik önlemleri "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası" ile "Kişisel Veri Saklama ve İmha Politikasında" belirlenmektedir.

6. Diğer Hukuki Düzenlemeler

Ayrıca, bu Politika'nın uygulanması açısından, Kişisel Verileri Koruma Kurumu'nun (Kurum) internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberi'nde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler başta olmak üzere, sektör uygulamaları, mesleki kurallar ve sair düzenlemeler de dikkate alınır.

Şirket, işbu Politika kapsamında, Kanun ve özel nitelikli kişisel verilere dair ilke kararının uygulanmasını sağlamak amacıyla gerekli denetimleri düzenli olarak yapar veya yaptırır.

7. İhlalin Bildirimi

Bir özel nitelikli kişisel verinin ihlal edilmesi halinde ve özel nitelikli kişisel veriler de dahil herhangi bir kişisel veri ihlali durumunda "Kriz Müdahale Dokümanı" süreci işletilir.

Kanun'un 12. maddesi uyarınca, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, Şirket bu durumu 72 saat içinde ilgilisine ve Kurul'a bildirmekle yükümlüdür.

8. Uygulama

8.1. Yayımlama : Bu Politika çalışanlara Veri Sorumlusu tarafından sunulacaktır.

8.2. Yürürlük Tarihi : Bu Politika yayımlandığı anda yürürlüğe girer.

8.3. Değişiklikler : Bu Politika'da gerçekleştirilecek değişikliklerin öncesinde, Veri Sorumlusu İrtibat Kişisi veya Veri Yetkilisi, Veri Sorumlusu'ndan talepte bulunabilir. Politika değişiklikleri Veri Sorumlusu tarafından yapılır.

9. Saklama

Veri Sorumlusu, bu Politika'yı yayınlamak ve saklamakla yükümlüdür. Her bölüm yöneticisi bu Politika'nın uygulanmasından sorumludur. Bu Politika'nın uygulanmasıyla ilgili olan sorular Veri Sorumlusu İrtibat Kişisi ve Veri Yetkilisi'ne yönlendirilmelidir.