

Hazırlayan	İnceleyen	Onaylayan
Kalite Yönetim Direktörü	Kalite Yönetim Direktörü	Başhekim

## 1.Amaç

Bu politikanın amacı, kişisel bir veri ihlali durumunda [Çevre Sağlık Tesisleri Ltd. Şti.] genelinde standart bir yönetim yaklaşımının uygulanmasını sağlamaktır.

Veri koruma, kişisel verilerin işlenmesiyle ilgili olarak bireylerin gizlilik haklarının güvenli bir şekilde korunmasını içerir. İnsanlar kendileri hakkında Çevre Sağlık Tesisleri Ltd. Şti.mize bilgi verirler. Veri koruma kanunu, “Veri sorumlusu” olarak bize ve bu kişisel verilere erişen, saklayan, kayıt eden veya kullanan tüm personele yükümlülükler getirir.

6698 sayılı KVKK’da belirtildiği gibi veri işleme prensipleri, verilerin aşağıdaki şekilde işlenmesini sağlar:

- İlgili kişi ilgili olarak yasal, adil ve şeffaf bir şekilde; (‘hukuki, adil ve şeffaflık’)
- Belirtilen, açık ve meşru amaçlarla toplanan kişisel veriler ve bu amaçlarla bağdaşmayan bir şekilde işlenemez; (‘Amaç sınırlaması’)
- İşlenecekleri amaçlarla ilgili olarak yeterli, ilgili ve sınırlı olan; (‘veri azaltılması’)
- Doğru ve gerektiğinde güncel tutulmalıdır. Hatalı olan kişisel verilerin, işlenecekleri amaçlara bakılmaksızın, gecikmeksizin silinmesi veya düzeltilmesi için her makul adımın atılması gerekir; (“doğruluk”)
- Kişisel verilerin işlendiği amaçlar için gerekli olandan daha uzun bir süre işlenmesi için ilgili kişilerin izni yazılı olarak tutulur; (“Saklama sınırlaması”)
- Uygun teknik veya idari önlemler; (‘dürüstlük ve gizlilik’) uygulanarak, yetkisiz veya yasa dışı işlemlere veya kazayla kayıp, tahribat veya hasara karşı kişisel bilgilerin güvenliğini sağlayacak şekilde işlenir.

## 2.Kapsam

Tüm çalışanları kapsamaktadır.

## 3.Tanımlar/Kısaltmalar

## 4. Sorumluluklar

### 4.1 Onay ve yürürlük

Bu prosedür Başhekim onayından sonra yürürlüğe girer.

### 4.2 Prosedürün Kullanıcıları

Tüm Çalışanlar sorumludur.

## 5.Prosedür:

### 5.1.Verİ İhlali nedir?

Bir ihlal, kasıtlı veya kasıtsız olarak tanımlanabilir. [Çevre Sağlık Tesisleri Ltd. Şti.]nın fiziksel ortamlarında, sistem veya sunucularında tutulan kişisel verilerin kasıtlı veya kasıtsız olarak, olası veya yetkisiz olarak ya da kaza ile ifşa edilmesi, yetkisiz erişimler, kişisel kayıp veya hırsızlık gibi durumlarla veri ihlali gerçekleşebilir.

### 5.2. İhlal veya şüpheli bir durum tespit edildiğinde ne yapılmalı?

#### • Sorunu hemen bildiriniz.

- Birim yöneticinize,
- Siz ve / veya birim yöneticiniz [telefon numarası] veya [e-posta adresi] 'de ki [KVKK Takım üyesi]' ne bildirimde bulunmalısınız. (Kişisel Verilerin Korunması Uyum Çalışma Ekibi Listesi'nde bulunan)

- Siz ve birim yöneticiniz bir Veri Koruma İhlali Olayı Raporunu tamamlamalı ve bunun taranmış bir kopyasını [**KVK Takım üyesi**] e-posta ile iletmelidir.

#### • İhlalin detayları

- ihlalin gerçekleştiği tarih ve saat
- İhlalin tespit edildiği tarih ve saat
- İhlali kimin bildirdiği
- ihlalin açıklaması
- Etkilenen herhangi bir BT sisteminin detayları
- Hata mesajları, kayıt dosyaları, vb. gibi ek kanıtlar

#### 5.3.İhlal yönetim planının dört ana unsuru vardır:

- A) Muhafaza ve İyileştirme
- B) Risk değerlendirmesi
- C) İhlal Bildirimi
- D) Değerlendirme ve Cevap

**A)Muhafaza ve İyileştirme:** İhlali fark ettiğinizde, siz ve / veya yöneticiniz veri / bilgi ihlalinin kapsamını ve etkisini sınırlandırmaya çalışmalısınız. [**KVK Takım üyesi**] veya birim yöneticiniz, ihlalin niteliğine bağlı olarak doğru süreci önerecektir.

Örneğin, kişisel veriler serbest bırakılmış veya yanlış bir yere gönderildiyse, pratik olarak en kısa zamanda gerekli önlemler alınmalıdır.

#### **Bir ihlal tespit edildikten ve bildirildikten sonra:**

- İhlal soruşturmasının başında kimin olacağına karar verin ve soruşturma için uygun kaynakların temin edildiğinden emin olun.
- [Çevre Sağlık Tesisleri Ltd. Şti.] 'da kimin ihlalden haberdar edilmesi gerektiğini ve veri saklama uygulamalarına yardımcı olmak için ne yapmaları gerektiği konusunda onları bilgilendirin.
- Örneğin bu, ağ güvenliği ihlal edilmiş bir bölüme erişimin kesilerek, kayıp bir dosya veya donanım parçasının bulunmasını veya sunucu odalarına erişim kodlarının vb. değiştirilmesini gerektirebilir.
- İhlalin neden olduğu hasarları sınırlandırmak ve kayıpları gidermek için yapılabilecek herhangi bir şey olup olmadığını belirleyin.

**B)Risk Değerlendirmesi:** [**Çevre Sağlık Tesisleri Ltd. Şti.**], güvenlik ihlalden kaynaklanan riski değerlendirecek, bireyler için potansiyel olumsuz sonuçların ne olabileceğini düşünecektir. Diğer bir ifadeyle, olumsuz sonuçların gerçekleşmesi olasılığının meydana gelme ihtimali ve ne kadar ciddi sonuçların doğurabileceğini belirleyecektir.

#### **Riskin değerlendirilmesinde aşağıdaki noktalar dikkate alınacaktır;**

- Ne tür Kişisel veriler yer alıyor?
- Kişisel veriler ne kadar hassas?
- Herhangi bir güvenlik mekanizması var mı (ör. Şifre, koruma, şifreleme)
- Kişisel veriler üçüncü bir kişiye/tarafa aktarılıyor mu?
- İhlalden kimler etkileniyor?

#### **C) İhlallerin Bildirilmesi**

##### **Kişisel Verileri Koruma Kurumuna**

1. Çevre Sağlık Tesisleri Ltd. Şti., Kişisel bir veri ihlali durumunda ilgili kişiler için bir risk bulunuyorsa, Kuruma mümkün olan en kısa zamanda aşağıdakileri yönergeyi takip ederek en geç 72 saat içinde bildirecektir:

- Mümkünse ilgili kişi ve kişisel veri kategorilerini ve ihlal edilen kayıtların sayısını ve kişisel veri ihlalinin niteliğini;
  - KVK Ekip lideri, KVK Takım üyesi veya daha fazla bilginin elde edilebileceği diğer irtibat kişilerinin adı ve iletişim bilgileri;
  - Muhtemel sonuçları;
  - Olası olumsuz etkileri azaltmak için önerilebilecek idari ve teknik tedbirler,
2. Eğer bunlar bir sebepten dolayı yapılamıyorsa uzmanlardan yardım isteyin.
3. İhlalin, [**Çevre Sağlık Tesisleri Ltd. Şti.**] adına başka bir organizasyon için işlediği verilerle ilgili olması durumunda, yapmamız gereken tek şey, ihlalin farkına vardıktan sonra gereksiz bir gecikme olmaksızın diğer kuruluşa bildirimde bulunmaktır.
4. Bilgiyi aynı anda vermenin mümkün olmadığı yerde, bilgiler gecikme olmadan aşamalar halinde sağlanabilir.
5. Veri Koruma İhlal Olayı ile ilgili yapılan her şeyin kaydını tutun.

### **Veri Konusu Kişi Grubuna / İlgili Kişilere**

Bir olayın kişisel verilerin yetkisiz bir şekilde ifşa edilmesi, kaybolması, imha edilmesi veya değiştirilmesi veri güvenliği riskine yol açması durumunda, manuel veya elektronik formda, [**Çevre Sağlık Tesisleri Ltd. Şti.**] etkilenen kişilere bilgi verecektir.

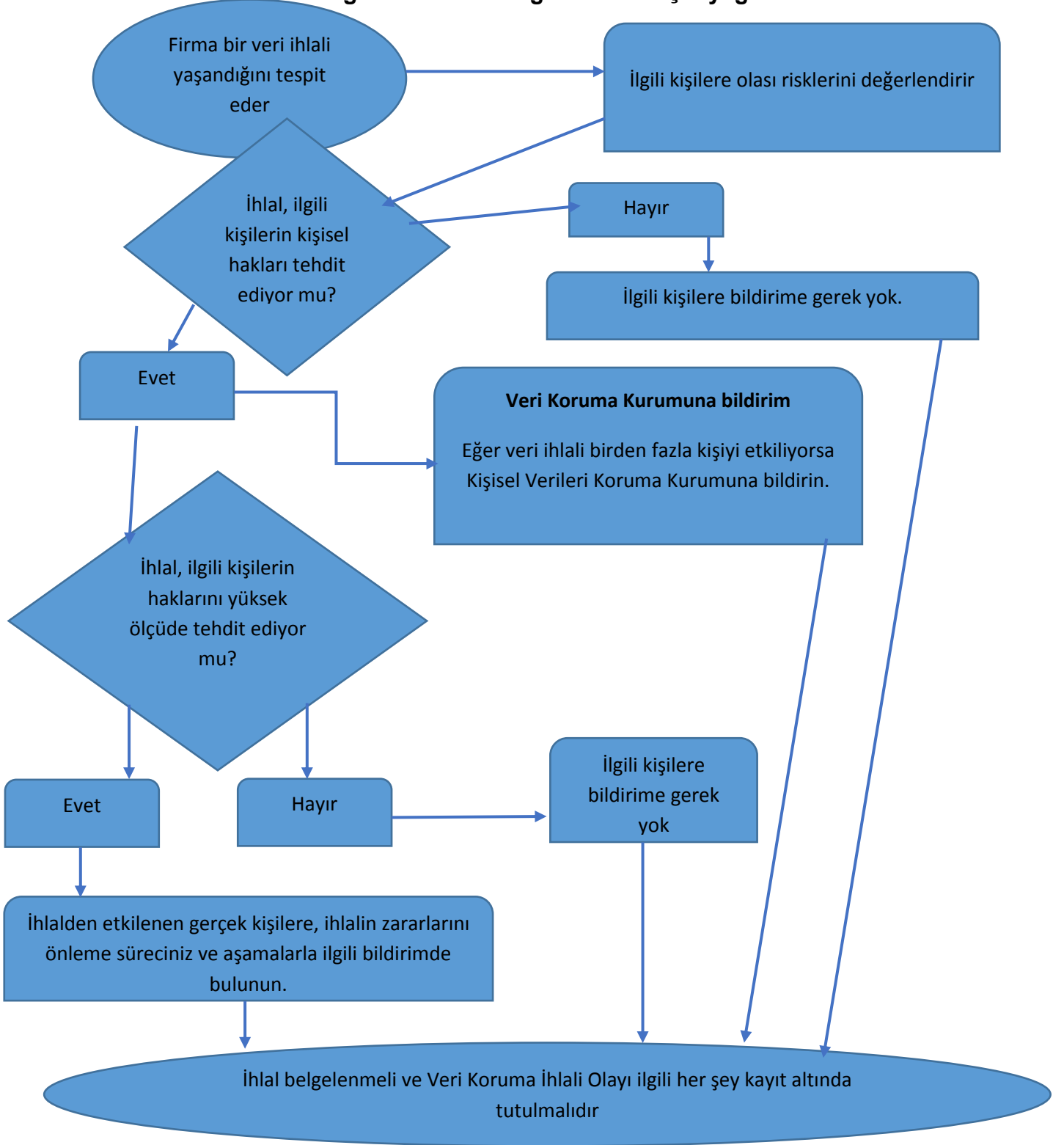
### **Veri Konusu Kişi Grubuna / İlgili Kişilere Zorunlu Bildirim**

- İhlalin bir kişi veya bireyler için yüksek risk oluşturması muhtemel ise, **Çevre Sağlık Tesisleri Ltd. Şti.** bu durumu ilgili kişilere gecikme olmaksızın aşağıdaki yönergeyi takip ederek iletmelidir,
  - açık ve sade dilde ihlalin niteliği;
  - Veri Koruma Yetkilisinin; KVK Ekip lideri veya daha fazla bilginin elde edilebileceği diğer irtibat Kişisinin; KVK Takım üyesinin adı ve iletişim bilgileri;
  - ihlalin olası sonuçları;
  - Veri Sorumlusu tarafından, kişisel veri ihlalinin önlemek ya dolası olumsuz etkileri azaltmak için alınan önlemler, Teknik ve idari koruma tedbirleri sayesinde, ihlal edilen veriler şifreleniyse veya maskeleyme işlemi yapıldıysa veya ihlalden sonra ilgili kişilerin zarar görme ihtimalini ortadan kaldıran önlemler alındıysa Yukarıdakiler Gerekli DEĞİLDİR.

Veri İhlalini ilgili kişilere tek tek bildirmek çok fazla çaba veya zaman gerektiriyorsa, bunun yerine kamuya açık bir duyuru yapabiliriz. Bu üst yönetim ile istişare olmadan yapılmamalıdır.

Veri Koruma Kurumu, ilgili kişilere bildirim yapılmasını veya yukarıdaki şartları karşılamamızı talep edebilir.

## Bildirim gereksinimlerini gösteren akış diyagramı



**D)Değerlendirme ve Yanıt:** Raporlama gerekliliklerinden bağımsız olarak [**Çevre Sağlık Tesisleri Ltd. Şti.**], herhangi bir kişisel veri güvenliği ihlalinin ardından, olayla ilgili kapsamlı bir inceleme yapar.

Bu incelemenin amacı, olay sırasında atılan adımların uygun olmasını ve iyileştirilmesi gerekebilecek alanları tespit etmektir.

[Çevre Sağlık Tesisleri Ltd. Şti.], aşağıdaki unsurları dikkatli bir şekilde ele alarak olayları inceleyerek raporu tamamlayacak olan Çevre Sağlık Tesisleri Ltd. Şti. içindeki kişileri tanımlayacaktır:

- Ele geçirilen kişisel verilerin miktarı ve niteliği;
- Ele geçirilen kişisel verileri güvenceye almak ve / veya kurtarmak için alınan önlem/eylem;
- olaydan etkilenenleri bilgilendirmek için yapılan eylemler;
- Olaydan etkilenen kişilere verilen zararı veya sıkıntıyı azaltmak için alınan eylemler;
- Kişisel verilerin kontrolünü kaybına yol açan olayların bir kronolojisi;
- Olayın tekrarlanmasını önlemek için alınan tedbirler.

#### 5.4. Veri Koruma İhlal Olay Raporu

Tüm veri koruma olayları veya şüpheli girişler, telefonla ve / veya e-posta adresiyle [Görevlendirilmiş KVK Ekip lideri]'ne iletilir.

Lütfen bu olay ile bağlantılı olarak hazırlanan e-postaların veya diğer belgelerin Özel ve Gizli olduğuna dikkat ediniz. Bu belgelerin dolaşımı, olayı soruşturmaya doğrudan katılanlarla sınırlandırılmalıdır. Bu Olay Raporunda HERHANGİ BİR VERİ KONUSU kişi grubunun ADINI REFERANS VERMEYİN.

Raporun kim [Ad, Ünvan] tarafından derlendiği		
Bölüm ve İletişim Bilgileri		
Olayın tespit edildiği tarih		
Olayın yaşandığı tarih(belirlenebilmişse)		
Kim tarafından bildirildi		
Kime raporlandı		
Olayın raporlama tarihi		
Etkilenen kişi sayısı		
<b>Olayın Detayı</b>		
<b>Bildirim</b>	<b>Evet/Hayır</b>	<b>Yapılmadıysa Neden</b>
Kişisel Verileri Koruma Kuruluna		
İlgili Kişiye		
<b>Olayın zararlarını azaltmak, verileri kurtarmak için alınan önlemler (Varsa)</b>		
<b>Değerlendirme ve Yanıt</b>		
<b>Tarih</b>		
<b>Ad-Soyad</b>		
<b>İmza</b>		

#### 6.İlgili Dokümanlar :

YÖN.LS.34 Kişisel Verilerin Korunması Uyum Çalışma Ekibi Listesi