VERİ İHLALİ KİŞİSEL MÜDAHALE PLANI

1. GİRİŞ, DAYANAK VE AMAÇ

Kişisel Verilerin Korunması Kanunu'nun (Kanun/KVKK) 12. maddesinin 5. fıkrasına göre **Egenur Bakıner Yücebilgiç,** kendisi tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kuruluna (Kurul) bildirmekle yükümlüdür.

İşbu "Kişisel Veri İhlali Müdahale Planı" (Plan), 24.01.2019 Tarih ve 2019/10 Sayılı Kişisel Verileri Koruma Kurulu kararı (Karar) uyarınca hazırlanmıştır. Bu Plan hazırlanırken; kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, kişisel veri ihlali olması durumunda oluşacak krize nasıl müdahale edileceği ve atılacak adımların neler olduğu konusunda çalışanları bilgilendirmek ve veri sorumlusunun müdahale sürecini belirlemek amaçlanmıştır.

2. KİŞİSEL VERİ İHLALİ

Kişisel veri ihlali; iletilen, saklanan veya sair şekilde işlenen kişisel verilerin kazara veya hukuka aykırı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik açığı şekillerinde ortaya çıkabilen ihlallerdir.

Aşağıda yer alan durumlar genel olarak kişisel veri ihlali olarak nitelendirilir:

- Gizli bilgilerin hukuka aykırı şekilde ifşası,
- Kişisel veri içeren e-postaların yanlışlıkla Klinik dışında ilgisiz kişilere iletilmesi, gönderimi,
- Bilgi işlem donanımlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin siber saldırı) gerçekleşmesi suretiyle kişiselverilere hukuka aykırı erişim sağlanması,
- Kişisel veri içeren fiziki dokümanların veya elektronik cihazların çalınması veya kaybolması,
- Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi.

Yukarıda belirtilen durumlar örnek mahiyetindedir. Bu tip veya benzer durumlarda bu Plan'da belirtilen şekilde hareket edilmelidir.

3. İHLAL MÜDAHALE TİMİ

Kişisel veri ihlali durumunda oluşan veya oluşabilecek kriz durumuna müdahale etmek ve KVKK kapsamında öngörülen yükümlülükleri yerine getirmek için irtibat kişisinin veri sorumlusu Egenur Bakıner Yücebilgiç'den farklı bir gerçek kişi olması halinde irtibat kişisine bildirim yapılır, bu bildirimin ardından irtibat kişisi tarafından **"acil"**

koduyla ilgili ihlalin meydana geldiği birim toplantıya çağrılır.

4. İHLAL MÜDAHALE SÜRECİ

Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin işbu planın 1. bölümünde belirtilen Karar uyarınca, Egenur Bakıner Yücebilgiç'in kişisel veri ihlalini öğrendiği tarihten itibaren **gecikmeksizin ve en geç 72 saat içinde** ihlali Kurul'a bildirmesi ve veri ihlalinden etkilenen kişilerin belirlenmesinimüteakip ilgili kişilere de **makul olan en kısa süre içerisinde** ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan,
Ulaşılamıyorsa Kliniğin kendi internet sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması gerekmektedir.

Söz konusu yükümlülüklerin yerine getirilebilmesi için, bir veri ihlali durumunda öncelikle Klinik içerisinde belirli adımlar takip edilecektir:

a) İhlale ilişkin ön değerlendirme,

b) Önleme ve kurtarma çalışmalarının yürütülmesi,

c) Risklerin değerlendirilmesi,

d) Bildirim,

e) İhlal sonrası durum tespiti ve iyileştirme çalışmaları.

4.1 İhlale İlişkin Ön Değerlendirme

Klinik nezdinde gerçek veya potansiyel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar Veri Sorumlusu İrtibat Kişisi'ne derhal ve gecikmeksizin durumu bildirmekle yükümlüdür. Bu kapsamda ilgili çalışan veya yöneticisi aşağıdaki hususları içerir bir rapor hazırlayarak, veri ihlalini Veri Sorumlusu ve İrtibat Kişisi'ne bildirir. Bu bildirimde;

- Kişisel veri ihlalinin gerçekleşme tarihi ve saati,
- Kişisel veri ihlalinin tespit edildiği tarih ve saat,
- Kişisel veri ihlali olayına ilişkin açıklamalar,
- Eğer biliniyorsa kişisel veri ihlalinden etkilenen kişi ve veri sayısı,
- Kişisel veri ihlalinin tespit edildiği tarihte varsa atılan adımlara, alınan önlemlere ilişkin açıklamalar,
- Raporu hazırlayan çalışanın/çalışanların adı soyadı, iletişim bilgileri ve rapor tarihi bilgileri yer almalıdır.

Veri Sorumlusu İrtibat Kişisi, rapor kapsamında belirtilen hususları dikkate alarak bir ön değerlendirme yapar. Bu değerlendirmeyi yaparken, gerçekten bir veri ihlalinin söz konusu olup olmadığını, ihlalin kapsamını, oluşabilecek etkilerini de göz önünde bulundurarak, veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

4.2 Önleme ve Kurtarma Çalışmalarının Yürütülmesi

Veri ihlalinin klinik ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için önleme ve kurtarma çalışmaları veri sorumlusu gözetiminde yürütülür. Bu kapsamda öncelikle veri ihlalinden haberdar edilmesi gereken birimler tespit edilir ve bu kişilere ihlalin kontrol edilebilmesi, mümkünse engellenebilmesi ve zararların azaltılabilmesi için atılması gereken adımlara ilişkin rehberlik edilir.

Akabinde veri ihlalinden etkilenecek kişilerin ve veri türlerinin neler olduğu tespit edilmeye çalışılır ve varsa bu kişilerin iletişim bilgileri de belirlenir. Eş zamanlı olarak, veri ihlali nedeniyle haberdar edilmesi gereken başka kurum ya da kuruluşlar olup olmadığı değerlendirilir.

4.3 Risklerin değerlendirilmesi

Kişisel veri ihlalleri, ilgili kişiler adına verilerinin Türk Ceza Kanunu kapsamında düzenlenen suçlara alet edilmesi gibi birçok olumsuz etki oluşturabilir. Bu nedenle ihlalin mevcut ve muhtemel sonuçlarının ilgili kişiler üzerinde ne gibi etkiler oluşturabileceğinin dikkatli bir şekilde değerlendirilmesi ve risklerin ortaya koyulması çok önemlidir.

Veri sorumlusu tarafından riskler değerlendirilirken, ihlalden etkilenen kişisel verilerin niteliği, hassasiyeti ve miktarı ile etkilenen bireylerin sayısı ve kişi gruplarının kimler olduğu, veri ihlalinin Klinik'in faaliyetleri ile itibarına olan etkisi, veri ihlalinin etkisinin azaltılmasında alınan önlemler ve ihlalin olası sonuçları ayrı ayrı ele alınmalıdır. Bunların sonucuna göre veri ihlalleri aşağıdaki şekilde sınıflandırılabilir.

- **1. Kademede İhlal:** İhlalin yarattığı etkiler, ilgili kişiler üzerinde kişisel verilerinin hukuka aykırı olarak elde edilmesi dışında somut birzarara neden olmamaktadır.
- **2. Kademede İhlal:** İhlal ilgili kişiler üzerinde olumsuz etkilere neden olabilecek niteliktedir. Ancak ihlalden etkilenen veri sayısı, çeşidi veboyutu düşünüldüğünde bu etki büyük değildir.
- **3. Kademede İhlal:** İhlal boyutu, niteliği, etkili olduğu kişisel verilerin türü, sayısı gibi etmenler değerlendirildiğinde ihlalden etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere ve somut zararlara neden olabilecek seviyededir.

Kişisel Verileri Koruma Kurumu'na göre: "Gerçekleşen veri ihlalinin düzeyinin belirlenmesinde ilgili kişiler üzerinde ne kadar bir potansiyel etkiye neden olduğunun değerlendirilmesi gerekmektedir. Söz konusu potansiyel etkinin değerlendirilmesinde ise ihlalin niteliği, ihlalin nedeni, ihlale maruz kalan verinin türü, ihlalin etkisinin azaltılmasında alınan önlemler ile ihlalden etkilenen ilgili kişi kategorileri göz önünde bulundurulmalıdır."

2. ve 3. kademedeki ihlallere ilişkin veri sorumlusu üst yönetimine bilgi verilir. İhlalin 3. kademede olduğunun değerlendirildiği durumlarda bubildirim hiç gecikmeksizin yapılır.

* Kişilerin sadece ad soyad bilgilerinin yer aldığı bir katılım listesinin yetkisiz kişiler tarafından görülmesi durumunda **1. kademede ihlal olduğu** değerlendirilebilir.

İhlalin ilgili kişiler üzerinde olumsuz etkileri bulunması ancak etkisinin büyük olmaması **2. kademede ihlal** kabul edilebilir. Örneğin ilgili kişilerinönemli olarak değerlendirilebilecek verilerinin ihlale maruz kaldığı bir olayda veri sorumlusunun ihlal akabinde aldığı güvenlik tedbirleri ile ihlalin etkilerinin önemli ölçüde azaltmış olması bu kademeye örnek verilebilir.

Özellikle ihlalden etkilenen kişilerin ve/veya kayıtların sayısal olarak çok olması, ihlale konu verilerin içerisinde özel nitelikli veriler olması ya dakredi kartı bilgileri gibi kişilerin önemli bilgilerinin yer alması durumunda ihlalin yüksek düzeyde risk taşıdığı ve **3. kademede ihlal** olduğu değerlendirilebilir.

Ancak Kurum'un risk değerlendirmesi konusu hakkındaki açıklamaları ve kararları takip edilmelidir.

5. BİLDİRİM

Veri ihlalinin gerek hukuki yükümlülük kapsamında gerekse veri ihlaline ilişkin tedbir alınması, ihlalin olası etkilerinin azaltılması gibi amaçlarlaŞirket dışında üçüncü kişilere bildirilmesi gerekmektedir.

5.1 Kurul'a Bildirim

Veri Sorumlusu İrtibat Kişisi, öncelikle **kişisel veri ihlalinden haberdar olduğu andan itibaren gecikmeksizin ve en geç 72 saat içerisinde** Kurul'a bu durumu bildirmekle yükümlüdür. Bu nedenle, Klinik içerisinde tüm çalışanların herhangi bir veri ihlali durumunu vakit kaybetmeksizin Veri Sorumlusu İrtibat Kişisi'ne bildirmesi, Klinik'in herhangi bir yaptırımla karşı karşıya kalmaması için önem arz etmektedir.

Kurul'a yapılacak bildirimde Kişisel Verileri Koruma Kurumu'nun (Kurum) internet sitesinde yayınlanmış olan Kişisel Veri İhlali Başvuru Formukullanılır. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak sağlanabilir.

Haklı bir gerekçe ile 72 saat içerisinde Kurul'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenleri de Kurul'aaçıklanır

5.2 İhlalden Etkilenen Kişilere Bildirim

Klinik, kişisel veri ihlalinden etkilen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişimadresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa uygun yöntemlerle (örneğin internet sitesi üzerinden duruma ilişkin bir duyuru yayınlanması) bildirim yapmalıdır. Söz konusu bildirimler, yetkilendirilmiş personelin desteğiyle Veri Sorumlusu İrtibat Kişisitarafından gerçekleştirilir.

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı uyarınca Klinik tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması veasgari olarak aşağıdaki unsurları içermesi gerekir:

- İhlalin ne zaman gerçekleştiği,
- Kişisel veri kategorileri bazında (kişisel veri/özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
- Kişisel veri ihlalinin olası sonuçları,
- Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,
- İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun internet sayfasının tam adresi, çağrı merkezi vb. iletişim yolları unsurlarına yer verilmesi.

5.3 Diğer Bildirimler

Klinik'in hukuken yapması zorunlu olan bildirimlerin yanı sıra, veri ihlalinin niteliği, büyüklüğü, ihlalin suç teşkil edip etmediği gibi hususlar göz önünde bulundurularak üçüncü kişilere de bildirim yapılması gerekebilir. Bu kişiler, diğer veri sorumluları ya da veri işleyenler, tedarikçiler, adli makamlar, noterler, bankalar olabilir. Veri sorumlusu, böyle bir gereklilik olup olmadığını ayrıca değerlendirir ve gerekli ise bildirimleri yapar.

5.4 İhlal Sonrası Durum Tespiti ve İyileştirme Çalışmaları

Klinik tarafından kişisel veri ihlallerine ilişkin tüm bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurul'un incelemesine hazır halde bulundurulması gerekmektedir. Veri Sorumlusu İrtibat Kişisi, veri ihlaline ilişkin atılan adımların uygun olup olmadığını ve olası bir veri ihlalinde geliştirilebilecek/ iyileştirilebilecek hususların neler olabileceğini belirlemek adına bir değerlendirme yapar. Bu kapsamda aşağıdaki unsurları içerir bir değerlendirme ve iyileştirme raporu hazırlanır.

- Somut olay kapsamında yapılan işlemler,
- Veri ihlalinin çıkış noktasının tespit edilip, zaafın giderilmesi adına yapılan faaliyetler ve zaaf noktasında ilave tedbir gerekip gerekmediği,
- Olası kişisel veri ihlallerinin etkilerini azaltmak için hangi adımların atılması gerektiği
- Kişisel veri ihlali nedeniyle herhangi bir politika, Plan ya da raporlamada iyileştirme gerekip gerekmediği
- Kişisel veri ihlalinin tekrarlanmasını önleyebilmek için ek idari ve/veya teknik tedbirlerin alınmasının gerekli olup olmadığı,
- İhlallere maruz kalmayı ve maliyet etkilerini azaltmak için kaynaklara/altyapıya ek yatırım yapılmasının gerekli olup olmadığı,
- İhlalin tekrarlanmasını önleyecek bir personel farkındalık eğitimi gerekliliği,

6. KVKK UYUM SÜRECİNİN BÜTÜNLÜĞÜ

Bu Plan, veri sorumlusu adına kişisel verilerin korunması ve işlemesine ilişkin yürürlüğe konmuş diğer politika ve metinlerden bağımsız düşünülemez. Tüm dokümanlar bir bütünün ayrılmaz parçaları olarak düşünülüp süreç ve ihlal

sonrası adımlar buna göre yönetilmelidir.

7. SORUMLULUK

Planın uygulanmasından veri sorumlusu tüm organizasyonu ile birlikte sorumludur. Bir başka ifade ile tüm çalışanlar Planın uygulanması ile yükümlüdür. Plana aykırı hareket eden çalışanlar hakkında disiplin hükümleri doğrultusunda disiplin soruşturması yürütülür.

8. GÜNCELLEME

Bu Plan yılda bir kez rutin olarak gözden geçirilir ve kayıt altına alınır. Mevzuatta meydana gelen değişiklikler derhal Plana işlenir. Mevzuattaki değişikliklerin uygulanması için, değişikliğin Plana eklenmesi beklenmez, mevzuata uygun hareket tarzı ne ise güncelleme yapılana dek o yol takip edilir.

9. YÜRÜRLÜK TARİHİ

İş bu plan, klinik yetkilisince imza edilmesinin ve internet sitesinde yayımlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, politikanın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile merkezimiz tarafından saklanır.