TRIVE PORTFÖY YÖNETİMİ A.Ş.

KİŞİSEL VERİLERİN İHLALİ, MÜDAHALE VE KRİZ YÖNETİMİ PROSEDÜRÜ

06/02/2024 V.03

İÇİNDEKİLER

A. AMAÇ

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("KVKK") 12. maddesinin 5. fıkrasına göre TRIVE PORTFÖY YÖNETİMİ A.Ş. **("Şirket")** veri sorumlusu olarak, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durumu en kısa sürede (en geç 72 saat içerisinde) ilgilisine ve Kişisel Verileri Koruma Kurulu'na ("Kurul") bildirmekle yükümlüdür. İşbu Kişisel Veri İhlali Müdahale Prosedürü ("Prosedür"), kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde diğer bir deyişle, kişisel veri ihlali olması durumunda oluşacak krize nasıl müdahale edileceği ve atılacak adımların neler olduğu konusunda çalışanları bilgilendirmek amacıyla hazırlanmıştır. Şirket'in tüm çalışanları Prosedür'ün uygulanmasından sorumludur.

B. KİŞİSEL VERİ İHLALİ VE ŞİRKETİN SORUMLULUKLARI

Kişisel veri ihlali, kişisel verilerin kanuna aykırı bir şekilde elde edilmesi, hukuka aykırı bir şekilde kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin yanlışlıkla/kasten yetkisiz kişilere açıklanması, kişisel verilerin hukuka aykırı bir şekilde silinmesi, değiştirilmesi veya bütünlüğünün bozulması gibi durumlarda ortaya çıkmaktadır. Aşağıda yer alan durumlar genel olarak kişisel veri ihlali olarak değerlendirilir:

▪ Kişisel veri içeren fiziki dokümanların veya elektronik cihazların çalınması veya kaybolması,

▪ Kişisel veri içeren elektronik belgelerin, donanım veya yazılımlar aracılığıyla şirket dışına çıkarılması,

▪ Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi,

▪Gizli bilgilerin hukuka aykırı şekilde ifşası,

▪ Kişisel veri ve/veya gizli bilgi içeren e-postaların yanlışlıkla şirket dışında ilgisiz kişilere gönderimi,

▪ IT ekipmanlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin; siber saldırı) gerçekleşmesi suretiyle kişisel verilere hukuka aykırı erişim sağlanması.

C. MÜDAHALE EKİBİ

Kişisel veri ihlali durumunda oluşan veya oluşabilecek kriz durumuna müdahale etmek ve KVKK kapsamındaki yükümlülükleri yerine getirmek için belirlenen personellerden arasından Veri Koruma Görevlisi (bir üst düzey şirket yetkilisi) ve Veri Koruma Görevlisi İrtibat

kişisinden (iç kontrolden sorumlu personel) oluşan bir Kriz Müdahale Ekibi ("Ekip") oluşturulmuştur. Ekip iş bu prosedürün uygulanmasından ve güncellenmesinden sorumludur.

D. VERİ İHLALİ DURUMUNDA YAPILACAKLAR

Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun Kararı ("Karar") uyarınca, Şirket'in kişisel veri ihlalini öğrendiği tarihten itibaren gecikmeksizin ve en geç yetmiş iki (72) saat içinde Kurul'a bildirmesi ve veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa Şirket'in kendi internet sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması gerekmektedir. Söz konusu yükümlülüklerin yerine getirilebilmesi için, bir veri ihlali durumunda öncelikle şirket içerisinde belirli adımlar takip edilmelidir:

I. Krize ilişkin ön değerlendirme,
II. Engelleme ve kurtarma çalışmalarının yürütülmesi,
III. Risklerin değerlendirilmesi,
IV. Bildirim,
V. Değerlendirme ve İyileştirme.

I. Krize İlişkin Ön Değerlendirme

Şirket nezdinde gerçek veya potansiyel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar Veri Koruma Görevlilerine derhal ve gecikmeksizin öğrendiği andan en geç 1 saat içinde durumu hem info@triveportfoy.com.tr mail adresine bildirmekle yükümlüdür. Bu kapsamda ilgili çalışan aşağıdaki hususları içerir bir rapor hazırlayarak, veri ihlalini Veri Koruma Görevlilerine ve Müdahale Ekibine bildirir:

- Kişisel veri ihlalinin gerçekleşme tarihi ve saati,
- Kişisel veri ihlalinin tespiti tarihi ve saati,
- Kişisel veri ihlali olayına ilişkin açıklamalar,
- Eğer biliniyorsa kişisel veri ihlalinden etkilenen kişi ve kayıt 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.

Veri Koruma Görevlileri, 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, Ekip ile birlikte veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

II. Engelleme ve Kurtarma Çalışmalarının Yürütülmesi

Veri ihlalinin, Şirket ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için engelleme ve kurtarma çalışmaları ekibin 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 kayıtların 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.

III. Risklerin Değerlendirilmesi

Kişisel veri ihlalleri, ihlalden etkilenen kişiler üzerinde kimlik hırsızlığı, hakların kısıtlanması dolandırıcılık, finansal kayıp, itibar kaybı, kişisel verilerin güvenliğinin kaybı, ayrımcılık gibi birçok olumsuz etki oluşturabilir. Bu nedenle kişisel veri ihlalinin olası sonuçlarının Şirket ve ihlalden etkilenen kişiler üzerinde ne gibi etkiler oluşturabileceğinin dikkatli bir şekilde değerlendirilmesi ve risklerin ortaya koyulması çok önemlidir. Ekip tarafından riskler değerlendirilirken, ihlalden etkilenen kişisel verilerin niteliği, hassasiyeti ve hacmi ile etkilenen bireylerin sayısı ve kişi gruplarının kimler olduğu, veri ihlalinin Şirket'in faaliyetleri ile itibarına olan etkisi, veri ihlalinin etkisinin azaltılmasında alınan önlemler ve ihlalin olası sonuçları ayrı ayrı ele alınmalıdır. Bunların sonucuna göre veri ihlali "düşük düzeyde, orta düzeyde veya yüksek düzeyde risk" olarak nitelendirilir:

- **Düşük düzeyde risk**: İhlal ilgili kişiler üzerinde olumsuz herhangi bir etkiye neden olmamakta ya da bu etki ihmal edilebilir düzeyde kalmaktadır.
- **Orta düzeyde risk:** İhlal ilgili kişiler üzerinde olumsuz etkilere neden olabilir fakat bu etki büyük değildir.
- **Yüksek düzeyde risk:** İhlal etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere neden olmaktadır. Orta ve özellikle yüksek düzeyde risk olarak tanımlanan veri ihlallerine ilişkin veri sorumlusu üst yönetimine Ekip tarafından bilgi verilir.

IV. Bildirim

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

a. **Kurul'a Bildirim**: Veri Koruma Görevlileri ve ekip, öncelikle kişisel veri ihlalinden haberdar olduğu andan itibaren gecikmeksizin ve en geç yetmiş iki (72) saat içerisinde Kurul'a bu durumu bildirmekle yükümlüdür. Bu nedenle, Şirket içerisinde oluşmuş olan tüm veri ihlallerinin Veri Koruma Görevlilerine derhal ve gecikmesizin bildirilmesi, Şirket'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 Formu kullanılır. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı

hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak sağlanabilir. Haklı bir gerekçe ile yetmiş iki (72) saat içerisinde Kurul'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenleri de Kurul'a açıklanır.

b. **İhlalden Etkilenen Kişilere Bildirim:** Şirket, kişisel veri ihlalinden etkilen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa uygun yöntemlerle (örneğin internet sitesi üzerinden duruma ilişkin bir duyuru yayınlanması) bildirim yapmalıdır. Söz konusu bildirimler, Ekibin desteğiyle Veri Koruma Görevlileri tarafından gerçekleştirilir. Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, Kurul'un 18.09.2019 tarih ve 2019/271 sayılı Kararı uyarınca Şirket tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak aşağıdaki unsurları içermesi gerekir:

    - İhlalinin 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.

c. **Diğer Bildirimler**: Şirket'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, dış danışmanlar, adli makamlar, bankalar olabilir. Ekip, böyle bir gereklilik olup olmadığını ayrıca değerlendirir ve gerekli ise bildirimleri yapar.

V. Değerlendirme ve İyileştirme

Şirket tarafından kişisel veri ihlallerine ilişkin tüm bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurul'un incelemesine hazır halde bulundurulması gerekmektedir. Veri Koruma Görevlileri ve Ekip, 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 Ekip, aşağıdaki unsurları içerir bir değerlendirme ve iyileştirme raporu hazırlar ve bu rapor Müdahale Ekip tarafından en kısa sürede ve en geç 5 gün içinde şirket üst yönetimine sunulur:

- Olası kişisel veri ihlallerinin etkilerini azaltmak için hangi adımların atılması gerektiği
- Kişisel veri ihlali nedeniyle herhangi bir politika, prosedür ya da raporlamada iyileştirme gerekip gerekmediği
- Kişisel veri ihlalinin tekrarlanmasını önleyebilmek için ek bir idari ve/veya teknik tedbir alınmasının gerekli olup olmadığı,
- İhlalin tekrarlanmasını önleyecek bir personel farkındalık eğitimi gerekliliği,
- İhlallere maruz kalmayı ve maliyet etkilerini azaltmak için kaynaklara/altyapıya ek yatırım yapılmasının gerekli olup olmadığı

E. PROSEDÜRÜN UYGULANMASI VE GÜNCELLENMESİ

Bu Prosedür, Şirket nezdinde kişisel verilerin korunması ve işlemesine ilişkin yürürlüğe konmuş tüm politika ve prosedürler ile birlikte ele alınır. İşbu Prosedür kurumsal ya da yasal kaynaklı içeriklerindeki değişiklik gereksinimlerine bakılmaksızın gerektiğinde ve en geç 1 yıl içinde gözden geçirilerek ve ihtiyaç halinde güncellenecektir. Prosedür henüz güncellenmemiş olsa bile, mevzuatta meydana gelen değişiklikler derhal uygulanacaktır.