Kişisel Veri İhlali Müdahale Planı

1. Amaç

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 12. maddesinin 5. fıkrasına göre XXX(Şirket) 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), 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.

2. Sorumluluk

Planın uygulanmasından tüm çalışanlar sorumludur. Plana aykırı hareket eden çalışanlar Disiplin Yönetmeliği hükümlerine tabi olacaktır.

3. Kişisel Veri İhlali

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

Yukarıda belirtilen veya benzer durumlarda bu Plan'da belirtilen şekilde hareket edilmelidir.

4. Kriz Müdahale Ekibi

Kişisel veri ihlali durumunda oluşan veya oluşabilecek kriz durumuna müdahale etmek ve Kanun kapsamında öngörülen yükümlülükleri yerine getirmek için irtibat kişisine bildirim yapılır, bu bildirimin ardından irtibat kişisi tarafından **"acil"** koduyla KVKK Komisyonu toplantıya çağrılır. Toplantıya KVKK Komisyon üyelerinin yanı sıra veri ihlalinin meydana geldiği birimin yöneticisi de katılır.

5. Kriz Müdahale Süreci

Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun 24.01.2019 Tarih ve 2019/10 Sayılı Kararı (Karar) uyarınca, Şirket'nin kişisel veri ihlalini öğrendiği tarihten itibaren **gecikmeksizin ve en geç 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:

- Krize ilişkin ön değerlendirme,
- Engelleme ve kurtarma çalışmalarının yürütülmesi,
- Risklerin değerlendirilmesi,
- Bildirim,
- İyileştirme Çalışmaları.

5.1. Krize İlişkin Ön Değerlendirme

Şirket 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 aşağıdaki hususları içerir bir rapor hazırlayarak, veri ihlalini Veri Sorumlusu İrtibat Kişisi'ne 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 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, KVKK Komisyonu ile birlikte veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

5.2. Engelleme ve Kurtarma Çalışmalarının Yürütülmesi

Veri ihlalinin Şirket ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için engelleme ve kurtarma çalışmaları KVKK Komisyonunun 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.[1]

5.3. 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.

KVKK Komisyonu tarafından riskler değerlendirilirken, ihlalden etkilenen kişisel verilerin niteliği, hassasiyeti ve miktarı ile etkilenen bireylerin sayısı ve kişi gruplarının kimler olduğu, veri ihlalinin Şirket'nin 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:

[1] [1] Örneğin bir siber saldırı nedeniyle savcılığa başvuruda bulunulması gerekebilir.

- **Düşük düzeyde risk:** İhlal, ilgili kişiler üzerinde olumsuz herhangi bir etkiye neden olmamaktadır.
- **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.[2]

Orta ve özellikle yüksek düzeyde risk olarak tanımlanan veri ihlallerine ilişkin Veri Sorumlusu Üst Yönetimi'ne KVKK Komisyonu tarafından bilgi verilir.

** Kişilerin sadece ad soyad bilgilerinin yer aldığı bir katılım listesinin ihlale konu olması durumunda **düşük düzeyde risk** taşıdığı değerlendirilebilir.*

*İhlalin ilgili kişiler üzerinde olumsuz etkileri bulunması ancak etkisinin büyük olmaması **orta düzeyde risk** kabul edilebilir. Her ne kadar kişilerin önemli bilgileri ihlale konu olsa da, veri sorumlusunun ihlal akabinde aldığını güvenlik tedbirleri ile ihlalin etkilerinin önemli ölçüde azaltmış olması bu risk türüne örnek verilebilir.*

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

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

5.4. 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.

5.4.1. 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, Şirket içerisinde tüm çalışanların herhangi bir veri ihlali durumunu vakit kaybetmeksizin Veri Sorumlusu İrtibat Kişisi'ne bildirmesi, 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[3] kullanılır. 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'a açıklanır.

5.4.2. 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, KVKK Komisyonunun desteğiyle Veri Sorumlusu İrtibat Kişisi tarafından

---

[1] [2] 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] [3]Başvuru formuna şu adresten ulaşılabilir : https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/617f166c-24e1-42b5-a9cb-d756d6443af9.pdf

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 Şirket tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari 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.

5.4.3. Diğer Bildirimler

Şirket'nin 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. KVKK Komisyonu, böyle bir gereklilik olup olmadığını ayrıca değerlendirir ve gerekli ise bildirimleri yapar.

5.5. 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 Sorumlusu İrtibat Kişisi ve KVKK Komisyonu, 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 KVKK Komisyonu, aşağıdaki unsurları içerir bir değerlendirme ve iyileştirme raporu hazırlar.

- 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,
- İhlalin tekrarlanmasını önleyecek bir personel farkındalık eğitimi gerekliliği,
- İhlallere maruz kalmayı ve maliyet etkilerini azaltmak için kaynaklara/altyapıya ek yatırım yapılmasının gerekli olup olmadığı

6. İlgili Politika Ve Planlar

Bu Plan, Şirket nezdinde kişisel verilerin korunması ve işlemesine ilişkin yürürlüğe konmuş tüm politika ve Planlar ile birlikte ele alınmalıdır.

7. Güncelleme

Bu Plan kurumsal ya da yasal kaynaklı içeriklerindeki değişiklik gereksinimlerine bakılmaksızın yılda bir kez gözden geçirilerek kayıt altına alınır. Plan güncellenmemiş olsa bile, mevzuatta meydana gelen değişiklikler derhal uygulanacaktır.