

VERİ İHLALİ MÜDAHALE PROSEDÜRÜ

1. Amaç

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("KVKK") 12. maddesinin 5. fıkrası uyarınca 7kita Petrolcülük Dağıtım Ve Pazarlama Anonim Şirketi ("**Firma**") işlenen kişisel verilerin yasal olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durumu en kısa sürede ilgisine ve Kişisel Verileri Koruma Kurulu'na ("**Kurul**") bildirmekle yükümlüdür.

İşbu Veri İhlali Müdahale Prosedürü ("**Prosedür**"), kişisel verilerin yasal olmayan yollarla başkaları tarafından elde edilmesi halinde ortaya çıkacak sorunun nasıl çözüleceği ve atılacak adımların neler olacağı konusunda çalışanları bilgilendirmek amacıyla hazırlanmıştır.

2. Sorumluluk

Prosedür'ün uygulanmasından Firma'nın tüm çalışanları birlikte sorumludur. Prosedür'e aykırı davranan çalışanlar hakkında Disiplin Yönetmeliği hükümlerine göre işlem yapılacaktır.

3. Kişisel Veri İhlali

Kişisel veri ihlali, kişisel verilerin yasaya aykırı bir şekilde elde edilmesi, hukuka uygun olmayan yollarla kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin ihmalen veya kasten yetkisiz kişilere açıklanması, kişisel verilerin hukuka aykırı bir şekilde silinmesi, değiştirilmesi veya bütünlüğünün bozulması gibi durumlarda söz konusu olmaktadır.

Aşağıda sayılan durumlar genel olarak kişisel veri ihlali niteliğindedir:

- ✓ Kişisel veri içeren fiziki belgelerin veya elektronik aletlerin çalınması, kaybolması veya yok olması,
- ✓ Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi,
- ✓ Gizli bilgilerin hukuka aykırı şekilde ifşa edilmesi,
- ✓ Kişisel veri ve/veya gizli bilgi içeren e-postaların ihmalen veya kasten Firma dışında ilgisiz kişilere iletilmesi, gönderilmesi,
- ✓ Bilişim ekipmanlarına, sistemlerine ve ağlarına virüs bulaşması veya diğer saldırıların (örneğin siber saldırı) gerçekleşmesi yoluyla kişisel verilere hukuka aykırı erişim sağlanması.

Yukarıda belirtilen veya benzer durumlarda işbu Prosedür'de öngörülen önlemlerin alınması gerekmektedir.

4. Kriz Müdahale Ekibi

Kişisel veri ihlali durumunda ortaya çıkan veya olası kriz durumuna müdahale etmek ve KVKK kapsamında öngörülen yükümlülükleri yerine getirmek için aşağıda belirtilmiş olan

bölümlerden seçilen katılımcıların üyesi olacağı bir Kriz Müdahale Ekibi (“**Ekip**”) oluşturulur:

- ✓ Veri Sorumlusu İrtibat Kişisi
- ✓ Bilgi Güvenliği (IT) Sorumlusu
- ✓ İhlalin Meydana Geldiği Departmanın Yöneticisi

5. Kriz Müdahale Süreci

Kişisel Verileri Koruma Kurulu’nun 24.01.2019 tarih ve 2019/10 sayılı Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kararı (Karar) uyarınca, Firma tarafından kişisel veri ihlalinin öğrenildiği tarihten itibaren ihlalin gecikmeksizin ve en geç 72 saat içinde Kurul’a bildirilmesi ve veri ihlalinin etkilenen kişilerin belirlenmesi sonrası ilgili kişilere de makul olan en kısa süre içerisinde mümkünse doğrudan, mümkün değilse Firma’nın kendi internet sitesi üzerinden duyuru yayımlanması gibi uygun yöntemlerle bildirim yapılması gerekmektedir.

Söz konusu yükümlülüklerin yerine getirilebilmesi için, gerçekleşmiş bir veri ihlali durumunda Firma içinde öncelikle yapılması gerekenler şunlardır:

- ✓ Krize ilişkin ön değerlendirme,
- ✓ Engelleme ve kurtarma çalışmalarının yürütülmesi,
- ✓ Risklerin değerlendirilmesi,
- ✓ Bildirim,
- ✓ Değerlendirme ve iyileştirme.

5.1. Krize İlişkin Ön Değerlendirme

Firma nezdinde gerçek veya muhtemel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar Veri Sorumlusu İrtibat Kişisi’ne derhal ve gecikmeksizin durumu bildirmek zorundadır. Bu kapsamda ilgili çalışan aşağıdaki hususları içeren bir rapor hazırlayarak, veri ihlalinin Veri Sorumlusu İrtibat Kişisi’ne bildirmekle yükümlüdür.

- ✓ Kişisel veri ihlalinin gerçekleşme tarihi ve saati,
- ✓ Kişisel veri ihlalinin tespit tarihi ve saati,
- ✓ Kişisel veri ihlali olayına ilişkin açıklamalar,
- ✓ Eğer biliniyorsa kişisel veri ihlalinin 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, hazırlanan raporda belirtilen hususları da gözeterek bir ön değerlendirme yapar. Bu ön değerlendirmeyi yaparken, gerçekten bir veri ihlalinin söz konusu olup olmadığını, ihlalin kapsamını, oluşabilecek etkilerini de ihtiyaç halinde dikkate alarak, Ekip ile birlikte veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

5.2. Engelleme ve Kurtarma Çalışmalarının Yürütülmesi

Veri ihlalinin Firma ve ilgili kişiler üzerindeki etkilerinin en aza indirilebilmesi için engelleme ve kurtarma çalışmaları Ekip'in denetim ve gözetiminde yapılır. Bu kapsamda öncelikle veri ihlalden haberdar edilmesi gereken bölümler tespit edilir ve bu bölümlerdeki çalışanlara ihlalin kontrol edilebilmesi, mümkünse engellenebilmesi ve zararların en aza indirilebilmesi için yapılması gereken eylemlere yönelik bilgilendirme yapılır.

Daha sonra, veri ihlalden etkilenmesi muhtemel kişiler ve kayıtlar tespit edilir ve varsa bu kişilerin iletişim bilgileri de belirlenir. Aynı anda, veri ihlali nedeniyle haberdar edilmesi gereken başka kurum ya da kuruluşlar olup olmadığı değerlendirilir.

5.3. Risklerin Değerlendirilmesi

Kişisel veri ihlallerinin, ihlalden etkilenen kişiler üzerinde kimlik hırsızlığı, hakların kısıtlanması, dolandırıcılık, finansal kayıp, itibar kaybı, kişisel verilerin güvenliğinin kaybı, ayrımcılık gibi birçok olumsuz sonuca sebep olması mümkündür. Dolayısıyla kişisel veri ihlalinin Firma ve ihlalden etkilenen kişiler üzerinde ne gibi etkiler oluşturabileceğinin detaylı olarak değerlendirilmesi ve risklerin tespit edilmesi gerekir.

Ekip tarafından riskler değerlendirilirken, ihlalden etkilenen kişisel verilerin niteliği, özelliği ve hacmi ile etkilenen bireylerin sayısı ve kişi gruplarının kimler olduğu, veri ihlalinin Firma'nın faaliyetleri ile saygınlığına olan etkisi, veri ihlalinin etkisinin azaltılması için alınacak tedbir ile ihlalin olası sonuçları ayrı ayrı değerlendirilmelidir. İşbu değerlendirmeye göre veri ihlali “düşük, orta veya yüksek düzeyde risk” olmak üzere üç farklı düzeyde nitelendirilir:

Düşük düzeyde risk: İhlal, ilgili kişiler üzerinde olumsuz herhangi bir etki yaratmamakta ya da bu etki ihmal edilebilir düzeyde kalmaktadır.

Orta düzeyde risk: İhlal, ilgili kişiler üzerinde olumsuz etkilere neden olabilmekte fakat yarattığı bu etki sınırlı kalmaktadır.

Yüksek düzeyde risk: İhlal, etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere sebep olmaktadır.

Kurul kararları uyarınca gerçekleşen veri ihlalinin düzeyinin belirlenmesi için, ihlalin ilgili kişiler üzerinde ne düzeyde bir muhtemel etki yarattığının değerlendirilmesi gerekmektedir. Söz konusu muhtemel etkinin değerlendirilmesinde ise ihlalin niteliği, ihlalin sebebi, ihlale maruz kalan verinin türü, ihlalin etkisinin azaltılması için alınan tedbirler ile ihlalden etkilenen veri sahibi kişi dikkate alınır.

Kişilerin sadece adı soyadı ve telefon bilgilerinin yer aldığı bir katılım listesinin ihlale konu olması durumunda ihlalin düşük düzeyde risk taşıdığı söylenebilir.

İhlalin ilgili kişiler üzerinde olumsuz etkileri bulunması ancak etkisinin büyük olmaması orta düzeyde risk olarak kabul edilebilir. Her ne kadar kişilerin önemli bilgileri ihlale konu olsa da, veri sorumlusunun ihlal sonrası aldığı güvenlik önlemleri ile ihlalin etkilerinin önemli ölçüde azalmış olması orta düzeyde risk niteliğindedir.

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 finansal bilgilerinin yer alması durumunda ihlalin yüksek düzeyde risk taşıdığı sonucuna varılacaktır.

Orta ve özellikle yüksek düzeyde risk olarak kabul edilen veri ihlallerine ilişkin Veri Sorumlusu Üst Yönetimi, Ekip tarafından bilgilendirilir.

5.4. Bildirim

Veri ihlali durumunda, hem hukuki yükümlülük gereği, hem de tedbir alınması ve ihlalin olası etkilerinin azaltılması gibi hedeflerle Firma dışında üçüncü kişilere bildirimde bulunulması 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 bildirmek zorundadır. Bu nedenle, Firma içerisinde tüm çalışanların herhangi bir veri ihlali durumunu vakit kaybetmeksizin Veri Sorumlusu İrtibat Kişisi'ne bildirmesi, Firma'nın herhangi bir hukuki, idari veya cezai yaptırımla karşı karşıya kalmaması için son derece önemlidir.

Kurul'a yapılacak bildirimde Kişisel Verileri Koruma Kurumu'nun internet sitesinde (<https://ihlalbildirim.kvkk.gov.tr/>) yayınlanmış olan Kişisel Veri İhlali Başvuru Formu kullanılır. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı durumlarda, işbu bilgiler gecikme olmaksızın aşamalı olarak sağlanabilir.

Haklı bir neden ile 72 saat içerisinde Kurul'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurul'a bildirilmesi gerekmektedir.

5.4.2. İhlalden Etkilenen Kişilere Bildirim

Firma, kişisel veri ihlalinden etkilen kişilerin belirlenmesi sonrasında ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliriyorsa doğrudan, ulaşamıyorsa uygun yöntemlerle (örneğin internet sitesi üzerinden ihlale ilişkin bir duyuru yayınlanması) bildirim yapılmalıdır. İşbu bildirimler, Ekip'in desteğiyle Veri Sorumlusu İrtibat

Kişisi tarafından yapılır.

Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarih ve 2019/271 sayılı Kararı uyarınca Firma tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması gerekmekte olup bildirimde asgari olarak bulunması gereken unsurlar şunlardır:

- ✓ 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 önlemler,
- ✓ 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 adres ve numaraları.

5.4.3. Diğer Bildirimler

Firma hukuken yapmakla yükümlü olduğu bildirimlerin yanı sıra; veri ihlalinin niteliği, büyüklüğü, ihlalin suç teşkil edip etmediği gibi hususları da dikkate alarak, üçüncü kişilere de bildirim yapmakla yükümlü olabilir. Bu kişiler, diğer veri sorumluları ya da veri işleyenler, danışmanlar, adli makamlar, bankalar ve diğer finans kuruluşları olabilir. Ekip, üçüncü kişilere bildirimde gerek olup olmadığını ayrıca tespit eder ve gerek bulunması halinde bildirimleri yapar.

5.5. Değerlendirme ve İyileştirme

Firma tarafından kişisel veri ihlallerine ilişkin tüm bilgilerin, ihlalin etkilerinin, olası sonuçlarının ve alınan önlemlerin kayıt altına alınması ve Kurul'un incelemesine hazır halde bulundurulması gerekmektedir. Veri Sorumlusu İrtibat Kişisi ve Ekip, veri ihlaline ilişkin yapılan eylem ve işlemlerin uygunluğunu ve olası bir veri ihlalinde geliştirilebilecek hususların neler olabileceğini belirlemek adına bir değerlendirme yapar. Bu kapsamda Ekip, aşağıdaki bilgileri içeren bir değerlendirme ve iyileştirme raporu hazırlar:

- ✓ Olası kişisel veri ihlallerinin etkilerini azaltmak için nelerin yapılması gerektiği,
- ✓ Kişisel veri ihlali nedeniyle herhangi bir politika, prosedür ya da raporlamada iyileştirmenin gerekip gerekmediği,
- ✓ Kişisel veri ihlalinin tekrarlanmasını engelleyebilmek için ek bir idari ve/veya teknik tedbir alınmasına gerek olup olmadığı,
- ✓ İhlalin tekrarlanmasını önleyecek bir personel farkındalık eğitimine gerek olup olmadığı,
- ✓ İhlallere maruz kalmayı ve bu ihlallerin maliyet etkilerini azaltmak için kaynaklara/altyapıya ek yatırım yapılmasına gerek olup olmadığı.

6. İlgili Politika ve Prosedürler

Bu Prosedür, Firma nezdinde kişisel verilerin korunması ve işlenmesine ilişkin yürürlüğe konmuş tüm talimat, politika ve prosedürler ile birlikte ele alınmalıdır.

7. Güncelleme

Bu Prosedür kanuni ya da kurumsal değişiklik gereksinimlerinden bağımsız olarak yılda bir kez gözden geçirilerek kayıt altına alınır. Prosedür güncellenmemiş olsa bile, mevzuatta meydana gelen değişiklikler derhal uygulanacaktır.

* Firma nezdinde gerçek veya potansiyel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar Veri Sorumlusu İrtibat Kişisi'ne durumu derhal bildirmekle yükümlüdür.