

T.C. ÇEVRE, ŞEHİRCİLİK VE İKLİM DEĞİŞİKLİĞİ BAKANLIĞI

TOPLU KONUT İDARESİ BAŞKANLIĞI

VERİ İHLALİ MÜDAHALE PROSEDÜRÜ

1. AMAÇ

T.C. ÇEVRE, ŞEHİRCİLİK VE İKLİM DEĞİŞİKLİĞİ BAKANLIĞI TOPLU KONUT İDARESİ BAŞKANLIĞI (“VERİ SORUMLUSU”), 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (“KANUN”) 12. maddesinin 5. fıkrasına göre işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, diğer bir deyişle kişisel veri ihlalinin gerçekleşmesi halinde, bu durumu en kısa sürede ilgisine ve Kişisel Verileri Koruma Kuruluna (“KURUL”) bildirmekle yükümlüdür.

İşbu Veri İhlali Müdahale Prosedürü (“PROSEDÜR”), VERİ SORUMLUSU’nun işlemekte olduğu kişisel veriler ile ilgili olarak bir kişisel veri ihlalinin gerçekleşmesi halinde oluşacak krize nasıl müdahale edileceği ve atılacak adımların neler olduğu konusunda çalışanları bilgilendirmek amacıyla hazırlanmıştır.

İşbu PROSEDÜR, VERİ SORUMLUSU’nun kişisel verilerin korunması ve işlemesine ilişkin yürürlüğe koymuş olduğu tüm politika ve prosedürler ile birlikte ele alınır.

2. KİŞİSEL VERİ İHLALİ

Kişisel veri ihlali, kişisel verilerin kanuna aykırı bir şekilde elde edilmesi, kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin yanlışlıkla veya kasten yetkisiz kişilere açıklanması, kişisel verilerin hukuka aykırı bir şekilde silinmesi, değiştirilmesi veya bütünlüğünün bozulması gibi durumlarda ortaya çıkmaktadır.

Aşağıda yer alan ve benzeri durumlar genel olarak kişisel veri ihlali olarak değerlendirilir:

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

- Kişiyeye 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 yanlışlıkla veya kasten Kurum dışında ilgisiz kişilere iletilmesi ve/veya gönderilmesi
- Bilgi işlem ekipmanlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin siber saldırı) gerçekleşmesi suretiyle kişisel verilere hukuka aykırı erişim sağlanması.

3. VERİ İHLALİ MÜDAHALE EKİBİ

Kişisel veri ihlali durumunda gerekli müdahalelerde bulunmak ve KANUN kapsamında öngörülen yükümlülükleri yerine getirmek için VERİ SORUMLUSU'nun bünyesinde aşağıdaki katılımcıların dahil edileceği bir Veri İhlali Müdahale Ekibi oluşturulur:

- Veri Sorumlusu İrtibat Kişisi,
- İhlalin Ortaya Çıktığı Departman Yetkilisi,
- Kişisel Verilerin Korunması Komitesi.

4. VERİ İHLALİ MÜDAHALE SÜRECİ

Bir veri ihlalinin gerçekleşmesi halinde, VERİ SORUMLUSU'nun bünyesinde sırasıyla veri ihlaline ilişkin bir ön değerlendirme yapılır, engelleme ve kurtarma çalışmaları yerine getirilir, ilgili riskler değerlendirilir, KURUL'a bildirim yapılır ve bunu takiben veri ihlali sonrası değerlendirme ve geliştirme yönünde neler yapılabileceği belirlenir.

4.1. VERİ İHLALİNE İLİŞKİN ÖN DEĞERLENDİRME YAPILMASI

VERİ SORUMLUSU'nun bünyesinde bir veri ihlalinin gerçekleşmesi ya da veri ihlali ihtimalinin ortaya çıkması halinde, ilgili tüm çalışanlar ilgili departmanın yetkilisine ve Veri Sorumlusu İrtibat Kişisi 'ne **derhal ve gecikmeksizin** durumu bildirmekle yükümlüdür. Bahse konu bildirim; ihlalin gerçekleşme tarihi ve saati, ihlalin tespiti tarihi ve saati, veri ihlalinin niteliği veya veri ihlalinden etkilenenleri içerir.

Veri Sorumlusu İrtibat Kişisi, Veri İhlali Müdahale Ekibi ile birlikte veri ihlaline ilişkin bildirim üzerine bir ön değerlendirme yapar.

4.2. ENGELLEME VE KURTARMA ÇALIŞMALARININ YÜRÜTÜLMESİ

Veri İhlali Müdahale Ekibi, gerçekleşen veya muhtemel veri ihlalinin VERİ SORUMLUSU'nun ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için engelleme ve kurtarma çalışmalarını yürütür. Bu çerçevede, öncelikle veri ihlalden haberdar edilmesi gereken departmanlar tespit edilerek ihlalin kontrol edilebilmesi, mümkünse engellenebilmesi ve zararların azaltılabilmesi için atılması gereken adımlar konusunda ilgili birimle koordineli bir şekilde bahse konu çalışmalar yürütülür. Bunu takiben, veri ihlalden etkilenen kişi ve varsa kurum ve kuruluşlar ve iletişim bilgileri tespit edilmeye çalışılır.

4.3. RİSKLERİN TESPİT EDİLMESİ

Gerçekleşen veri ihlalinin düzeyinin belirlenmesinde ilgili kişiler üzerinde ne kadar bir potansiyel etkiye neden olduğu değerlendirilmektedir. Veri İhlali Müdahale Ekibi tarafından gerçekleşen veya muhtemel veri ihlalinin düzeyi, ihlalden etkilenen kişiler üzerinde oluşturabileceği olumsuz etkiler, ilgili riskler ortaya konularak ve değerlendirilerek tespit edilir. Söz konusu tespit işleminin yapılması sırasında; ihlalin niteliği, ihlalin nedeni, ihlale maruz kalan verinin türü, ihlalin etkisinin azaltılmasında alınan önlemler ile ihlalden etkilenen ilgili kişi kategorileri göz önünde bulundurulur.

4.4. KURULA, İLGİLİ KİŞİLERE VE GEREKTİĞİNDE ÜÇÜNCÜ KİŞİLERE BİLDİRİM YAPILMASI

VERİ SORUMLUSU, Kişisel Verileri Koruma Kurulu'nun Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin 24.01.2019 tarihli ve 2019/10 sayılı Kararı uyarınca, kişisel veri ihlalinin öğrenildiği tarihten itibaren en geç 72 saat içinde veri ihlalinin KURUL'a bildirir.

KURUL'a yapılacak bildirimde Kişisel Verileri Koruma Kurumu'nun 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 72 saat içerisinde KURUL'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenleri de KURUL'a açıklanır.

Veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de **makul olan en kısa süre içerisinde** ilgili kişinin iletişim adresine ulaşılabilirse doğrudan, ulaşamazsa VERİ SORUMLUSU'nun kendi internet sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirir.

Kişisel Verileri Koruma Kurulunun 18.09.2019 tarihli ve 2019/271 sayılı Kararı gereğince; VERİ SORUMLUSU tarafından ilgili kişiye yapılacak olan ihlal bildirim açık ve sade bir dille yapılır ve asgari olarak;

- İhlalin ne zaman gerçekleştiği,
- Kişisel veri kategorileri bazında (kişisel veri/özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
- Kişisel veri ihlalinin muhtemel 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 web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları, unsurlarına yer verilir.

Veri İhlali Müdahale Ekibi tarafından veri ihlalinin niteliği ve kapsamı, ihlalin suç teşkil edip etmediği gibi hususlar değerlendirilerek diğer veri sorumluları, veri işleyenler, dış danışmanlar, adli makamlar ve bankalar gibi üçüncü kişilere de bildirim yapılabilir.

4.5. DEĞERLENDİRME VE GELİŞTİRME ÇALIŞMALARININ YÜRÜTÜLMESİ

Veri ihlalini takiben son aşamada Veri İhlali Müdahale Ekibi tarafından; muhtemel kişisel veri ihlallerinin etkilerini azaltmak için hangi adımların atılması gerektiği, bunun için ek bir idari ve/veya teknik tedbir alınmasının gerekip gerekmediği, kişisel veri ihlali nedeniyle herhangi bir politika veya prosedürde değişiklik ya da iyileştirme gerekip gerekmediği, tekrar bir veri ihlali ile karşı karşıya kalmamak için ek kaynak ve/veya alt yapıya ihtiyaç olup olmadığı, eğitim gerekliliğinin olup olmadığı gibi hususları içeren bir rapor hazırlanır ve Koordinatöre sunulur.

5. PROSEDÜRÜN GÜNCELLENMESİ

İşbu PROSEDÜR, kurumsal ya da mevzuattan kaynaklanan içerik deęişiklik gereksinimlerine bakılmaksızın yılda bir kez gözden geçirilip gerektiğinde güncellenir.

VERİ SORUMLUSU'nun ayrıca KANUN, Kişisel Verileri Koruma Kurulu kararları uyarınca ya da mevzuattaki gelişmeler doğrultusunda işbu PROSEDÜR metninde deęişiklik yapma hakkını saklı tutar.