



ADANA

TİCARET BORSASI

KİŞİSEL VERİ GÜVENLİĞİ İHLAL PROSEDÜRÜ

Hazırlayan: Adana Ticaret Borsası Genel Sekreter Yrd. M. Hakan KAHYALAR

Onaylayan: 18.02.2025 tarih ve 119 sayılı Yönetim Kurulu kararıyla onaylanmıştır.

Yürürlük Tarihi:18.02.2025

// İş bu belge Adana Ticaret Borsasının yazılı izni olmaksızın çoğaltılıp, dağıtılamaz.//

KİŞİSEL VERİ GÜVENLİĞİ İHLAL PROSEDÜRÜ

1. Amaç

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 12. Maddesinin 5. fıkrasına göre ADANA TİCARET BORSASI (Borsa) işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durumu en kısa sürede ilgisine ve Kişisel Verileri Koruma Kuruluna (Kurul) bildirmekle yükümlüdür.

İşbu 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.

2. Sorumluluk

Prosedür 'ün uygulanmasından tüm çalışanlar sorumludur. Prosedüre 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 Borsa 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 Prosedür 'de 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 aşağıdaki departmanlardan belirlenen katılımcıların dahil edileceği bir Kriz Müdahale Ekibi (Ekip) oluşturulur:

- Veri Sorumlusu İrtibat Kişisi
- Veri Sorumlusu Üst Yöneticisi (Genel Sekreter)
- İhlalin Meydana Geldiği Departmanın Yöneticisi
- KVK Danışma Grubu
- KVK Konusunda Veri Sorumlusunun Yetkilendirdiği Üst Yöneticiler (KVK Üst Yöneticiler)

5. Kriz Müdahale Süreci

Borsanın kişisel veri ihlalinin öğrendiği tarihten itibaren gecikmeksizin ve **en geç 72 saat içinde** Kurul'a bildirmesi ve veri ihlalinin etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde ilgili kişinin iletişim adresine ulaşabiliyorsa doğrudan, ulaşamıyorsa Borsanın kendi internet sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması gerekmektedir.

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

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

5.1. Krize İlişkin Ön Değerlendirme

Borsa 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 ihlalinin 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 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, 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.

5.2. Engelleme ve Kurtarma Çalışmalarının Yürütülmesi

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

Akabinde veri ihlalinin etkilenen 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.

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 Borsa 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 Borsanın 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 Yönetimi'ne Ekip tarafından bilgi verilir.

5.4. Bildirim

Veri ihlalinin gerek hukuki yükümlülük kapsamında gerekse veri ihlaline ilişkin tedbir alınması, ihlalin olası etkilerinin azaltılması gibi amaçlarla Borsa 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, Borsa içerisinde tüm çalışanların herhangi bir veri ihlali durumunu vakit kaybetmeksizin Veri Sorumlusu İrtibat Kişisi'ne bildirmesi, Borsanın 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 72 saat içerisinde Kurul'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenleri de Kurul'a açıklanır.

5.4.2. İhlalden Etkilenen Kişilere Bildirim

Borsa, kişisel veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşabiliyorsa doğrudan, ulaşamıyorsa uygun yöntemlerle (örneğin internet sitesi üzerinden duruma ilişkin bir duyuru yayınlanması) bildirim yapılmalıdır. Söz konusu bildirimler, Ekibin desteğiyle Veri Sorumlusu İrtibat Kişisi tarafından gerçekleştirilir.

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, 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.

5.4.3. Diğer Bildirimler

Borsanın 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.

5.5. Değerlendirme ve İyileştirme

Borsa 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 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.

- 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

6. İlgili Politika Ve Prosedürler

Bu Prosedür, Borsa nezdinde kişisel verilerin korunması ve işlemesine ilişkin yürürlüğe konmuş tüm politika ve prosedürler ile birlikte ele alınmalıdır.

7. Güncelleme

Bu Prosedür kurumsal ya da yasal kaynaklı içeriklerindeki değişiklik gereksinimlerine bakılmaksızın 3 yılda bir kez gözden geçirilerek kayıt altına alınır. Prosedür güncellenmemiş olsa bile, mevzuatta meydana gelen değişiklikler derhal uygulanacaktır.

HAZIRLAYAN

ONAYLAYAN

M. Hakan KAHYALAR
Genel Sekreter Yrd.

T. Gökhan ÖZTÜRK
Genel Sekreter

Şahin BİLGİÇ
Yönetim Kurulu Başkanı