DEĞİŞİKLİKLER (REVİZYON) TABLOSU

No	Konusu	Tarih	Talep Eden Kişi/Birim
1	Prosedür oluşturulması	07.2026	Hukuk ve Uyum Departmanı BT Departmanı

DAĞITIM LİSTESİ:

Borusan Holding A.Ş. ve grup şirketleri ("**Borusan Grubu**") personeli

HAZIRLAYAN(LAR)	KONTROL(LER)	ONAY(LAR)
Nurhak Özer **Uyum Birim Yöneticisi** **Saliha Atiş** **Grup Bilgi Güvenliği Mimarı**	**Yaşar Sarcan** **Grup Bilgi Güvenliği Direktörü**	**Selin Tiftikçi Tuncer** **Baş Hukuk Müşaviri** **Deniz Emre** **Strateji ve İş Geliştirme Genel Müdür Yardımcısı**

İçindekiler

2. PROSEDÜR HAKKINDA ... 3
3. AMAÇ VE YASAL DAYANAK ... 3
4. TANIMLAR ... 4
5. KİŞİSEL VERİ İHLALİ ... 4
5.1. Kişisel Veri İhlali Nedir? ... 5
5.2. Kişisel Veri İhlaline Sebep Olabilecek Durumlar Nelerdir? ... 5
6. VERİ İHLALİ MÜDAHALE EKİBİ ... 6
7. VERİ İHLALİ MÜDAHALE EKİBİNİN YÜKÜMLÜLÜKLERİ ... 7
8. VERİ İHLALİ MÜDAHALE SÜRECİ ... 8
8.1. Veri İhlali Müdahale Planı ... 8
8.1.1. Tanımlama ve İlk Değerlendirme ... 9
8.1.2. Engelleme ve Kurtarma ... 9
8.1.3. Bildirim ... 10
8.1.4. Değerlendirme ve İyileştirme ... 11
9. İHLALİN KURUL'A BİLDİRİLMESİ ... 11
10. İHLALİN İLGİLİ KİŞİLERE BİLDİRİLMESİ ... 12
11. İHLALİN VERİ SORUMLULARINA VE VERİ İŞLEYENLERE BİLDİRİLMESİ ... 13
11.1. Birlikte Veri İşlenen Veri Sorumlularına Bildirim ... 13
11.2. Veri İşleyenler Tarafından Borusan Grubu'na Bildirim Yapılması ... 13
12. İHLALİN ÜÇÜNCÜ TARAFLARA BİLDİRİLMESİ ... 14
13. İHLAL BİLDİRİM SÜRECİNDE İÇ VE DIŞ KURUMSAL İLETİŞİMİN YÜRÜTÜLMESİ ... 14
14. ÇALIŞANLARIN SORUMLULUĞU ... 14
15. PROSEDÜR'ÜN GÜNCELLENMESİ ... 15
EK-1 KİŞİSEL VERİ İHLALLERİNE MÜDAHALE AKIŞI
EK-2 KİŞİSEL VERİ OLAY RAPORU

2. PROSEDÜR HAKKINDA

Borusan Holding A.Ş. ve grup şirketleri ("**Borusan Grubu**") olarak, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**")[1] ile Kanun kapsamındaki ikincil düzenlemeler ile Kişisel Verileri Koruma Kurulu'nun ("**Kurul**") kararları uyarınca, Borusan Grubu içerisinde bir kişisel veri ihlali meydana gelmesi halinde çeşitli yükümlülüklerimiz bulunmaktadır.

Borusan Grubu, bünyesindeki görevli çalışanlarımızın tamamı başta Borusan Grubu Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Prosedürü'nde belirtilenler olmak üzere, kişisel verilerin güvenliğinin sağlanmasına yönelik ilgili politika ve prosedürlerde belirtilen tüm önlemleri almalı ve veri güvenliğinin sağlanması adına iş birliği içerisinde hareket etmelidir. Bu kapsamda, Borusan Grubu çalışanlarının tamamı, olası bir kişisel veri ihlalinin meydana gelmesi halinde bu Prosedür'ü en iyi ve en etkin şekilde uygulamakla yükümlüdür.

Bu Prosedür kişisel veri ihlali meydana geldiğinde çalışanlarımızın alacağı aksiyonları açıklayan ve kişisel veri ihlali durumunda çalışanlarımızı yönlendiren bir rehber niteliğine sahiptir.

Grup şirketleri bu Prosedürü esas alarak, bu Prosedüre aykırı olmayacak şekilde kendi iç prosedürlerini oluşturabilir. Kendi iç prosedürlerini oluşturan şirketler açısından bu prosedür, kendi iç prosedürlerinin eki niteliğindedir.

3. AMAÇ VE YASAL DAYANAK

Borusan Grubu tarafından hazırlanan bu Prosedür, dayanağını Kanun'un 12. maddesinin 5. fıkrasında düzenlenen, kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve her halükarda en geç 72 saat içerisinde Kurul'a bildirme yükümlülüğünden almaktadır. İşbu Prosedür, Kurul'un 24.01.2019 tarih ve 2019/10 sayılı kararı ile 18.09.2019 tarih ve 2019/271 sayılı kararına uygun bir şekilde hazırlanmıştır.

Bu Prosedür, Borusan Grubu bünyesinde bir kişisel veri ihlali gerçekleşmesi halinde ilgili ekiplerin bilgilendirilmesi, söz konusu kişisel veri ihlaline en etkili şekilde müdahale edilmesi ve şirket/grup içi koordinasyonun sağlanması amacıyla hazırlanmıştır.

[1] Resmî Gazete Tarihi: 07.04.2016 Resmî Gazete Sayısı: 29677.

4. TANIMLAR

a. **Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

b. **Kişisel verilerin işlenmesi:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

c. **Kurum:** Kişisel Verileri Koruma Kurumu.

d. **Özel Nitelikli Kişisel Veri:** Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.

e. **Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

f. **Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.

g. **Şirket:** Borusan Holding A.Ş. veya Borusan Grubu şirketleri.

h. **Şirket İrtibat Kişisi:** İlgili Borusan Grubu Şirketi'ndeki uyum sorumlusu. Uyum sorumlusu bulunmayan şirketlerde ise kişisel verilerin korunmasına ilişkin mevzuata uyumu sağlamaktan sorumlu kişi.

i. **İlgili Kişi/Veri Sahibi:** Kişisel verileri işlenen gerçek kişi.

j. **Kişisel Veri İhlal Kaydı:** Herhangi bir kişisel veri ihlali olması durumunda söz konusu ihlale ilişkin Şirket tarafından tutulan her türlü kayıt, Kurul'a ve ilgili kişilere yapılan bildirimler.

Bu Prosedür'de ayrıca tanımlanmayan ifadeler ise Kanun ve diğer ikincil düzenlemelerde yer alan tanımlarıyla birlikte kullanılmaktadır.

5. KİŞİSEL VERİ İHLALİ

Borusan Grubu, kişisel verilerin hukuka aykırı olarak işlenmesini, kişisel verilere hukuka aykırı olarak erişilmesini ve kişisel verilerin güvenliğini sağlamak amacıyla uygun güvenlik düzeyini temin

etmeye yönelik gereken her türlü teknik ve idari tedbirleri alır. Uygun güvenlik düzeyi, işlenen kişisel verilerin niteliği, veri işleme faaliyetinin kapsamı, olası riskler, ilgili mevzuat gereklilikleri ve kurumsal bilgi güvenliği politikaları dikkate alınarak belirlenir. Teknik ve idari tedbirlerin belirlenmesinde başta ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Gizlilik Bilgi Yönetim Sistemi, NIST Sibergüvenlik Çerçevesi ve ilgili KVKK düzenlemeleri olmak üzere kabul görmüş ulusal ve uluslararası güvenlik standartları ve iyi uygulamalar referans alınır.

5.1. Kişisel Veri İhlali Nedir?

Borusan Grubu'nun tüm süreçlerinde işlediği kişisel verilerin gizliliğini, bütünlüğünü, güvenliğini ve ulaşılabilirliğini etkileyen veya etkileyebilecek olan herhangi bir olay kişisel veri ihlali olarak nitelendirilmektedir.

Kişisel Veri ihlali, genellikle şu şekillerde karşımıza çıkabilmektedir:

- Yetkisiz kişilerce hukuka aykırı şekilde kişisel verilere erişim sağlanması,
- Yetkisiz kişilerce kişisel verilerin ifşa edilmesi/açıklanması veya
- Kişisel verilerin hukuka aykırı bir şekilde imhasına, kaybına veya değiştirilmesine sebep olunması.

5.2. Kişisel Veri İhlaline Sebep Olabilecek Durumlar Nelerdir?

Kanun'da, kişisel verilerin gizliliğini, bütünlüğünü, ulaşılabilirliğini veya güvenliğini etkileyebilecek çeşitli olaylar belirtilmiştir.

Somut olayın özelliklerine bağlı olarak değişebilmek kaydıyla, Kurul tarafından genellikle kişisel veri ihlali olarak değerlendirilebilecek durumlar aşağıda örneklendirilmiştir:

- Kişisel veri veya özel nitelikli kişisel verilerin e-posta veya posta yoluyla yanlış alıcıya gönderilmesi,
- Kişisel verileri içeren herhangi bir fiziki dokümanın veya elektronik cihazın çalınması yahut kaybolması,
- Kişisel veri içeren elektronik belgelerin, donanım veya yazılımlar aracılığıyla hukuka aykırı biçimde Borusan Grubu dışına çıkarılması,
- Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi ve bu suretle kişisel verilere yetkisiz erişim sağlanması,

- Kişisel verilerin Borusan Grubu dışı yetkisiz kullanımına izin veren uygunsuz erişim sağlanması,
- Kişisel verilerin yetkisiz kişilere açıklanması,
- Kişisel verilerin hukuka aykırı şekilde değiştirilmesi veya silinmesi,
- IT ekipman sistemleri veya ağları üzerinde virüsler, diğer güvenlik saldırılar (örneğin siber güvenlik saldırıları) sonucu kişisel verilere yetkisiz erişim sağlanması,
- Kişisel verilerin güvenliğine ilişkin fiziksel güvenlik ihlalleri (örneğin Şirket'te meydana gelen olası bir hırsızlık, yağma olayı) meydana gelmesi,
- Kişisel verilerin yanlışlıkla veya yetkisiz kişilerce silinmesi durumunda verilere erişim sağlanamaması,
- Gizli bilgilerin erişilebilir alanlarda gözetimsiz olarak bırakılması (örneğin kişisel veri içeren çıktıların yazıcıda bırakılması),
- Borusan Grubu adına kişisel veri işleyen üçüncü şirketler (örneğin tedarikçiler) nezdinde Borusan Grubu şirketleri tarafından iletilen kişisel verilere ilişkin kişisel veri ihlali meydana gelmesi.

Herhangi bir kişisel veri ihlali durumunda, Kanun ve ilgili mevzuat uyarınca en kısa sürede Kurul'a ve ilgili kişilere bildirim yapılması gerekmektedir. Kurul, yayımlamış olduğu bir kararında "en kısa sürede" ifadesinin ihlalden haberdar olunmasından itibaren 72 saat olarak yorumlanması gerektiğini belirtmiştir. Bu kapsamda Borusan Grubu olarak, veri sorumlusu olduğumuz durumlarda **kişisel veri ihlalini öğrendiğimiz tarihten itibaren Kurul'a gecikmeksizin ve en geç 72 saat içinde, ihlalden etkilenmiş olabilecek kişilerin belirlenmesinin akabinde ise ilgili kişilere makul olan en kısa süre içerisinde kişisel veri ihlal bildiriminde bulunma yükümlülüğümüz bulunmaktadır.**

6. VERİ İHLALİ MÜDAHALE EKİBİ

Kişisel Veri İhlali Müdahale Ekibi ("**Müdahale Ekibi**"), asgari olarak aşağıda belirtilen departmanlarda yer alan kişilerden oluşmalıdır. Her bir Borusan Grubu Şirketi, aşağıda belirtilen departmanları gözeterek kendi Müdahale Ekibi'ni oluşturmakla yükümlüdür. İlgili şirkette bu departmanların bulunmaması halinde, şirketin organizasyon yapısına uygun olarak eşdeğer görev ve sorumlulukları üstlenen departmanlarda yer alan kişiler veya bu konularda doğrudan Holding'den destek alınıyor ise Holding'de ilgili şirket için bu görev ve sorumlulukları üstlenen departmanlar Müdahale Ekibi'ne dahil edilmelidir.

Hukuk ve Uyum Departmanı	İhlalin KVKK ve ilgili mevzuat kapsamında değerlendirilmesini sağlar. Kurul'a ve ilgili kişilere bildirim gerekliliğini değerlendirir, bildirim metinlerini hazırlar ve yasal süreçlerin takibini yapar.
Kurumsal İletişim Departmanı	İhlale ilişkin iç ve dış iletişim süreçlerini kurumsal dil ve itibar yönetimi açısından değerlendirir. Gerekli durumlarda çalışan, müşteri, iş ortağı veya kamuoyu bilgilendirmelerini hazırlar ve koordine eder.
Bilgi Teknolojileri Departmanı	İhlalin teknik ve güvenlik olayı boyutunu değerlendirir; etkilenen sistem, uygulama, veri tabanı, kullanıcı hesabı, log ve erişim kayıtlarını analiz eder. İhlalin kaynağı, kapsamı, etkisi ve kök nedeninin belirlenmesini destekler; gerekli teknik müdahale, izolasyon, iyileştirme ve güvenlik önlemlerinin uygulanmasını sağlar.
İnsan Kaynakları Departmanı	Çalışan verilerinin etkilenmesi veya çalışan kaynaklı ihlal şüphesi bulunması halinde sürece destek olur. Çalışan bilgilendirmeleri, disiplin süreçleri ve farkındalık aksiyonlarının koordinasyonunu sağlar.

İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi, Müdahale Ekibi'nin daimi üyesidir ve müdahale edilecek kişisel veri ihlalinin niteliğine ve etkilerine göre gerekli gördüğü durumlarda, diğer departmanlardan (örneğin kişisel veri ihlalinin gerçekleştiği departmandan) Müdahale Ekibi'nde yer almak üzere gerekli bilgi ve tecrübeye sahip ek sorumlular belirleyebilir.

7. MÜDAHALE EKİBİNİN YÜKÜMLÜLÜKLERİ

Müdahale Ekibi, hukuka aykırı olarak erişim sağlanan kişisel verilerin korunması için gerekli güvenlik tedbirlerini ve söz konusu koruma için ihtiyaç duyulan kaynakları tespit etmenin yanı sıra, kişisel veri ihlallerinin sona erdirilmesi, etkilerinin azaltılması veya mümkünse tamamen ortadan kaldırılması, kişisel veri ihlaline ilişkin Borusan Grubu'nun içi ve dışında zorunlu yasal bildirimler de dahil olmak üzere tüm bildirim ve iletişim süreçleri için gerekli çalışmalar kapsamında Grup veya Şirket içindeki koordinasyonu sağlamakla yükümlüdür. İlgili Borusan Grubu Şirketinde yer alan Müdahale Ekibi, kendi şirketi nezdinde meydana gelen kişisel veri ihlalini derhal Borusan Holding Hukuk ve Uyum Departmanı ile Bilgi Teknolojileri Departmanı'na bildirmekle yükümlüdür. Süreçte, Müdahale Ekibi tarafından yapılması gerekenler şunlardır:

- Meydana gelen kişisel veri ihlalinin doğrulanması,
- Denetim Departmanı'nın kişisel veri ihlali hakkında bilgilendirilmesi,
- Kişisel veri ihlali sürecinde mevzuata ve şirket politika ve prosedürlerine uygun olarak hareket edilmesinin sağlanması,
- Kanun ve ilgili diğer mevzuat uyarınca belirlenmiş idari ve teknik veri güvenliği önlemlerinin alınması ve öngörülen sair yükümlülüklerin yerine getirilmesi,
- Kurul'a, ihlalden etkilenen ilgili kişilere ve yasal/sözleşmesel gereksinimler uyarınca bildirim yapılması gereken diğer kişilere bildirim yapılması, hukuka aykırı erişimin kısıtlanması veya kaldırılması, ihlale konu hizmet ve servislerin askıya alınması,
- Borusan Grubu politika ve prosedürlerinin söz konusu ihlalin tekrar meydana gelmesini önlemeye yönelik olarak tekrar gözden geçirilmesi ve
- İhlale ilişkin ilgili Borusan Grubu şirketi içerisinde raporlamaların yapılması.

8. VERİ İHLALİ MÜDAHALE SÜRECİ

Borusan Grubu şirketleri bünyesindeki çalışanlar, kişisel verilerin ihlaline neden olabilecek bir durum tespit edilmesi halinde derhal ve hiç gecikmeksizin İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi'ne bildirimde bulunmakla, Müdahale Ekibi'ne gerekli tüm desteği sağlamakla ve kişisel veri ihlali müdahale sürecinde üzerine düşen sorumlulukları yerine getirmekle yükümlüdür.

İhlalin kişisel veri ile beraber Borusan Grubu'nun bilgi varlıklarına da ilişkin olması halinde bilgi güvenliği ihlal olayı yönetimi kapsamında Bilgi Güvenliği İhlal Olayı Yönetim Politikası'na da uygun hareket edilir. Aynı zamanda, Olay Yönetim Prosedürü kapsamında izlenmesi gereken adımlar varsa bu adımlar da izlenir.

8.1. Kişisel Veri İhlali Müdahale Planı

İlgili Borusan Grubu Şirketi'nin kişisel veri ihlalinden haberdar olması üzerine kişisel veri ihlaline müdahale süreci başlar. İhlal hakkında derhal İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi'ne bilgi verilir, İrtibat Kişisi ihlalden haberdar olduktan sonra Müdahale Ekibi ile birlikte bir ön inceleme yaparak ihlalin kişisel verilere ilişkin olup olmadığını tespit eder. Ön inceleme sonrasında İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi, Müdahale Ekibi ile birlikte söz konusu ihlali araştırmak ve kapsamlı bir inceleme başlatmakla yükümlüdür.

Müdahale Ekibi, kişisel veri ihlaline ilişkin bütün çalışmaları, atılan adımları, tüm tespitleri, bilgileri, ihlalin etkilerini, yapılan bildirimleri ve alınan önlemleri kayıt altına alır ve bu kayıtları Kurul'un olası bir inceleme talebine hazır halde tutar.

Müdahale Ekibi, veri güvenliği müdahale süreci kapsamında aşağıda detayları açıklanan Kişisel Veri İhlali Müdahale Planını uygular.

8.1.1. Tanımlama ve İlk Değerlendirme

Kişisel veri ihlalini fark eden tüm ilgili Borusan Grubu Şirketi çalışanlarının, derhal ve hiç gecikmeksizin çalışmakta olduğun ilgili Borusan Grubu Şirketi'nin KVKK e-posta adresine yüksek önem düzeyi işaretlenerek gönderilecek "Kişisel Veri İhlali" başlıklı bir e-posta ile, kişisel veri ihlalini kısaca açıklayarak bildirmesi gerekmektedir. İlgili Borusan Grubu Şirketi çalışanlarının, bu Prosedürde tanımlanan adımların uygun şekilde yerine getirilebilmesi için ihlale ilişkin tüm bilgi ve belgeleri olduğu şekilde muhafaza etmesi gerekmektedir.

Borusan Grubu çalışanları, ayrıca, İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi'ni telefonla da arayarak kişisel veri ihlalinden haberdar etmek üzere makul tüm çabayı gösterir.

İrtibat Kişisi, Müdahale Ekibi'ni toplayarak, gerek görülürse ihlal bildirimini yapan ilgili çalışan veya çalışanlarla birlikte, aşağıdaki hususlar üzerinden ilk değerlendirme yapılmasını sağlar:

- Gerçekten bir kişisel kişisel veri ihlalinin söz konusu olup olmadığı,
- Kişisel veri ihlali söz konusu ise, ihlalden dolayı hangi kişisel verilerin etkilendiği,
- Kişisel Veri ihlalinin gerçekleşme tarihi ve saati,
- İhlalin kapsamı ve sebebi,
- İhlalden kaç kişinin etkilenmiş olabileceği,
- İhlalden etkilenen kişilerin kimler olduğu (örneğin çalışanlar, müşteriler, tedarikçiler gibi),
- Alınabilecek ilk müdahale önlemleri.

8.1.2. Engelleme ve Kurtarma

Kişisel veri ihlalinin meydana geldiğinin tespit edilmesi halinde, ihlalin gerekli önlemler alınarak olabildiğince sınırlanması ve veri kaybının önüne geçilerek veri güvenliğinin tekrar sağlanması gerekir. Müdahale Ekibi bu kapsamda, Borusan Grubu içinde ihlalin etkilerinin azaltılması veya ortadan kaldırılması için yol gösterici çalışmalar yürütür.

İhlalden doğabilecek zararları engellemek veya azaltmak için Müdahale Ekibi ve Bilgi Teknolojileri Departmanı alınacak aksiyonlar konusunda koordineli bir şekilde çalışır. Bu çerçevede, Engelleme ve Kurtarma aşamasında; kaybolan verilerin kurtarılması, muhtemel bir siber saldırının sonlandırılması, verilerin yedeklenmesi gibi ihlalin etkilerini azaltmak/ortadan kaldırmak amacıyla alınması gereken teknik önlemlerin belirlenmesi ve ilgili süreçlerin yürütülmesi konusunda ana sorumlu ilgili Şirket'in Bilgi Teknolojileri Departmanıdır, Şirket Bilgi Teknolojileri Departmanı, Holding Bilgi Teknolojileri Departmanı süreçte Holding Bilgi Teknolojileri Departmanı ile koordineli şekilde hareket eder. Bilgi Teknolojileri Departmanı uygun gördüğü ve aldığı önlemleri üyesi olduğu Müdahale Ekibi 'ne eş zamanlı olarak bildirmekle yükümlüdür.

8.1.3. Bildirim

Herhangi bir kişisel veri ihlali söz konusu olduğunda hem yasal zorunluluklar çerçevesinde hem de kurumsal iletişim süreçleri kapsamında aşağıdaki listede sayılan kişi ve kurumlara bildirim yapılması gündeme gelebilir:

- Kişisel Verileri Koruma Kurulu (yasal olarak zorunlu bildirim),
- Kişisel Veri ihlalinden kişisel verileri etkilenen ilgili kişiler (yasal olarak zorunlu bildirim),
- Sözleşmesel ilişkiler kapsamında bildirim yapılması gereken kişi/kurumlar,
- Adli makamlar,
- Basın kuruluşları,
- Dış danışmanlar,
- Yurt dışındaki otoriteler (yasal olarak zorunlu olabilir),
- Diğer ilgili veri sorumluları veya veri işleyenler.

Kurul'a yapılacak yasal olarak zorunlu bildirimler ve ilgili kişilere yapılacak bildirimlerde Prosedür'de belirtilen usullere göre bildirimler yapılır.

İhlalin aynı zamanda suç teşkil etmesi halinde adli makamların bilgilendirilmesi veya yasal olarak zorunlu olarak yapılacak bildirimlerde süreç yürütülürken ilgili Borusan Grubu Şirketi'nin Hukuk ve Uyum Departmanı eğer yoksa Holding Hukuk ve Uyum Departmanı ile birlikte hareket edilmesi gerekmektedir. Dış iletişim gerektiren hallerde belirtilen departmanlara ek olarak Kurumsal İletişim Departmanı ile koordinasyon sağlanır.

Diğer kişi, kurum veya kuruluşlara bildirim yapılırken, bildirim yapılacak taraf ile Borusan Grubu şirketleri arasında bir sözleşme ve bu sözleşmede belirlenen süreler varsa bunlar da dikkate alınmalıdır.

8.1.4. Değerlendirme ve İyileştirme

Müdahale Ekibi, meydana gelen kişisel veri ihlalinin bir daha gerçekleşmemesi için genel bir değerlendirme ve iyileştirme süreci yürüterek; ileride meydana gelebilecek ihlalleri önlemek adına alınabilecek önlemleri, kök neden analizini, kişisel verilerin güvenliğinin sağlanmasında yer alan eksiklikleri, ihlalin önüne geçilmesi için varsa yapılması gereken yatırımları içeren iyileştirme aksiyonlarını belirler ve gerekli görülmesi durumunda ilgili iç ve dış paydaşları aksiyonlar hakkında bilgilendirir.

9. İHLALİN KURUL'A BİLDİRİLMESİ

Olası bir kişisel veri ihlali durumunda, **ihlal, kişisel veri ihlalinin öğrenildiği tarihten itibaren gecikmeksizin ve en geç yetmiş iki (72) saat içinde** Kurul'a bildirmelidir. Kurul'a bildirim süreci bu süre gözetilerek Müdahale Ekibi tarafından yönetilir. Herhangi bir idari yaptırım ile karşılaşmamak adına Kurul'a yasal bildirimin yapılabilmesi için tüm çalışanların kişisel veri ihlalini derhal ve gecikmeksizin İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi'ne haber vermeleri gerekmektedir.

Bildirimin haklı bir sebeple (örneğin Borusan Grubu'nu ilgilendiren kişisel veri ihlali, yurt dışındaki hissedar şirkette meydana gelmiş olabilir ve Türkiye'deki ilgili kişilerin ihlalden etkilenip etkilenmediğinin tespiti uzun sürmüş olabilir) Kurul'a en geç 72 saat içerisinde yapılamamış olması halinde, sonradan yapılacak bildirimle birlikte gecikmenin nedenleri Kurul'a detaylıca bildirilir.

Yurt dışında yerleşik veri sorumlusu nezdinde meydana gelen bir kişisel veri ihlalinin, Türkiye'de yerleşik kişileri etkilemesi durumunda söz konusu kişisel veri ihlalinin Borusan Grubu tarafından Kurul'a bildirilmesi gerekebilir. Bu kapsamda, Borusan Grubu'nun yurt dışında yerleşik hissedarlar ve iş ortakları nezdinde meydana gelen ihlaller de değerlendirilerek gerekli hallerde bu Prosedür'e uygun şekilde bildirim yapılır.

Borusan Grubu adına veri işleyen taraflar nezdinde bulunan kişisel verilerin bir kişisel veri ihlaline konu olması durumunda, bu ihlale ilişkin Kurul'a bildirim yükümlülüğü veri sorumlusu olarak hareket eden Borusan Grubu tarafından yerine getirilir.

Kurul'a aşağıdaki yöntemlerden biri ile kişisel veri ihlal bildirimi gerçekleştirilebilir:

1. Online Bildirim Sistemi

Kişisel veri ihlali, ihlalbildirim.kvkk.gov.tr bağlantısı üzerinden Kurul'a bildirilebilir. Online bildirimin nasıl yapılacağına ilişkin yönlendirmelere bildirim kılavuzundan ulaşılabilir.

2. Kişisel Veri İhlal Bildirim Formu

Kurul'a yapılacak ihlal bildirimlerinde süreç Hukuk/Uyum Departmanı koordinasyonunda Müdahale Ekibi tarafından yürütülür ve kişisel veri ihlal bildirim formu doldurularak, Kurul'a e-posta yoluyla bildirilebilir. Kişisel veri ihlal bildirim formunun ihlalbildirimi@kvkk.gov.tr e-posta adresine, "Kişisel veri ihlali bildirimi" konusuyla gönderilmesi gerekmektedir. Kişisel veri ihlal bildirim formu, Kurul'un güncel adresine posta yoluyla da gönderilebilir.

Bildirim yapılmadan önce güncel bildirim yöntemleri, talep edilen dokümanlar, https://www.kvkk.gov.tr/ adresinden kontrol edilmelidir.

İhlal bildirim formunda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bildirim süresinde gecikme olmaması için, bilgiler aşamalı olarak sağlanır. Bununla birlikte geri kalan bilgiler gecikmeksizin Kurul'a sağlanır.

Formda yer verilen bilgileri destekleyici dokümanlar, (inceleme raporu, ilgili kişilere bildirim yapıldığını tevsik edici belgeler vb.) başvuru ekinde gönderilir.

10. İHLALİN İLGİLİ KİŞİLERE BİLDİRİLMESİ

Kişisel veri ihlali gerçekleştiğinde, kişisel veri ihlalinden etkilenen kişilerin belirlenmesinin ardından ilgili kişilere makul olan **en kısa süre içerisinde** ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamayan hallerde ise uygun yöntemlerle (örneğin Borusan Grubu'nun kendi internet sitesi üzerinden duruma ilişkin bir duyuru yayımlanması) bildirim yapılması gerekmektedir.

İhlalin ilgili kişiler üzerindeki olumsuz etkilerini azaltmak için ilgili kişilere iletilecek metinlerde açık ve sade bir dil kullanılır. İhlalden etkilenen ilgili kişilere yapılacak bildirimin yasal olarak asgari düzeyde aşağıdaki unsurları içermesi gerekmektedir:

- 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,

- Kişisel veri ihlalinin olumsuz etkilerinin minimize edilmesi için alınan veya alınması önerilen tedbirler,
- İlgili kişilerin kişisel 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.

11. İHLALİN VERİ SORUMLULARINA VE VERİ İŞLEYENLERE BİLDİRİLMESİ

Olası bir kişisel veri ihlali durumunda, Müdahale Ekibi, kişisel veri ihlalini derhal/gecikmeksizin diğer veri sorumlularına ve gerekiyorsa veri işleyenlere (ihlalin bu tarafları da ilgilendirmesi şartıyla) bildirir. Veri işleyenler bünyesinde gerçekleşen ve Borusan Grubu'nu ilgilendiren kişisel veri ihlallerinin ilgili Borusan Grubu'na derhal ve gecikmeksizin bildirilmesi için başta sözleşmesel ilişki kapsamında uygun düzenlemelere yer verilmesi olmak üzere gerekli uygun adımlar atılır.

11.1. Birlikte Veri İşlenen Veri Sorumlularına Bildirim

Borusan Grubu'nun bir sözleşme, proje veya bir iş ortaklığı kapsamında birlikte veri işlediği ortak veri sorumluları bulunuyorsa ve söz konusu kişisel veri ihlali, birlikte veri işlenen veri sorumlularını da ilgilendiriyorsa, Hukuk/Uyum Departmanı'nın yönlendirmesi ve onayı ile bu veri sorumlularına da bildirimde bulunulur.

11.2. Veri İşleyenler Tarafından Borusan Grubu'na Bildirim Yapılması

Borusan Grubu adına kişisel veri işleyenler nezdinde, kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi suretiyle Borusan Grubu'nu ilgilendiren bir kişisel veri ihlali meydana gelmesi halinde, veri işleyenler, Borusan Grubu'nu bu kişisel veri ihlalinden derhal ve gecikmeksizin haberdar eder. Veri işleyenlerle yapılan sözleşmelerde buna ilişkin maddelere yer verilir.

Borusan Grubu, veri işleyenler tarafından kişisel veri ihlali bildiriminde bulunulmasının akabinde işbu Prosedür' de yer alan usul ve esasları yürütür. Böyle bir durumda veri işleyen taraf Şirket'e bilgi verilmesi hususunda gerekli desteği sağlar. Bu kapsamda, başta olay logları, teknik raporları ve forensic destek ile ilgili olmak ancak bunlarla sınırlı olmamak kaydıyla veri işleyen taraftan bilgi ve belge talep edilebilir.

12. İHLALİN ÜÇÜNCÜ TARAFLARA BİLDİRİLMESİ

Kişisel veri ihlali meydana geldiğinde, her olay özelinde, Müdahale Ekibi tarafından yapılacak değerlendirme sonrasında; adli makamlara, bankalara, yurt dışındaki otoritelere veya ilgili sair düzenleyici kurumlara bilgi verilmesi gerektiğine karar verilebilir. Örneğin, kişisel veri ihlalinin aynı zamanda bir suç teşkil etmesi durumunda adli makamlara bildirim veya kişisel veri ihlali neticesinde ilgili kişilerin banka veya kredi kartı bilgilerinin ele geçirilmesi gibi durumlarda bankalara bildirim gerekliliği ayrıca değerlendirilmelidir.

13. İHLAL BİLDİRİM SÜRECİNDE İÇ VE DIŞ KURUMSAL İLETİŞİMİN YÜRÜTÜLMESİ

Kişisel Veri İhlali Müdahale Planı uygulanırken, Müdahale Ekibi tarafından dikkate alınması gereken konulardan biri de meydana gelen kişisel veri ihlalinin ve bu ihlalin sonuçlarının Borusan Grubu'nun itibarına ve toplumsal imajına etkisidir. Buna yönelik iç ve dış iletişim, Kurumsal İletişim Departmanı'nın yönlendirmeleri ile yürütülür.

14. ÇALIŞANLARIN SORUMLULUĞU

Çalışma biçimine bakılmaksızın tüm Borusan Grubu çalışanlarının, bu Prosedür ile belirlenen usul ve esaslara uyum sağlamaları beklenmektedir.

Tüm Borusan Grubu çalışanları bu Prosedür' ün etkin biçimde yerine getirilmesi ve uygulanması için azami tüm çabayı göstermekle yükümlüdür. Bu kapsamda, çalışanlar, sorumlu oldukları iş süreçleri kapsamında başta bir kişisel veri ihlalinin meydana gelmemesi adına gerekli tüm önlemlerin alınmasını, Prosedür'de yer alan süreçlerin derhal ve gecikmeksizin yürütülmesini, yapılacak yasal ve diğer tüm bildirimlerin aksamamasını sağlar. Olası bir kişisel veri ihlalinde Prosedür'e uygun hareket etmeyen çalışanlar, iş akdinin feshine varabilecek yaptırımlara tabi olur. Ayrıca eylemlerin hukuka aykırı olması durumunda bireysel olarak cezai yükümlülükler meydana gelebilir.

15. PROSEDÜR'ÜN GÜNCELLENMESİ

Bu Prosedür, Hukuk ve Uyum Departmanı ve Bilgi Teknolojileri Departmanı'nın sahipliğinde ve Baş Hukuk Müşaviri ve Strateji, İş Geliştirme ve BT Genel Müdür Yardımcısı onayıyla en az yılda bir kez gözden geçirilir ve gerektiğinde güncellenir. Kanun ve ikincil düzenlemeler ile Kurul kararları olmak

üzere ilgili mevzuatta yapılan değişiklikler nedeniyle güncellenmemiş olsa bile, ilgili mevzuatta meydana gelen değişiklikler derhal uygulanacaktır.

EK-1: KİŞİSEL VERİ İHLALLERİNE MÜDAHALE AKIŞI

1. Şirket bir kişisel veri ihlalinin meydana geldiğini tespit eder.

↓

2. Kişisel veri ihlali, ihlali tespit eden çalışan tarafından İrtibat Kişisi'ne derhal ve gecikmeksizin bildirilir.

↓

3. İrtibat Kişisi, Veri İhlali Müdahale Ekibi ile birlikte kişisel veri ihlaline ilişkin risk değerlendirmelerini gerçekleştirir ve alınacak aksiyonları belirler.

↓

4. İrtibat Kişisi, EK-2 Kişisel Veri İhlali Olay Raporu'nun ilgili kısımlarını doldurur ve ihlalin kapsamını belirler.

↓

5. Bilgi Teknolojileri Departmanı başta olmak üzere ilgili tüm departmanlar ve çalışanlar veri ihlalinin olumsuz etkilerini minimize etmek için gerekli teknik ve idari önlemleri alır.

↓

6. Kişisel veri ihlali, veri ihlali müdahale planına göre ele alınır.

↓

7. Kişisel veri ihlali kontrol altına alınır.

↓

8. Kişisel veri ihlali kapsamındaki riskler ve sonuçları değerlendirilir.

↓

9.Kişisel veri ihlali, ihlalin tespit edilmesinden itibaren gecikmeksizin ve en geç 72 saat içerisinde Kurul'a ve ihlalin tespit edilmesinden itibaren makul olan en kısa süre çerisinde ihlalden etkilenen ilgili kişilere bildirilir.

↓

10. Yasal bildirimler dışında haberdar edilmesi gereken üçüncü taraflar var ise, bunlara da bilgi verilir.

↓

11. Değerlendirme ve Müdahale aşaması sonuçlandırılır.

↓

12. Kişisel veri ihlaline ilişkin bilgiler, kişisel veri ihlalinin etkileri ve alınan önlemler kayıt altına alınarak Kurul'un incelemesine hazır halde bulundurulur.

EK:2 KİŞİSEL VERİ İHLALİ OLAY RAPORU

KİŞİSEL VERİ İHLALİ OLAY RAPORU *Müdahale Ekibi Tarafından Doldurulacaktır.*	
Olay numarası	*Örneğin KVİ/yıl/001*
Raporu derleyen Kişisel Veri İhlali Müdahale Ekibi üyelerinin adı-soyadı ve unvanları	
Kişisel veri ihlal olayının tespit edildiği tarih	
Biliniyor ise, veri ihlal olayının gerçekleştiği tarih ve saat	
Kişisel veri ihlal olayını İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi'ne bildiren kişiye ilişkin bilgiler	
Kişisel veri ihlal olayının İlgili Borusan Grubu Şirketi'nin İrtibat Kişisi'ne bildirildiği tarih ve saat	
Kişisel veri ihlali veri işleyen nezdinde mi meydana geldi? Evet ise veri işleyen tarafından Şirket'e bildirim yapılan tarihi ve saati yazınız.	**Evet/Hayır** **Evetse bildirim yapılan tarih ve saat:** **Detaylar:**

Kişisel veri ihlali yurtdışında yerleşik veri sorumlusu nezdinde mi meydana geldi? Evet ise detaylarını ve Şirket'e bildirim yapılan tarihi ve saati yazınız.	**Evet/Hayır** **Evetse bildirim yapılan tarih ve saat:** **Detaylar:**
<u>Kişisel Veri Kaybının Detayları</u>	
Kişisel veri ihlali ile ilişkili BT sistemlerinin, ekipmanların, cihazların, kayıtların detayları	
Ne kadar bir veri kaybı söz konusu-İhlalin kaynağı belirlenebiliyor mu?	
Kişisel veri ihlali siber saldırı olarak mı gerçekleşti? Evet ise detaylarını yazınız	
Kişisel verinin kaybı, Şirket veya üçüncü kişiler için olumsuz operasyonel, ticari, yasal, sorumluluk veya itibar kaybı gibi sonuçlar doğuracak mı?	
Kaç ilgili kişi ve kayıt kişisel veri ihlalinden etkilendi?	
Söz konusu kişisel verilere ilişkin sözleşmesel bir veri güvenliği yükümlülüğü bulunmakta mıdır?	
İhlalden etkilenen ilgili kişi grupları kimlerdir?	

Kişisel verilerin hassasiyetinin niteliği nedir? Lütfen aşağıdaki kategorilerden birine giren her türlü bilginin ayrıntılarını sağlayın.	
YÜKSEK RİSK içerir kişisel veri - **Bir gerçek kişiye ilişkin veya ilişkilendirilebilir özel nitelikli veri** *a. Irk* *b. Etnik köken* *c. Siyasi düşünce,* *d. Felsefi inanç, din, mezhep veya diğer inançlar,* *e. Kılık ve kıyafet,* *f. Dernek, vakıf ya da sendika üyeliği* *g. Sağlık,* *h. Cinsel hayat,* *i. Ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler* *j. Biyometrik veri* k. *Genetik veri* - **Kişisel banka hesabı ve diğer finansal bilgiler gibi kimlik dolandırıcılığı yapmak için kullanılabilecek bilgiler (kimlik, pasaport fotokopisi gibi).** - **İş performansı, maaşı, özel hayatına ilişkin bilgiler dahil olmak üzere açıklanması durumunda kişiyi zarara veya sıkıntıya sokabilecek bilgiler.** - **Açıklandığı takdirde bireylerin güvenliğini tehlikeye atabilecek güvenlik/işlem güvenliği bilgileri.**	
İhlalin sınırlandırılması/önlenmesi için alınan ilk tedbirler	

İhlalin etkilerinin azaltılması için atılan adımlar	
Kişisel veri ihlallerine ilişkin tüm bilgiler, ihlalin etkileri ve alınan önlemler kayıt altına alındı mı?	

İhlal sebebiyle ilgili kişilerin önemli olumsuz etkilere maruz kalma olasılığı **Çok Yüksek** *(Kişilerin üstesinden gelemeyecekleri zorluklar ve geri dönülemez sonuçlar ile karşılaşması – örneğin uzun süreli psikolojik veya fiziksel rahatsızlık, ölüm vb.)* **Yüksek** *(Kişilerin zorluklara rağmen üstesinden gelmeleri gereken ciddi sonuçlarla karşılaşması – örneğin maddi zarar, iş kaybı, adli soruşturma, sağlığın kötüleşmesi vb.)* **Orta** *(Kişilerin zorluklara rağmen üstesinden gelebilecekleri olumsuzluklarla karşılaşması – örneğin fazla efor, ek maliyet, stres, küçük fiziksel rahatsızlıklar vb.)* **Düşük** (*Kişilerin üstesinden gelebilecekleri küçük olumsuzluklarla karşılaşması – örneğin fazla zaman harcama, sıkıntı vb.)* **Henüz Bilinmiyor**	

İhlalin Şirket'e olan etkileri **Çok Yüksek** *(Her türlü hizmet sunma yetisinin kaybedilmesi)* **Yüksek** *(Önemli hizmetleri sunma yetisinin kaybedilmesi)* **Orta** *(Bazı hizmetlerin sunumunda kontrol kaybı ve eksikliğin oluşması)* **Düşük** *(Herhangi bir etkinlik ve kontrol kaybının olmaması)* **Henüz Bilinmiyor**	
Bildirim süreçlerine ilişkin aşağıdaki sorular bu Prosedürdeki "Bildirim" aşaması sonrasında doldurulacaktır	
Kişisel veri ihlali adli makamlara bildirildi mi?	**Evet/Hayır** **Evetse, bildirim tarihi:**

Yurtdışındaki herhangi bir kişi veya kuruluşa bildirim yapıldı mı?	**Evet/Hayır** **Evetse, bildirim tarihi:** **Detaylar:**
İç iletişim süreci işletildi mi?	**Evet/Hayır** **Evetse, bildirim tarihi:** **Detaylar:**
Kurul'a bildirim yapıldı mı?	**Evet/Hayır** **Evetse, bildirim tarihi:** **Detaylar:**
İhlalden etkilenen ilgili kişilere (veri sahiplerine) bildirim yapıldı mı?	**Evet/Hayır** **Evetse, bildirim tarihi:** **Detaylar:**

Şirket dışı diğer taraflara bildirim yapıldı mı?	**Evet/Hayır** **Evetse, bildirim tarihi:** **Detaylar:**
Aşağıdaki sorular bu Prosedürdeki "Değerlendirme ve İyileştirme" aşaması sonrasında doldurulacaktır	
Tavsiye edilen/gerekli olan takip adımları	
İhlalin tekrarlanmaması için yapılması gerekenler	
İhlale ve atılan adımlara ilişkin eklenmek istenen diğer tüm açıklama ve notlar	
Tarih ve İmza **(Sürecin doğası gereği Formdaki tüm sorulara aynı anda cevap verilemeyebilir, bu nedenle Formda yapılan her bir güncellemenin açıklaması ve tarihi ayrıca kayıt altına alınmalıdır)**	