ECZACIBAŞI MONROL NÜKLEER ÜRÜNLER SANAYİ VE TİCARET ANONİM ŞİRKETİ

VERİ İHLALİ YÖNETİMİ VE MÜDAHALE PLANI POLİTİKASI

Versiyon 0.1

01.02.2022

İÇİNDEKİLER

1 GİRİŞ 3

2 TANIMLAR 3

3 AMAÇ VE KAPSAM 4

4 ROL VE SORUMLULUKLAR 4

5 VERİ İHLALİ YÖNETİMİ 5

5.1 GÜVENLİK KONTROLLERİNDE TESPİT EDİLEN VERİ İHLALLERİ 5

5.2 VERİ İHLALİNİN ŞİRKET'E BİLDİRİLMESİ 5

5.3 ŞİRKET'İN VERİ SORUMLUSU KONUMUNDA OLMASI DURUMUNDA VERİ İHLALİ YÖNETİMİ 5

5.3.1 İHLALE YÖNELİK İVEDİ ÖNLEMLERİN ALINMASI 5

5.4 ŞİRKET'İN VERİ İŞLEYEN KONUMUNDA OLMASI DURUMUNDA VERİ İHLALİ YÖNETİMİ 6

5.5 VERİ İHLALİNİN ŞİRKET İÇİNDE RAPORLANMASI 6

5.6 VERİ İHLALİNİN KURUL'A BİLDİRİLMESİ 6

5.6.1 VERİ İHLALİNİN 72 SAAT İÇİNDE KURUL'A BİLDİRİLMESİ 6

5.6.2 KURUL'A 72 SAAT İÇİNDE BİLDİRİM YAPILAMADIĞI TAKDİRDE NASIL HAREKET EDİLECEĞİ 6

5.7 VERİ İHLALİNİN VERİ SAHİPLERİ'NE BİLDİRİMİ 7

5.8 İHLALİN DİĞER ÜÇÜNCÜ KİŞİLERE BİLDİRİLMESİ 7

6 DEĞERLENDİRME 8

7 YÜRÜRLÜK TARİHİ 9

EK-1 ..... VERİ İHLALİ BİLDİRME FORMU 10

EK-2 ÖRNEK RİSK DEĞERLENDİRME RAPORU 12

1 GİRİŞ

Eczacıbaşı Monrol Nükleer Ürünler Sanayi ve Ticaret Anonim Şirketi ("**Şirket**") olağan iş faaliyetleri sırasında, pek çok Kişisel Veri'yi Veri Sorumlusu veya Veri İşleyen sıfatı ile işlemektedir. Şirket, yürütmekte olduğu Kişisel Veriler'in işlenmesi faaliyetleri esnasında başta KVKK ve Kurul kararları olmak üzere, Kişisel Veriler'in korunmasına ilişkin mevzuat uyarınca tabi olduğu kural ve yükümlülüklerin gereklilikleri ile Eczacıbaşı Monrol Nükleer Ürünler Sanayi ve Ticaret A.Ş. Kişisel Verilerin Korunması ve İşlenmesi Politikası'na uygun şekilde hareket etmek üzere azami çaba göstermektedir. Şirket'in ilgili kurallar bütünü içerisinde tabi olduğu yükümlülükler arasında veri güvenliğine ilişkin yükümlülükleri önemli bir yere sahiptir. Bu kapsamda Şirket, bir Veri Sorumlusu veya Veri İşleyen olarak işlemekte olduğu Kişisel Veriler'in; **(i)** hukuka aykırı olarak işlenmesini önlemeye, **(ii)** Kişisel Veriler'e hukuka aykırı olarak erişilmesini önlemeye ve **(iii)** Kişisel Veriler'in muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almakla yükümlüdür.

Ancak bahse konu önlemlerin alınması için azami çabanın gösterilmiş olmasına rağmen, belirli durumlar altında Şirket'in Veri Sorumlusu veya Veri İşleyen sıfatıyla işlediği Kişisel Veriler'in güvenliğine ilişkin ihlaller yaşanabilmektedir.

Bu bağlamda, Şirket, Veri Sorumlusu veya Veri İşleyen olarak, KVKK'nın 12. maddesinde belirtildiği üzere, topladığı ve işlediği Kişisel Veriler'in güvenliğini sağlamaya ilişkin olarak karar ve operasyonlarına uygun nitelikteki tüm idari ve teknik tedbirleri gerekli ve yeterli ölçüde almaktadır. Şirket tarafından işleme faaliyetlerine konu edilen verilerin KVKK'nın 6. Maddesinde, *ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler biçiminde sınırlı sayıda belirlenmiş olan* Özel Nitelikli Kişisel Veriler'den olması halinde ise KVKK'da belirtilen tedbir yükümlülüğüne ek olarak, Kurul'un *31.10.2018 tarihli ve 2018/10 sayılı özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler* ile ilgili kararda belirlediği ek önlemler de uygulanmaktadır. Şirket, söz konusu tedbirleri alma konusundaki herhangi bir ihmalin veri ihlali sonucunu doğurabileceğinin bilincindedir.

2 TANIMLAR

İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi;
Kişisel Veri/ler	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi;
Kişisel Verilerin İşlenmesi	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;
Kurul	Kişisel Verileri Koruma Kurulu;
KVKK	24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu;
Özel Nitelikli Kişisel Veri/ler	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;

Veri Güvenliği Ekibi	Veri ihlali yaşanması halinde gerekli aksiyonları almak üzere, şirket bünyesindeki departmanlardan seçilmiş belirli temsilcilerden oluşan ve Veri İhlali Yetkilisi tarafından yönlendirilen ekibi;
Veri İhlali Yetkilisi	Veri ihlali sürecinde Veri Güvenliği Ekibi'ni yönlendirmek üzere, üst yönetim tarafından şirket bünyesinden veya dışarıdan atanan; KVKK ve ilgili mevzuata hâkim ve deneyimli olan ekip lideri;
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi;
Veri Sahibi/Sahipleri	Kişisel verisi işlenen gerçek kişi;
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

3 AMAÇ VE KAPSAM

İşbu Eczacıbaşı Monrol Nükleer Ürünler Sanayi ve Ticaret A.Ş. Veri İhlal Yönetimi ve Müdahale Politikası ("**Politika**") ile amaçlanan, Şirket bünyesinde gerçekleşmesi olası ve başta Şirket'in sunduğu hizmet kalitesi olmakla birlikte, Veri Sahipleri'ne ve Şirket'in ticari itibarına önemli ölçüde zarar verebilecek veri ihlallerine karşı etkin ve hızlı bir çözüm mekanizması oluşturarak ihlalin ortadan kaldırılması için gerekli ve yeterli ölçüde aksiyon alınmasıdır.

Politika, Şirket'in Veri İşleyen veya Veri Sorumlusu sıfatıyla olağan iş faaliyetleri çerçevesinde işlediği Kişisel Veriler'in güvenliğine ilişkin gerçekleşebilecek olası ihlalleri kapsamakta ve bu kapsamda alınabilecek teknik ve idari tedbirleri belirlemektedir.

4 ROL VE SORUMLULUKLAR

Veri ihlaline ilişkin gerekli aksiyonların alınması adına, Şirket bünyesinde bir "Veri Güvenliği Ekibi" oluşturulacaktır.

Veri Güvenliği Ekibi şirket bünyesindeki şu departmanlardan birer temsilcinin, Şirket'in bağlı bulunduğu Eczacıbaşı Sağlık Grubu bünyesinde görev yapan hukuk danışmanının ve Eczacıbaşı Sağlık Grubu Kurumsal İletişim biriminde görev yapan bir temsilcinin katılımıyla oluşturulacaktır:

- Hukuk,
- Bilgi Teknolojileri,
- Kurumsal İletişim,
- İnsan kaynakları (çalışanların Kişisel Verileri'nin etkilenmesi halinde),

Bu süreçte, Şirket bünyesinden veya dışarıdan KVKK ile ilgili mevzuata hâkim ve deneyimli olan ve üst yönetim tarafından atanan bir Veri İhlali Yetkilisi, Veri Güvenliği Ekibi'ni yönlendirecektir.

Veri İhlali Yetkilisi, veri ihlali sürecinde yürütülecek işlemler için Veri Güvenliği Ekibi içerisindeki rol ve sorumluluk dağılımını yapmakla ve süreci Veri Güvenliği Ekibi ile birlikte yönetmekle yükümlüdür.

Veri ihlaline ilişkin süreçler, Şirket'in Veri Güvenliği Ekibi tarafından, Şirket bünyesinde önceden gerekli teknik ekipman desteğiyle kurulan ve güvenliği sağlanan bir komuta odası/war room'da yönetilecektir.

5 VERİ İHLALİ YÖNETİMİ

5.1 GÜVENLİK KONTROLLERİNDE TESPİT EDİLEN VERİ İHLALLERİ

Şirket tarafından yapılan güvenlik kontrollerinde, aşağıda yer alan ve benzeri durumlarla karşılaşıldığı takdirde veri ihlaline yönelik araştırma başlatılır:

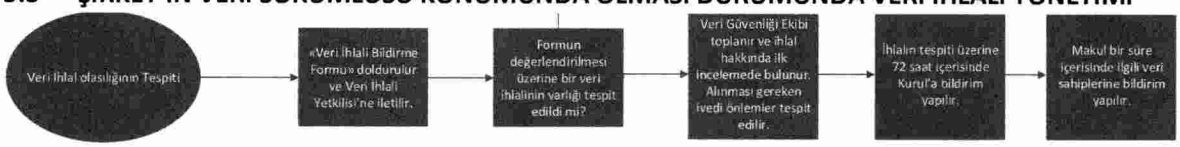
- Şirket çalışanları veya üçüncü kişi/ler tarafından Kişisel Veriler'e yetkisiz erişilmesi,
- Şirket çalışanları veya üçüncü kişi/ler tarafından Kişisel Veriler'in yetkisiz şekilde kullanımı veya ifşası,
- Şirket çalışanları veya üçüncü kişi/ler tarafından Kişisel Veriler üzerinde gerçekleştirilen yetkisiz tashih, silme veya bozma işlemleri,
- Kişisel Veriler'in yetki tanınmamış iletişim kanalları vasıtasıyla aktarımı,
- Kişisel Veriler'in yetki tanınmamış cihazlarda depolanması,
- Kişisel Veriler'in depolandığı ortamların (USB, laptop, tablet, kâğıt vb.) kaybı veya çalınması,
- Tedarikçilerin Kişisel Veriler'e ön izin olmadan erişmesi veya teknik kontrolleri ihlal etmesi,
- Kişisel Veri içeren fiziki dosyaların güvenli şekilde imha edilmemesi,
- Siber saldırılar,
- Sistem hatası,
- İnsan hatası,
- Ekipman arızası,
- Bilgisayar korsanlığı,
- Mücbir sebepler (sel, deprem, yangın vb.).

5.2 VERİ İHLALİNİN ŞİRKET'E BİLDİRİLMESİ

Şirket tarafından yapılan güvenlik kontrolleri dahilinde Şirket tarafından tespit edilen veri ihlalleri haricinde, yaşanan ihlali öğrenen kişilerin Şirket'e veri ihlal bildiriminde bulunması gerekecektir. Veri ihlali bildirimi, şirket içerisinden kişiler tarafından yapılabileceği gibi (ortaklar, yöneticiler, çalışanlar vb.) şirket dışından kişiler (tedarikçiler, Veri Sahipleri vb.) tarafından da yapılabilir. Veri ihlali bildiriminin, üst yönetim tarafından atanan Veri İhlali Yetkilisi'ne kvkk@monrol.com e-mail adresi üzerinden EK-1'de yer alan "Eczacıbaşı Monrol Nükleer Ürünler Sanayi ve Ticaret A.Ş. **Veri İhlali Bildirme Formu**" aracılığıyla mümkün olan en kısa sürede (herhalukarda 24 saat içerisinde) yapılması gerekmektedir.

İhlalin tespitiyle birlikte Şirket ilgili işleme faaliyeti bakımından Veri Sorumlusu mu yoksa Veri İşleyen mi olduğuna karar verecektir.

5.3 ŞİRKET'İN VERİ SORUMLUSU KONUMUNDA OLMASI DURUMUNDA VERİ İHLALİ YÖNETİMİ



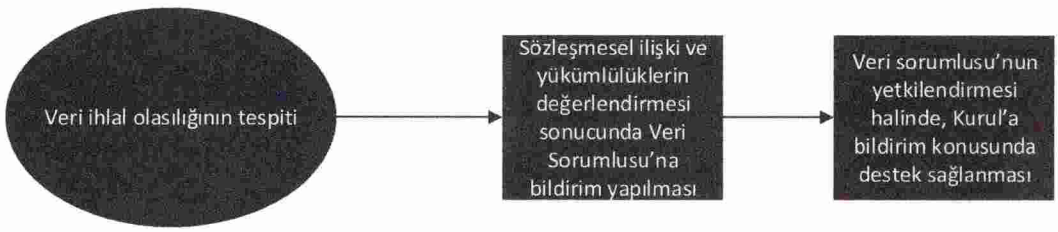
5.3.1 İHLALE YÖNELİK İVEDİ ÖNLEMLERİN ALINMASI

Yapılan veri ihlal bildirimi ile birlikte, ihlalin tespit edilmesinin ardından, ihlale yönelik şu önlemlerin ivedi şekilde alınması gerekmektedir:

1. Şirket ağındaki tehlike altında olan bölümlerin izole edilmesi veya kapatılması,
2. Bireylerin Şirket ağına ve sistemlerine erişiminin kaldırılması,
3. Etkilenen alanlara fiziksel erişimin kaldırılması,
4. İhlalden etkilenen şifre ve kodların değiştirilmesi ve etkilenen çalışanların konuya ilişkin olarak bilgilendirilmesi,

5. İhlal sebebiyle ödeme işlemlerinin etkilenmesi halinde ilgili bankaların bilgilendirilmesi,
6. İhlalin yasadışı bir faaliyete sebebiyet vermesi/verme ihtimalinin bulunması halinde polis ile irtibata geçilmesi,
7. Kaybolan Kişisel Veriler'in geri alınabilmesi için gereken aksiyonların alınması,
8. İlgili ihlalin tekrar yaşanmaması için zafiyet noktalarının belirlenmesi.

5.4 ŞİRKET'İN VERİ İŞLEYEN KONUMUNDA OLMASI DURUMUNDA VERİ İHLALİ YÖNETİMİ



Şirket'in yürütmekte olduğu ilgili işleme faaliyeti kapsamında, Veri Sorumlusu sıfatıyla değil; *başka bir üçüncü kişinin verdiği yetkiye dayanarak onun adına Kişisel Veriler'i işlemesi halinde* dolayısıyla Veri İşleyen sıfatıyla hareket etmesi halinde, Şirket öncelikle Veri Sorumlusu'nu bilgilendirme konusunda sözleşmesel bir yükümlülüğünün bulunup bulunmadığını denetleyecek; bu tür bir yükümlülüğünün bulunması halinde öncelikle sözleşme ilişkisi içerisinde bulunduğu Veri Sorumlusu'nu; daha sonra da ilgili Veri Sorumlusu'nun onu yetkilendirmesi halinde Kurul'u bilgilendirecektir.

5.5 VERİ İHLALİNİN ŞİRKET İÇİNDE RAPORLANMASI

Veri İhlali Yetkilisi, veri ihlaline ilişkin olarak kendisine mail adresi üzerinden Eczacıbaşı Monrol Nükleer Ürünler Sanayi ve Ticaret A.Ş. Veri İhlali Bildirme Formu aracılığıyla yapılan bildirimi öncelikle üst yönetime iletecektir.

Ardından Veri İhlali Yetkilisi, *bildirime konu ihlalin kapsamının, niteliğinin ve ihlalden etkilenen verilerin tür ve boyutunun tespit edilerek, gerekli koruma ve iyileştirme işlemlerine yönelik aksiyonların alınması ve ihlale ilişkin olarak 24 saat içerisinde rapor hazırlanması için ilgili bildirimi bilgi teknolojileri departmanına* iletecektir.

Veri İhlali Yetkilisi ilgili bildirimi, bilgi teknolojileri departmanı ile birlikte hukuk ve kurumsal iletişim departmanlarına da iletecektir. Bu kapsamda hukuk departmanı, veri ihlaline uğrayan Veri Sahipleri (çalışanlar, tedarikçiler, iş ortakları vb.) ile yürütülen ilişkiler bağlamında ilgili desteği sağlayacak ve veri ihlaline yönelik yazılı bir özet yayınlayacaktır.

Bu çerçevede, kurumsal iletişim departmanı, halk ve medya ilişkilerinde bildirim ve duyuruları yönetecek ve güvenlik ihlalinden etkilenen Veri Sahipleri'ne bildirimlerde bulunmak dahil olmak üzere iletişim stratejilerini geliştirip uygulayacaktır.

Buna ek olarak, Veri İhlali Yetkilisi gerçekleşen ihlalin diğer iştirakleri de etkileyen bir nitelikte olması halinde, ilgili iştiraklere de bildirimde bulunacak ve diğer iştirakler de konu ile ilgili olarak aldıkları aksiyonları Veri İhlali Yetkilisi'ne yazılı olarak ileteceklerdir.

5.6 VERİ İHLALİNİN KURUL'A BİLDİRİLMESİ

5.6.1 VERİ İHLALİNİN 72 SAAT İÇİNDE KURUL'A BİLDİRİLMESİ

Veri İhlali Yetkilisi, Kurul tarafından yayımlanan Kişisel Veri İhlali Bildirim Formu'nu doldurup ihlalin öğrenilmesinden itibaren **72 saat içerisinde** Kurul'a sunmalıdır.

5.6.2 KURUL'A 72 SAAT İÇİNDE BİLDİRİM YAPILAMADIĞI TAKDİRDE NASIL HAREKET EDİLECEĞİ

Eğer söz konusu bildirim haklı bir gerekçe ile 72 saat içerisinde gerçekleştirilemiyorsa; Veri İhlali Yetkilisi yapılacak bildirimle birlikte **gecikme nedenini** de açıklayacaktır.

5.7 VERİ İHLALİNİN VERİ SAHİPLERİ'NE BİLDİRİMİ

Veri İhlali Yetkilisi tarafından bilgi teknolojileri departmanına yapılan bildirimle birlikte, bilgi teknolojileri departmanı söz konusu ihlale ilişkin olarak şu hususları içeren bir rapor (ilgili rapor hazırlanırken işbu Politika'daki EK-2'de yer alan "Risk Değerlendirme Raporu" kullanılabilir) hazırlamalıdır:

- İhlal konusu verilerin türleri,
- İhlal konusu verilerin Özel Nitelikli Kişisel Veriler'den olup olmadığı,
- İhlalin gerçekleşme sebebi (ör. yetkisiz erişim),
- İhlalin Kişisel Veriler üzerinde ne tür bir etkiye sebep olduğu (verilerin gizliliği, bütünlüğü ve erişilebilirliği bakımından)
- Devreye sokulan güvenlik önlemleri,
- İhlale uğrayan Kişisel Veriler'in şifreli olup olmadığı,
- İhlalden etkilenen veri sahiplerinin sayısı ve ihlalin veri sahiplerine gelecekteki potansiyel etkileri.

Hazırlanan raporla birlikte ihlalden etkilenen kişilerin belirlenmesinin ardından veri sahiplerine de **makul olan en kısa süre içerisinde**, veri sahiplerinin iletişim adresine *ulaşılabiliyorsa* **doğrudan**; *ulaşılamıyorsa* Veri Sorumlusu'nun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle kurumsal iletişim departmanı tarafından bildirim yapılmalıdır.

Veri sahiplerine yapılacak bildirimlerde şu hususlara dikkat edilmelidir:

1. Sade ve anlaşılır bir dil kullanılmalı,
2. Veri Sorumlusu olarak Şirket'in tüzel kişiliğine ilişkin bilgiler sağlanmalı,
3. Veri İhlali Yetkilisi'nin kimlik ve iletişim bilgileri sağlanmalı,
4. İhlalin niteliğinin, gerçekleşme tarihinin, ihlalden etkilenen Kişisel Veriler'in tür ve içeriklerinin belirtilmesi,
5. İhlalin mevcut ve olası sonuçları hakkında öngörü sağlanması,
6. İhlale yönelik olarak Şirket tarafından alınan önlemlerin açıklanması.

5.8 İHLALİN DİĞER ÜÇÜNCÜ KİŞİLERE BİLDİRİLMESİ

Veri İhlali Yetkilisi'nin gerekli görmesi veya destek alınmasının faydalı olacağına kanaat getirmesi halinde söz konusu ihlal diğer üçüncü kişilere de (polis, diğer düzenleyici kurumlar, sigorta kurumları, bankalar veya sendikalar vb.) bildirilecektir.

Söz konusu ihlalin KVKK'nın 17. maddesi aracılığıyla atıfta bulunduğu Türk Ceza Kanunu'nun;

- **Madde 135- (1)** *Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*

  (2) *Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.*

- **Madde 136- (1)** *Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.*

- **Madde 137- (1)** *Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır.*
- **Madde 138- (1)** *Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.*

  (2) (Ek: 21/2/2014-6526/5 md.) *Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.*
- **Madde 139- (1)** *Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyete bağlıdır.*
- **Madde 140- (1)** *Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*

maddelerinde yer alan suçlardan herhangi birini teşkil etmesi halinde Veri Sorumlusu tarafından polis ve savcılığa gerekli bildirim yapılacaktır.

6 DEĞERLENDİRME

Gerçekleşen ihlale yönelik hem Şirket hem de Kurul tarafından belirlenen gerekli ve yeterli aksiyonların alınmasıyla birlikte ihlalin sona erdirilmesi halinde, Veri Güvenliği Ekibi tarafından, bilgi güvenliği tarafından hazırlanan rapor baz alınarak aşağıdaki hususlara yönelik bir değerlendirme yapılacak ve bu değerlendirme sonucunda veri ihlallerinin çözümü için Şirket bünyesinde oluşturulmuş olan mekanizma geliştirilecektir:

- Kişisel Veriler'in tutulduğu alanlar nerelerdir ve bu alanlara kimlerin erişim yetkisi bulunmaktadır,
- Mevcut koruma önlemlerinin/politikalarının zayıf noktaları nelerdir,
- Çalışanların veri güvenliğine ilişkin bilgilerinin yeterliliği,
- Veri aktarımında kullanılan yöntemlerin güvenliği hangi seviyededir,
- Söz konusu ihlalde Veri Güvenliği Ekibi etkin şekilde görevini yerine getirebildi mi,
- Getiremediyse sebep/leri nelerdir.

7 YÜRÜRLÜK TARİHİ

İşbu Politika Şirket Yönetim Kurulu tarafından onaylanarak 01.02.2022 tarihinde yürürlüğe girmiştir. KVKK ve ilgili mevzuatta ve/veya Şirket bünyesindeki iç işleyiş ve rol-sorumluluk dağılımında değişiklik olması durumlarında, yapılan değişiklikler, Şirket Yönetim Kurulu tarafından onaylandıkları tarihte yürürlüğe girer ve QDMS Kalite Yönetim Sistemi üzerinden yayımlanır.

EK-1 ECZACIBAŞI MONROL NÜKLEER ÜRÜNLER SANAYİ VE TİCARET A.Ş. VERİ İHLALİ BİLDİRME FORMU

Lütfen Eczacıbaşı Monrol Nükleer Ürünler Sanayi ve Ticaret A.Ş. bünyesinde, işbu Politika'nın "**1. GİRİŞ**" başlığı kapsamında tespit ettiğiniz herhangi bir veri ihlali bulunması halinde; ekteki formu doldurarak "**5.2. VERİ İHLALİNİN ŞİRKET'E BİLDİRİLMESİ**" başlığı uyarınca üst yönetim tarafından atanan Veri İhlali Yetkilisi'nin kvkk@monrol.com e-mail adresine iletiniz.

İHLAL BİLDİRİMİNDE BULUNANIN ADI-SOYADI:	
İHLAL BİLDİRİMİNDE BULUNANIN ŞİRKET İLE İLİŞKİSİ (ÇALIŞAN/MÜŞTERİ/TEDARİKÇİ VB.):	
İHLAL BİLDİRİMİNDE BULUNAN KİŞİNİN İLETİŞİM BİLGİSİ (Telefon numarası, adres, e-mail vb.)	
İHLALİN FARK EDİLME TARİHİ:	
İHLALİN GERÇEKLEŞME TARİHİ:	
İHLALİN GERÇEKLEŞTİĞİ ORTAM:	
İHLALİN AÇIKLAMASI VE/VEYA KAYBOLAN BİLGİLERİN DETAYLARI:	

BİLİNİYORSA İHLALDEN ETKİLENEN KİŞİ SAYISI:	
İHLALE KONU OLAN KİŞİSEL VERİ TÜRLERİ:	
VARSA ALINAN ÖNLEMLER:	
DİĞER AÇIKLAMALAR:	

1. **İhlale konu Kişisel Veriler'in işlenmesinden sorumlu kişi**

   Adı-Soyadı-departman ve iletişim bilgisi

2. **Veri İhlali Yetkilisi**

   Adı-Soyadı ve iletişim bilgisi

3. **Risk değerlendirmesinde görev alan kişi/ler**

   Adı-Soyadı- Pozisyonu

4. **Veri ihlaline yönelik açıklama**

5. **Veri ihlalinin gerçekleşme sebebi**

   - ☐ **Kişisel Veri/ler'in imhası**
   - ☐ **Kişisel Veri/ler'in kaybı**
   - ☐ **Kişisel Ver/ler üzerinde gerçekleştirilen yetkisiz tashih işlemleri**
   - ☐ **Kişisel Veri/ler'in yetkisiz ifşası**
   - ☐ **Kişisel Veri/ler'e yetkisiz erişim**
   - ☐ **Diğer:** _____

6. **İhlalin Kişisel Veriler üzerindeki etkisi**

   - ☐ **Gizlilik**
   - ☐ **Bütünlük**
   - ☐ **Erişilebilirlik**

7. **Etkilenen kişi grup ve sayıları**

   - ☐ **Çalışanlar**
   - ☐ **Müşteriler**
   - ☐ **Tedarikçiler**
   - ☐ **İş ortakları**
   - ☐ **Alt işverenler**
   - ☐ **Yönetim Kurulu Üyeleri**
   - ☐ **Çalışan Adayları**
   - ☐ **Potansiyel Müşteriler**
   - ☐ **Diğer:** _____

   - **İhlalden etkilenen kişi sayısı:**

8. **İhlalden etkilenen Kişisel Veriler:**

9. **İhlalden etkilenen Özel Nitelikli Kişisel Veriler:**

10. **İhlalin olası sonuçları:**

- ☐ **Ayrımcılık**
- ☐ **Kimlik hırsızlığı**
- ☐ **Mali kayıp**
- ☐ **İtibar zedelenmesi**
- ☐ **Ticari sır ifşası**
- ☐ **Ekonomik dezavantajlar**
- ☐ **Fiziksel bütünlüğün zarar görmesi**
- ☐ **Diğer:** _____

11. **Risk değerlendirmesinin sonucu:**

☐ **Veri sahiplerinin temel hak ve özgürlükleri zarar görmemiştir.**
Öncelik olarak Kurul'a bildirim iletilmesi

☐ **Veri sahiplerinin temel hak ve özgürlükleri kabul edilebilir seviyede zarar görmüştür.**
Öncelik olarak Kurul'a bildirim iletilmesi

☐ **Veri sahiplerinin temel hak ve özgürlükleri yüksek derecede zarar görmüştür.**
Kurul ve veri sahiplerine aynı öncelikle bildirim iletilmesi