VERİ İHLALİ MÜDAHALE PLAN YÖNETMELİĞİ

KVKK_Y2 VERSİYON 1.00

1. AMAÇ VE KAPSAM

1.1. Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi (Bundan böyle "Şirket" olarak anılacaktır) işbu Kişisel Veri İhlali Müdahale Planı, Kişisel Veri İhlali Bildirim Usul Ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyurunun "Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmesi" yönündeki hükmü doğrultusunda Şirketimizin veri güvenliği ihlallerine karşı acil eylem gerçekleştirme noktasında hazırlıklı olmasını sağlamak amacıyla alınan stratejik planlama eylemleri kapsamında kabul etmiştir. Herhangi bir ihlal durumunda uygulanacak müdahale planının odak noktası, bireyleri ve kişisel verilerini korumak için hızlı bir şekilde eyleme geçmek olacaktır. Şirketimiz öncelikle veri ihlali durumlarında şu eylemleri gerçekleştirmeyi amaçlamaktadır:

(a) Kişisel Verilerin Korunması Kurulu'na (Kurul) bir kişisel veri ihlalini gereksiz gecikme olmaksızın ve veri güvenliği ihlalinin gerçekleştiğinin farkına vardıktan sonra en geç 72 saat içinde bildirmek (kişisel veri ihlalinin doğal hak ve özgürlüklere yönelik bir risk oluşturması olası değilse bildirimde bulunup bulunmamak Şirketin ihtiyari kararına bırakılmıştır.)

(b) Kişisel veri ihlalinin gerçek kişilerin hak ve özgürlüklerine yönelik yüksek bir riskle sonuçlanma olasılığı düşük olmadığı sürece, etkilenen veri sahiplerine gereksiz gecikme olmaksızın bildirimde bulunmak.

1.2. İşbu Yönetmelik:

(a) İlgili tüm veri işleyen taraflara sirküle edilecektir. Veri işleyen sıfatını haiz olanlar Şirketimiz adına işlemekte oldukları kişisel verilerin güvenliğinin ihlal edildiğinden haberdar olur olmaz derhal tarafımıza bildirimde bulunmakla mükelleftir.

(b) Göreve başladıkları zaman çalışanlarımıza tebliğ edilerek periyodik personel toplantısı ve eğitimlerinde ele alınarak personelin Müdahale Planı hükümleri hakkında bilgi sahibi olması sağlanacaktır.

1.3. İşbu Yönetmeliğin bir parçasını oluşturan Akış Şemasında takip edilecek adımlar özetlenmiştir.

1.4. Tanımlar: İşbu Yönetmelik hükümleri bakımından geçerli olacak tanımlar aşağıda sıralanmıştır:

1.4.1. İhlalden Haberdar Olmak: Bir veri sorumlusu, kişisel verilerin güvenliğinin tehlikeye atılmasına neden olan bir güvenlik ihlali olayının meydana geldiğine dair makul bir kesinlik derecesine sahip olduğunda, veri sorumlusunun " ihlalden haberdar olduğu" kabul edilmelidir.

1.4.2. Hasar: kişisel verilerin değiştirilmiş, bozulmuş veya artık tam olmadığı hal.

1.4.3. İmha: Verilerin artık mevcut olmaması veya veri sorumlusunun herhangi bir şekilde kullanabileceği bir biçimde mevcut olmaması.

1.4.4. Kayıp: Veriler hala mevcut olabilir, ancak denetleyici veriler üzerinde sahip olduğu kontrolünü veya erişimini kaybetmiştir veya verileri artık elinde bulundurmamaktadır.

1.4.5. Kişisel Veri İhlali iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalidir;

1.4.6. "Geçici veri kaybı": kişisel verilerin bir süre için kullanılamaz hale getirilmesine neden olan olay.

1.4.7. "Yetkisiz veya yasadışı işleme", kişisel verilerin, verileri alma (veya bunlara erişme) yetkisi olmayan alıcılara ifşa edilmesini (veya bunlara erişilmesini) veya 6698 sayılı Kanunun hükümlerini ihlal eden başka herhangi bir işleme biçimini ifade eder.

1.5. Bir veri güvenliği ihlali, aşağıda sıralanan durumlar da dâhil olmak üzere çeşitli nedenlerle meydana gelebilir:

• İnsan hatası

• İçerisinde kişisel verilerin yer aldığı evrak ya da cihazların kaybı veya çalınması

• İzinsiz giriş, hırsızlık, gasp

• Yetkisiz kullanıma / erişime imkân tanıyan yetersiz erişim kontrollerinin uygulanması

• Ekipman arızası ve yetersiz sistem yedeklemeleri

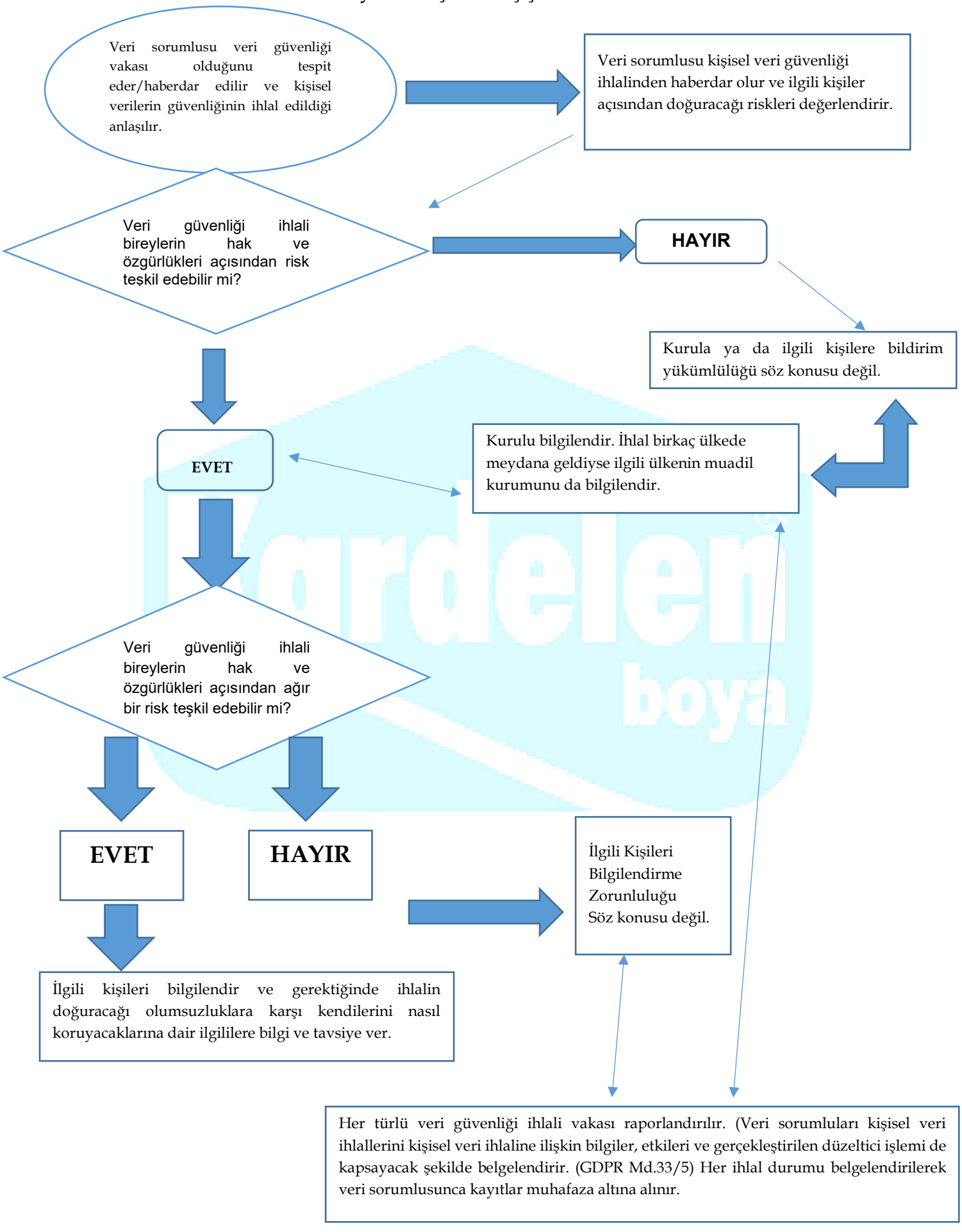
• Sel veya yangın gibi felaket halleri.

• Kişisel bilgilerin aldatma veya sahtekârlık yoluyla elde edildiği şifre avcılığı (mesaj göndererek yasadışı yollarla bir kişinin şifresini veya kredi kartı detaylarının öğrenilmesi), elektronik dolandırıcılık veya bilgi hırsızlığı

• Bilgisayar korsanlığı, zararlı yazılımlar, hizmet dışı bırakma (DoS-DDoS), veya fidye yazılımı(ransomware) saldırısı gibi kötü amaçlı siber saldırılar.

1.6. Kişisel veri ihlalleri, bireyler üzerinde fiziksel, maddi veya manevi zarara neden olabilecek olumsuz etkilere neden olabilir. Bu durumlar, veri sahibinin utanç verici duruma düşmesine, üzülmesine veya aşağılanmasına neden olabilir. Diğer olumsuz etkiler şunları içerebilir: "kişisel verilerin üzerindeki kontrolün kaybedilmesi, bireysel haklarının sınırlandırılması, ayrımcılık, kimlik hırsızlığı veya dolandırıcılığı, mali kayıp, itibarın zarar görmesi, mesleki gizlilikle korunan kişisel verilerin gizliliğinin kaybedilmesi, mağdur olan bireylerin önemli ekonomik veya sosyal dezavantajlara maruz kalması.

A. İhlal Bildirim Mükellefiyetine İlişkin Akış Şeması



1.7. Kişisel veri ihlalleri, aşağıda örnek kabilinden sıralanan durumlara neden olabileceğinden Şirketimize de zarar verebilir:

• Personel ve müşterilerimizle kurduğumuz güven ilişkisinin zedelenmesi,

• Şirketimizin yönetimi için gerekli olan kişisel verilerin kaybı, silinmesi veya zarar görmesi,

• Şirketimizin kurumsal itibarının zedelenmesi,

• Veri Koruma mevzuatı kapsamında idari yaptırımlara maruz kalmamız ya da aleyhimizde maddi/manevi tazminat davaları ve soruşturmaların açılması.

2. MÜDAHALE PLANI

Olası bir kişisel veri güvenliği ihlalinde Şirket aşağıda açıklanan müdahale planı çerçevesinde hareket edecektir:

2.1.Bir veri güvenliği ihlalinin tespiti ve ilgili görevlilerin keyfiyetten haberdar edilmesi

2.1.1. Veri Koruma İrtibat Görevlisi ya da Sorumlusu[1] en kısa süre zarfında haberdar edilecektir.

2.1.2. Veri Koruma İrtibat Görevlisi ya da Sorumlusu, Genel Müdürü derhal bilgilendirecektir.

2.1.3. Veri Koruma İrtibat Görevlisi/Sorumlusu, potansiyel hasar, kayıp, yetkisiz erişim, geçici veri kaybı gibi durumları değerlendirmek ve uygun ihlali sınırlama / durumun iyileştirilmesi ve ihlalin giderilerek ihlal öncesi duruma dönülebilmesi için gerekli önlemlerini almak üzere Siber Olaylar Müdahale Ekibi(SOME) olarak anılacak olan küçük bir ekibi bir araya getirecektir. Tüm personel ve tüm veri işleyicileri ve / veya ortak veri denetleyicileri Veri Koruma İrtibat Görevlisi/Sorumlusuna ve oluşturduğu ekipte görev alan personele gerekli tüm yardımı sağlamakla mükelleftir.

2.1.4. Veri Koruma İrtibat Görevlisi/Sorumlusu aşağı sıralanan hususlar dâhil olmak üzere ihlalle ilgili tüm hususları kaydederek yazılı bir olay kronolojisi hazırlayacaktır:

(a) İhlalin bildirildiği tarih ve saat (GG / AA / YYYY ve 24 saatlik zaman dilimi formatını kullanarak).

(b) Bildirim olası bir ihlalle ilgiliyse, bir ihlalin gerçekten meydana gelip gelmediğini belirlemek için yürütülecek ön soruşturmaya (gerekirse) dair ayrıntılar.

(c) Konuyu kimin ihbar ettiğine ilişkin ayrıntılar.

(d) Bu ilk aşamada nelerin bilindiği / nelerden şüphelenildiği.

(e) veri ihlalinin hangi sistem / veri seti ile ilişkili olduğuna dair ayrıntılar.

(f) Gerçek kişilerin hak ve özgürlüklerine yönelik riskin değerlendirilmesi.

---

[1] Veri Koruma İrtibat Görevlisi, Kurul nezdinde Şirketimizin irtibat görevlisi olarak atanan kişi olup Şirket idari teşkilatlanma yapısı dâhilinde görevlendirilen üst düzey bir yönetici, bu amaçla Şirket nezdinde istihdam edilen Veri Koruma Uzmanı ya da bu amaçla hizmet aldığımız bir hukukçu olabilir.

(g) Acil olarak alınması icap eden eylemler (soruşturma, zararın sınırlandırılması, durumun iyileştirilmesi, veri kurtarma, vb.).
(h) Yardımcı olmak için toplanan ekibin detayları.
(i) Her ekip üyesine tahsis edilen görevlerin detayları.
(j) (g) ile aynı zamanda, ihlalden haberdar olduktan sonraki 72 saat içinde Kurula yapılacak bildirim.
(k) (gerekirse) gereksiz gecikmeye yer vermeksizin etkilenen kişilere yapılacak bildirim.

2.1.5. Kurula bildirim yapılması yönünde karar alınıp alınmadığına bakılmaksızın muhtemel, rapor edilen ya da vuku bulduğundan şüphe edilen her bir kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirilecektir.

2.2. **Güvenlik İhlali Durumunun Sınırlandırılması, Etkilerinin Hafifletilmesi Ve Giderilmesine Yönelik Tedbirler**

2.2.1. Şirket derhal vuku bulan ihlalin sınırlandırılabilme amacıyla adım atacak ve muhafaza edilen kişisel verilere yetkisiz erişimin önlenmesi ve meydana gelecek zararın sınırlandırılabilmesi için gerekli tedbirleri uygulamaya koyacaktır.

2.2.2. Veri güvenliği ihlalinin Bilgi Teknolojileri (IT) sistemleri ve/veya elektronik verileri ilgilendirmesi durumunda Şirket bünyesinde IT destek hizmetleri yürüten görevlilerle derhal irtibat kurularak zararın sınırlandırılması, etkilenen veri saklama alanlarının karantinaya alınması, veriler ve log kayıtlarının muhafazası gibi alınması icap eden uygun tedbirler hususunda tavsiyeleri ve teknik desteklerinden istifade edilecektir.

2.2.3. Kişisel verilere yönelik ihlalin / tehdidin niteliğine bağlı olarak, alınması gereken tedbirler aşağıdaki adımları içerebilir:

(a) Kullanılan kişisel bilgisayarların bir kısmının ya da tamamının, ağların vb. karantinaya alınması

(b) Personelin bilgisayarlara, ağlara, cihazlara vb. erişim sağlamaması yönünde ikaz edilmesi.

(c) Kullanıcı hesaplarının askıya alınması,

(d) Yedek sunucularda tutulan kayıtların kontrol edilmesi,

(e) Potansiyel olarak hangi kişisel veri türlerinin ifşa edilmiş olabileceğinin ve yetkisiz erişim olayının nasıl meydana geldiğinin belirlenmesi.

2.2.4. Gerekli olacağının değerlendirildiği takdirde el yordamıyla ve diğer şekillerde tutulan veri kayıt alanlarının da karantinaya alınması düşünülebilir.

2.2.5. Gerekli hallerde IT suç araştırma ekibinden yararlanılması ve hukuki danışmanlık hizmetlerinden istifade edilmesi düşünülebilir.

2.3. Risk Analizi

2.3.1. Şirket bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet verip vermediği yönünde kapsamlı bir risk analizi yapmakla mükelleftir.

2.3.2. Değerlendirmeye esas olacak risk kategorileri aşağıdaki gibidir:

- Risk Yok: Uygun teknik ve idari koruma tedbirleri uygulaması ve kişisel verilerin bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirlerle korunmuş olması, veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alınmış olması
- Düşük Risk: İlgili kişiler üstesinden gelebilecekleri küçük çaplı olumsuzluklarla karşılaşabilirler (fazla zaman harcama, sıkıntı vb.)
- Orta Risk: İlgili kişiler, üstesinden gelebilecekleri olumsuzluklarla karşılaşabilirler. (fazla efor, ek maliyet, stres, küçük fiziksel rahatsızlıklar vb.)
- Yüksek Risk: Yüksek: İlgili kişiler üstesinden gelmeleri gereken ciddi sonuçlarla karşılaşabilirler.(Maddi zarar, iş kaybı, adli soruşturma, sağlığın kötüleşmesi vb.)
- Çok Yüksek Risk: İlgili kişiler, üstesinden gelemeyeceği zorluklar ve geri dönülemez sonuçlar ile karşılaşabilir(İşin durması, uzun süreli psikolojik ve fiziksel rahatsızlık, ölüm vb.)

Gerçek kişilerin hakları ve özgürlükleri açısından herhangi bir risk gerçekleşmeyeceği değerlendiriliyor ise bu değerlendirmeye varılmasına neden olan sebepler kayıt altına alınacaktır.

2.3.3. Riski analizi yaparken, Şirket, ihlal nedeniyle daha büyük risk altında olup olmayacaklarını belirlemek için verilerin hassasiyet düzeyini ve ilgili kişi kategorilerini (örneğin çocuk, savunmasız kişi) dikkate alacaktır.

2.3.4. Kişisel verilerin son teknolojik şifreleme yöntemleriyle ile güvenli bir şekilde şifrelenmiş olması ve herhangi bir güvenlik ihlalinde anahtarların tehlikeli bir duruma düşmemiş olmaması gibi durumlar veri ihlalinin gerçek kişilerin hak ve özgürlüklerine yönelik bir risk doğurmayacağı ve Kurulu ve veri sahiplerini bilgilendirmenin gerekli olmayacağı yönünde değerlendirme yapılmasına esas teşkil edebilir.

2.3.5. Şirket risk analizi değerlendirmesinde Kurul ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile Avrupa Ağ ve Bilgi Güvenliği Ajansının[2] (European Union Agency for Network and Information Security-ENISA) tavsiyelerini dikkate alacaktır.

2.3.6. Kurulu ve veri sahiplerini bilgilendirmenin gerekli olmayacağı yönünde değerlendirme yapılmışsa bu kararın alınmasına neden olan sebepler belgelendirilecek ve Kurul tarafından yapılabilecek denetimlerde ibraz edilmek üzere bahse konu dokümantasyon muhafaza altına alınacaktır.

[2] www.enisa.europa.eu/publications/dbn-severity

2.4. İlgili Kurum ve Kişilere İhlale İlişkin Bildirim Yapılması

2.4.1. Veri Güvenliği İhlali Olaylarınının Kişisel Verilerin Korunması Kuruluna bildirilmesi: Kişisel verilerin ve hassas kişisel verilerin riske girebileceği tüm olaylar, (veri sahiplerinin hak ve özgürlüklerine yönelik bir risk oluşturmayacak durumlar bu kapsama dâhil değildir) gereksiz gecikmeler olmaksızın ve ihlal durumundan haberdar olunduktan itibaren en geç 72 saat içerisinde Kurula bildirilecektir.

2.4.2. **KVKK KİŞİSEL VERİ İHLALİ BİLDİRİM FORMUNUN DOLDURULMASI**: Kişisel Verileri Koruma Kurumunun internet sayfası olan www.kvkk.gov.tr adresine giriş yapıldıktan sonra Anasayfa'da sağ taraftaki menüler içerisinde yer alan Kişisel Veri İhlal Bildirimi ikonuna tıklanarak kişisel veri ihlal bildirimi alanına giriş yapılacaktır.

2.4.3. Giriş yapılan sayfada "KİŞİSEL VERİ İHLALİ BİLDİRİM USUL VE ESASLARINA İLİŞKİN KİŞİSEL VERİLERİ KORUMA KURULUNUN 24.01.2019 TARİH VE 2019/10 SAYILI KARARINA İLİŞKİN DUYURU" yer almaktadır. Söz konusu duyuru sayfasının altında yer alan Kişisel Veri İhlal Bildirim Formuna (İnternet) tıklanarak bildirim sayfasına geçilebilmektedir. Form el ile doldurulmak isteniyorsa Kişisel Veri İhlal Bildirim Formuna (PDF) tıklanır.

2.4.2. Kurula yapılacak olan bildirimde asgari olarak aşağıda sıralanan hususlara yer verilecektir:

- İhlalin kaynağı ve nasıl gerçekleştiği hakkında bilgi
- İhlalden etkilenen birey grupları (örneğin çocuk, diğer hassas gruplar, engelli kişiler, çalışanlar, müşteriler).
- Veri ihlalinden etkilenen kişi ve kayıt sayısı.(En azından tahmini olarak)
- İhlalden etkilenen kişisel veri kategorileri (Örneğin kimlik bilgileri, eğitim kayıtları, sosyal güvenlik verileri, mali bilgiler, banka hesap numaraları, pasaport numaraları ve sağlık verileri, ırk ve etnik köken gibi özel nitelikli veriler)
- Veri Koruma İrtibat Görevlisi/Sorumlusunun isim ve irtibat bilgileri (ayrıntılı bilginin elde edilebileceği görevli bilgileri)
- İhlalin ilgili kişiler üzerindeki olası etkilerinin tarifi (Örneğin kişisel veriler üzerinde kontrol kaybı, kimlik hırsızlığı, ayrımcılık, hakların kısıtlanması, dolandırıcılık, finansal kayıp, itibar kaybı, mesleki gizli bilgilerin ifşa olma riski vb).
- Şirket tarafından ihlalden önce alınan idari ve teknik tedbirler ile ihlale müdahale etmek için alınan ya da alınması planlanan tedbirlerin tarifi. (Örneğin yanlışlıkla gönderilmiş olan verilerin yok edilmesi, şifrelerin güvenliğinin sağlanması, veri güvenliği eğitiminin planlanması vb.)Mümkünse ihlalin olumsuz etkilerinin azaltılması yönünde alınan tedbirler de bu başlığa eklenecektir.
- Önemli Not: Yukarıda sıralanan hususlara dair kesin bilgilere henüz ulaşılamıyor olması Kurula zamanında bildirimde bulunma noktasında gecikmeye neden olmamalıdır. Mevcut bilgiler aktarılarak daha ayrıntılı bilgilere ulaşıldığında derhal kuruma bildirileceği hususu belirtilmelidir.

2.4.3. Veri ihlali ile ilgili yurtdışında bulunan yargının, kolluk kuvvetlerinin veya diğer kamu kurumlarının görev alanına giren bir husus olduğu durumlarda ve bu ihlal hakkında bu

yurtdışında bulunan organizasyon veya kurumlara bilgi verilmesi gerekebilir. Bildirimde bulunulması durumunda bildirim yapıldığını tevsik edici belgeler kayıt altına alınarak Kurula yapılacak bildirimde ibraz edilmelidir.

2.4.4 Şirketin Bildirimde Bulunma Nedenleri:

(a) İdari para cezasından kaçınma: 6698 sayılı Kişisel Verilerin Korunması Kanununun 18. Maddesi uyarınca Kurula bildirimde bulunulmaması idari para cezasına neden olabilir.

(b) Tavsiye Alma: Şirket yaşanan ihlal karşısında alınacak tedbirler konusunda Kuruldan tavsiye alabilir ve etkilenen veri sahiplerini bilgilendirme veya bildirmeme hakkında verilen kararlarının gerekçelendirilebilmesi hususunda Kurulla yapılacak işbirliği önem arz etmektedir.

2.4.5. İhlalden Etkilenen İlgili Kişilerin Bilgilendirilmesi

2.4.5.1. Yukarıda yer alan 2.3.1 başlığında zikredilen risk analizi yapıldıktan sonra, kişisel veri ihlalinin gerçek kişilerin hak ve özgürlükleri için "yüksek risk" oluşturması muhtemel ise, Şirket:

(a) İlgili kişilerle telefon, e-posta vb. yollarla gereksiz bir gecikmeye mahal vermeksizin iletişim kuracaktır.

(b) Bir veri ihlali meydana geldiği ilgili kişilere bildirecektir.

(c) Veri sahiplerine yukarıda 2.4.2 başlığı altında açıklanan hususlar hakkında ayrıntılı bilgileri sağlayacaktır.

(d) Uygun olduğu durumlarda, veri sahiplerinin ihlalin olası olumsuz sonuçlarından kendilerini koruyabilmeleri için (şifrelerin yeniden belirlenmesi gibi) spesifik tavsiyelerde bulunacaktır.

2.4.5.2. Veri sahibine ilişkin bildirimde kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanacak ve en azından veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgileri, kişisel veri ihlalinin olası sonuçları, uygun olduğu hallerde, kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dâhil olmak üzere kişisel veri ihlalinin ele alınması için Şirketimiz tarafından alınan veya alınması önerilen tedbirlere dair açıklamalara yer verilecektir.

2.4.6. Aşağıdaki koşulların herhangi birinin yerine getirilmesi durumunda veri sahibine bildirim yapılması zorunlu değildir:

(a) Şirketin uygun teknik ve idari koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirler başta olmak üzere bu tedbirlerin kişisel veri ihlalinden etkilenen kişisel verilere uygulanmış olması;

(b) Şirketin veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alması;

(c) bildirimin ölçüsüz bir çaba gerektirecek olması. Bu durumda, bunun yerine, veri sahiplerinin aynı etkililikle bilgilendirildiği kamuya yönelik bir bildirim veya benzeri bir tedbir uygulanır.

2.4.7. Kolluk Kuvvetlerine Bildirim

(a) Kişisel verilere yetkisiz erişildiğinde, konu derhal ilgili kolluk birimine bildirilecektir.

(b) Risk altındaki kişisel verilerin niteliğine bağlı olarak ve özellikle hassas kişisel verilerin risk altında olabileceği durumlarda, kolluktan daha fazla yardım istenmelidir.

(c) Verilerin "zarar görmesi" durumunda konu kolluk kuvvetlerine bildirilmelidir. Bunun yapılmaması, Şirketi ceza ve güvenlik tedbirlerine maruz bırakabilir.

2.4.8. Diğer Kurum ve Kuruluşlar: Gerekli olması halinde Sağlık Bakanlığı, Aile ve Sosyal Politikalar Bakanlığı, finans kuruluşları ve diğer ilgili bakanlık ve kuruluşlara bilgi verilmesi gerekebilir.

2.4.9. Şirket sigortalı sözleşmesi akdedilen sigorta şirketine bildirimde bulunacak ve bir kişisel veri güvenliği ihlali olduğunu bildirecektir.

2.5. Hukuki Danışmanlık ve Avukatlık Hizmetlerinden Yararlanılması: Şirket, hukuki danışmanlık ve avukatlık hizmeti aldığı paydaşları bilgilendirebilir ve hukuki danışmanlık ve açılacak davalarda savunma yapılması, uzlaşma veya sair dostane çözüm yolları bulunması amacıyla kişisel veri güvenliği ihlali olduğunu bildirebilir.

2.6. İhlal Sonrası Yapılacaklar: İlk aşamada uygulanması gereken acil müdahale tedbirleri alındıktan sonra makul bir süre içerisinde ihlalle ilgili eksiksiz bir değerlendirme ve gözden geçirme süreci işletilmelidir. Bu süreçte aşağıda sıralanan hususlar göz önünde bulundurulacaktır:

2.6.1. Kişisel veri ihlallerinin kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirilmiş olduğu teyit edilecektir.

2.6.2 yaşanılan hadiseden çıkarılan sonuçlar, geliştirilmesi gereken boyutlar ve önlemlerin ayrıntıları belirlenmelidir.

2.6.3 Şirket, Veri Koruma İrtibat Görevlisi/Sorumlusundan (ve / veya kendisine yardımcı olmak için deneyimlerinden istifade edilecek diğer harici uzmanlardan) uygun bir brifing ve araştırma raporu isteyecek ve Kurul ve / veya ihlalden etkilenen ilgili kişilerle karşılıklı olarak yapılan yazışmaların bir kopyası saklanacaktır.

2.6.4 Şirket, gerektiği takdirde disiplin prosedürlerinin başlatılıp başlatılmaması konusunda dikkatli bir değerlendirme yapacaktır.

2.6.5 İyileştirici eylemlerin uygulanmasının gerekli olduğu durumlarda, sorumluluk ilgili görevlilere verilecek ve sorumluluk alanlarına göre gerekecek eylemlerin belirli zaman dilimleri içinde tamamlanmasını sağlamak için görevlendirilmeleri sağlanacaktır.

2.6.6 Personel, bu Müdahale Planında yapılacak değişikliklerden ve güncellenecek güvenlik önlemlerinden haberdar edilmelidir. Personel gerektiğinde tazeleme eğitimi almalıdır.

EK-ÖRNEK İHLAL BİLDİRİM RAPORU
VERİ GÜVENLİĞİ İHLALİ BİLDİRİM RAPORU

KARDELEN BOYANIN KULLANIMINA MAHSUSTUR

Kişisel Veri İhlali: İletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalini ifade eder.

İhlal Takip Numarası:	
Veri güvenliği ihlali ne zaman gerçekleşti?	
Veri güvenliği ihlali nerede gerçekleşti?	*İhlalin Gerçekleştiği yer*
İhlalden ne zaman haberdar olundu?	*Tarih ve Zaman belirtiniz.*
Güvenlik İhlali kim tarafından bildirildi?	
Veri ihlalini rapor eden kişinin irtibat bilgileri?	
Kişisel Veri Koruma Kuruluna bildirim yapıldı mı?	**Evet □ Hayır □**
Eğer cevap "Evet" ise bildirim şekli(telefon, e-mal vb) ile bildirimin gün ve saatini belirtiniz	
Cevap "Hayır" ise, başka herhangi bir üst düzey yetkili, Direktör vb. ile iletişime geçildi mi ve iletişime geçildi ise, hangi yollarla (örneğin telefon, e-posta vb.) Ve kurulan iletişimin saati ve tarihi?	
Olayla ilgili tanık var mıdır? Cevap "Evet" ise, İsimleri ve telefon iletişim bilgilerini belirtiniz.	

İhlalin Kaynağı hakkında bilgi veriniz.
İhlalin nasıl gerçekleştiği hakkında detaylı bilgi veriniz.
İhlalden etkilenen ya da etkilenmesi muhtemel olan ilgili kişi kategorileri hakkında bilgi veriniz. (Stajyer, çalışan, çalışan adayı, müşteri, tedarikçi, yüklenici firmalar vb.)
Veri ihlalinden etkilenen ya da etkilenmesi muhtemel kişi ve kayıt sayısı nedir?(Kişi ve/veya Kayıt Sayıları tahmini ise kesin sayıların tespit edilememe nedenini açıklayınız)
İhlalden etkilenen kişisel veri kategorileri nelerdir? (Kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlemleri, fiziksel mekân güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, pazarlama, görsel ve işitsel kayıtlar, ırk ve etnik köken, siyasi düşünce, felsefi inanç, kılık kıyafet, dernek üyeliği, sağlık bilgileri, ceza mahkûmiyeti ve güvenlik tedbirleri, biyometrik veri vb.)

İhlalin ilgili kişiler üzerindeki olası etkilerini tarif ediniz.(Kişisel veriler üzerinde kontrol kaybı, kimlik hırsızlığı, ayrımcılık, hakların kısıtlanması, dolandırıcılık, finansal kayıp, itibar kaybı, kişisel verilerin güvenliğinin kaybı vb.)
Kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dâhil olmak üzere kişisel veri ihlalinin ele alınması için Şirket tarafından alınan veya alınması önerilen tedbirleri açıklayınız. Önemli Not: Yukarıda zikredilen tedbirlere dair ayrıntılara henüz vakıf olunmaması, Kişisel Veri Koruma Kuruluna bildirimde bulunmaktan imtina edilmesini haklı kılmayacaktır. Bilgiler gereksiz herhangi bir ek gecikmeye mahal verilmeksizin aşamalı olarak sağlanabilir. Böyle bir durum varsa açık bir şekilde belirtiniz.
Size göre veri güvenliği ihlali geçici bir durum mudur? Güvenliği ihlal edilen kişisel verilerin kurtarılması ve yeniden erişiminin kontrol altına alınması mümkün müdür?

Herhangi bir IT sistemi olaydan etkilendi mi? (Örneğin e-mail, web sitesi, bulut programları, elektronik belge yönetim sistemleri vb.) Etkilendi ise liste halinde aşağıya sıralayınız.
Hata mesajları, ekran görüntüleri (screen shot), log dosyaları, CCTV görüntü kayıtları gibi Ek bilgi materyalleri mevcut mudur?
Şimdiye kadar etkilendiğini düşündüğünüz veri sahibi ilgili kişiler veya etkilenmiş olabileceğini düşündüğünüz diğer ilgili kişiler için oluşabilecek riskleri ortadan kaldırmak / azaltmak için herhangi bir eylemde bulundunuz mu? Cevabınız "EVET" ise, lütfen aşağıda açıklayın.
Şirket Yönetim Kurulu üyesi ya da İcra Müdürü, IT Departmanı Şefi gibi yönetici personeli konu hakkında bilgilendirdiniz mi? Eğer cevap "EVET" ise lütfen kiminle görüştüğünüzü ve görüşme sırasında size verilen tavsiye ya da talimatları kısaca açıklayınız.
Herhangi bir Şirket harici kurumla, örn. Sigorta Şirketi, BT sağlayıcısı, kolluk kuvvetleri vb. ile irtibat kurdunuz mu? Cevap "EVET" ise, lütfen aşağıda kiminle iletişime geçtiğinizi açıklayın ve bunların adını ve iletişim bilgilerini yazınız. .

Başkaca açıklamak istediğiniz bir husus varsa lütfen aşağıda belirtiniz.

Düzenleyen:	
Göreviniz:	
Görevli Olunan Birim:	
İrtibat Bilgileriniz: (İdeal olarak telefon numaranız)	
Tarih:	
Rapor Bitiş Saati:	

Bu formu doldurmak için gösterdiğiniz çabadan ötürü teşekkür ederiz. Bu formun tanzim edilmiş olması Kardelen Boyanın konuyu daha iyi araştırmasına / analiz etmesine yardımcı olacaktır.
Lütfen işbu Raporun doğrudan Şirketin Veri Koruma İrtibat Görevlisine/Sorumlusuna iletildiğinden emin olun:
Veri Koruma İrtibat Görevlisi/Sorumlusu:
Adı Soyadı:
Görevi:
Adres:
Telefon:
E-mail:

***BU FORM HUKUK VE CEZA DAVALARI GÖZ ÖNÜNDE BULUNDURULARAK HAZIRLANMIŞTIR**.

BİLGİNİZ İÇİN:

Veri güvenliği ihlalleri aşağıda sıralanan genel kabul gören bilgi güvenliği prensiplerine göre sınıflandırılmaktadır:

A) Veri Gizliliği: Verinin yetkisiz kişilerce ele geçirilmesinin engellenmesidir. Gizlilik ihlali" - kişisel verilerin yetkisiz veya yanlışlıkla ifşa edilmesi veya bunlara erişim olması durumunu ifade eder.
B) Veri Bütünlüğü: Verinin olması gerektiği şekilde tutulması ve korunmasıdır. "Bütünlük ihlali" - kişisel verilerde yetkisiz veya kazara değişiklik olması durumunu ifade eder.
C) Veriye Erişebilirlik/Ulaşılabilirlik: Verinin her an ulaşılabilir ve kullanılabilir olmasıdır. "Erişim ihlali" - kişisel verilere erişimin kazara veya yetkisiz olarak kaybedilmesi veya kişisel verilerin kazara ya da yetkisiz kişilerce yok edilmesi durumunu ifade eder.

Koşullara bağlı olarak, veri güvenliği ihlali kişisel verilerin gizliliği, bütünlüğü ve erişilebilirliği ile ya da bunların bir kaçının aynı anda gerçekleşmesi ile meydana gelebilir. Bir gizlilik veya bütünlük ihlali olup olmadığının belirlenmesini sağlayacak bilgiler nispeten açık bir şekilde görülebilir. Fakat verilerin erişilebilirlik durumunun ihlal edilip edilmediğini belirlemek daha zor olabilir. Kişisel veriler kalıcı olarak kaybedildiğinde veya yok edildiğinde, her zaman veri erişilebilirliği ilkesinin ihlal edildiği kabul edilecektir.

GÜVENLİK İHLALLERİNE MÜDAHALE EDERKEN YAPILMASI VE YAPILMAMASI GEREKENLER:

YAPILMASI GEREKENLER:

- Daha fazla izinsiz giriş, verilerin ifşa edilmesi, kayıt sistemlerinin hasar görmesi vb. durumları önlemek için etkilenen sistemi hemen izole edin.
- İletişim için telefon kullanın. Saldırganlar, e-posta trafiğini izleyebilir.
- Gecikmeden Şirketin Veri Koruma İrtibat Görevlisi/Sorumlusu ile iletişime geçin.

  Veri Koruma İrtibat Görevlisi/Sorumlusu:
  Adı Soyadı:
  Görevi:
  Adres:
  Telefon:
  E-mail:
- İlgili tüm log kayıtlarını muhafaza altına alınız, ör. Güvenlik duvarı, yönlendirici(router) ve saldırı tespit sistemi.
- Hasarlı veya değiştirilmiş dosyaların yedek kopyalarını oluşturun ve bu yedeklemeleri güvenli bir yerde saklayınız.
- Etkilenen sistemin ağ topolojisi içinde nerede bulunduğunu belirleyiniz.
- Etkilenen sisteme bağlanan tüm sistemleri ve birimleri belirleyiniz.
- Etkilenen sistem (ler) üzerinde çalışan programları ve süreçleri, kesintinin etkisini ve izin verilen maksimum kesinti süresini belirleyiniz.
- Etkilenen sistemin kanıt olarak toplanması durumunda, hizmetlerin devamlılığını sağlamak için düzenlemeler yapın, yani yedekli sistem hazırlayın ve veri yedeklerini alınız.

YAPILMAMASI GEREKENLER:

- Etkilenen istemlerde yer alan dosyaları silmeyiniz, başka bir konuma taşımayınız ya da üzerlerinde değişiklik yapmayınız.
- Şüpheli saldırganlarla irtibat kurmayınız.
- Görevlendirilmemiş iseniz dijital suç analizi yapmayınız.

YALNIZCA SOME-VERİ İHLALİ MÜDAHALE EKİBİNCE DOLDURULACAKTIR

Veri Koruma İrtibat Görevlisi/Sorumlusu:		
İşbu Formun Şirkete Teslim Tarihi Ve Saati:		
Veri güvenliği ihlalinin etkisini belirtiniz *Veri Gizliliği, Veri Bütünlüğü, Veriye Erişim /ulaşılabilirlik (Bkz. yukarıdaki açıklamalar)*		
Veri İhlalinden Etkilenen Kişi ve Kayıt Sayısı	*Tahmini ihlalden etkilenen kişi ve kayıt sayısı?* *Etkilenen veri kategorileri?*	
Veri ihlali nedeniyle özel nitelikli kişisel veriler (Irk ve etnik köken, Siyasi Düşünce, Dini, felsefi inanç, mezhep ve diğer inançlar, Dernek, sendika üyeliği, Biyometrik ve genetik veri, Sağlık Bilgileri, Cinsel Hayat) etkilendi mi?	**Evet □ Hayır □** *İlgili bilgileri aşağıya yazınız. Örneğin ne kadar veri sahibi ilgili kişi(ler)nin özel nitelikli verisi ihlalden etkilendi? İhlale konu olan özel nitelikli kişisel veriler nelerdir?*	
İlgili kişilerin olumsuz etkilere maruz kalma olasılığı" *İletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalinin düzeyinin belirlenmesinde ilgili kişiler üzerinde ne kadar bir potansiyel etkiye neden olduğu değerlendirilmelidir. Söz konusu etkinin değerlendirilmesinde ise ihlalin niteliği, nedeni, ihlale maruz kalan verinin türü, ihlalin etkisinin azaltılması için alınan tedbirler ile ihlalden etkilenen ilgili kişi kategorileri göz önünde bulundurulmalıdır.* **** Risk olmadığı değerlendiriliyorsa sebeplerini açıklayınız:***		**Çok Yüksek**: İlgili kişiler, üstesinden gelemeyeceği zorluklar ve geri dönülemez sonuçlar ile karşılaşabilir(İşin durması, uzun süreli psikolojik ve fiziksel rahatsızlık, ölüm vb)
		**Yüksek**: İlgili kişiler üstesinden gelmeleri gereken ciddi sonuçlarla karşılaşabilirler.(Maddi zarar, iş kaybı, adli soruşturma, sağlığın kötüleşmesi vb.)
		**Orta**: İlgili kişiler, üstesinden gelebilecekleri olumsuzluklarla karşılaşabilirler. (fazla efor, ek maliyet, stres, küçük fiizksel rahatsızlıklar vb.)
		**Düşük**: İlgili kişiler üstesinden gelebilecekleri küçük çaplı olumsuzluklarla karşılaşabilirler (fazla zaman harcama, sıkıntı vb.)
		**Risk Yoktur**: Uygun teknik ve idari koruma tedbirleri uygulaması ve kişisel verilerin bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirlerle korunmuş olması, veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alınmış olması.

Yönetim kurulunda görevli üst düzey yöneticiler bilgilendirildi mi?	**Evet □ Hayır □**
IT Hizmet Sağlayıcı/IT Teknik Destek Ekibi Bilgilendirildi mi?	**Evet □ Hayır □**
Sigorta şirketine bilgi verildi mi?	**Evet □ Hayır □**
Kolluk kuvvetlerine ihbar/şikâyet yapıldı mı?	**Evet □ Hayır □**
Hukuk danışmanlarına bilgi verildi mi?	**Evet □ Hayır □**
İlgili kişilere bilgi verildi mi? *İlgili kişi sayısı?* *İlgili kişilere ulaşmamızı sağlayacak irtibat bilgisi listeleri var mı? Yoksa irtibat bilgilerinin kurtarılması mümkün mü?*	**Evet □ Hayır □**
Kişisel Veri Koruma Kuruluna Bildirim Yapıldı mı? *Kişisel Verileri Koruma Kurumu* *Telefon: 0312 216 50 00* *Çağrı Merkezi: ALO 198 Veri Koruma Hattı* *Bilgi Danışma Merkezi* *E-mail: veriguvenligi@kvkk.gov.tr* *İhlal Bildirim Formunun Yer Aldığı Web Sayfası:https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi* *Adres: Nasuh Akar Mahallesi 1407. Sok. No:4, 06520 Çankaya/Ankara*	**Evet □ Hayır □** *Cevap "EVET" ise bildirimin tarih ve saati ile (varsa) Kurumdan alınan tavsiye ve talimatları aşağıya yazınız:*
Belirtilmek İstenen Başkaca Hususlar	
Veri Koruma İrtibat Görevlisi/Sorumlusunun İmzası:	
İcra Kurulu Başkanı ya da Atadığı Temsilcinin İmzası:	
Tarih:	

***BU FORM HUKUK VE CEZA DAVALARI GÖZ ÖNÜNDE BULUNDURULARAK HAZIRLANMIŞTIR.**