ERKUNT TRAKTÖR SANAYİİ A.Ş.

VERİ İHLALİ MÜDAHALE PLANI

İÇİNDEKİLER

1.AMAÇ

6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir, Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmüne amirdir.

İşbu "Kişisel Veri İhlali Müdahale Planı" (Plan), 24.01.2019 Tarih ve 2019/10 Sayılı Kişisel Verileri Koruma Kurulu kararı gereğince hazırlanmıştır. Bu Plan; kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, kişisel veri ihlali olması durumunda oluşacak krize nasıl müdahale edileceği ve atılacak adımların neler olduğu konusunda çalışanları bilgilendirmek ve veri sorumlusunun müdahale sürecinde benimsenecek ve uygulamada dikkate alınacak faaliyetleri belirlemek amacıyla **ERKUNT TRAKTÖR SANAYİİ A.Ş.** ("Şirket") tarafından hazırlanmıştır.

2. KAPSAM

Kişisel veri ihlalleri; iletilen, saklanan veya işlenen kişisel verilerin kazara veya hukuka aykırı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik açığı şekillerinde ortaya çıkabilen ihlallerdir.

Aşağıda yer alan durumlar genel olarak kişisel veri ihlali olarak nitelendirilir:

• Gizli bilgilerin hukuka aykırı şekilde ifşası,

• Kişisel veri içeren e-postaların yanlışlıkla Şirket dışında ilgisiz kişilere iletilmesi, gönderimi,

• Bilgi işlem donanımlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin siber saldırı) gerçekleşmesi suretiyle kişisel verilere hukuka aykırı erişim sağlanması,

• Kişisel veri içeren fiziki belgelerin veya elektronik cihazların çalınması veya kaybolması,

• Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi.

Yukarıda belirtilen durumlar örnek mahiyetindedir. Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Plan kapsamında olup, Şirketimizce yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Plan uygulanır.

3.TANIMLAR VE KISALTMALAR

İşbu Veri İhlali Müdahale Planında kullanılan ve önem teşkil eden tanımlar aşağıda yer almaktadır:

İLGİLİ KİŞİ: Kişisel verisi işlenen gerçek kişiyi (Ör: Müşteriler, ziyaretçiler, çalışanlar ve çalışan adayları),

KİŞİSEL VERİ: Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi (Örn: İsim-Soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.),

KİŞİSEL VERİLERİN İŞLENMESİ: 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 işlemi,

VERİ İŞLEYEN: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişiyi,

VERİ SORUMLUSU: Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi,

KVK KANUNU: 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu

KVK KURUMU: Kişisel Verileri Koruma Kurumu'nu

KVK KURULU: Kişisel Verileri Koruma Kurulu'nu

KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİNE İLİŞKİN YÖNETMELİK: 20 Ekim 2016 tarihli ve 29863 sayılı Resmi Gazete'de yayımlanan, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğini ifade etmektedir.

4. SORUMLULUKLAR

ERKUNT TRAKTÖR; işbu planın şirketteki faaliyet ve süreçlerde uygulanması, teknik ve hukuki yönden Kanun'da açıklanan risklerin önlenmesi amaçlarıyla gereken her türlü tedbiri almakla ükümlüdür.

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.

5. VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

KVKK'nın 12. Maddesinde, İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu tarafından alınması gereken önlemler tanımlanmıştır.

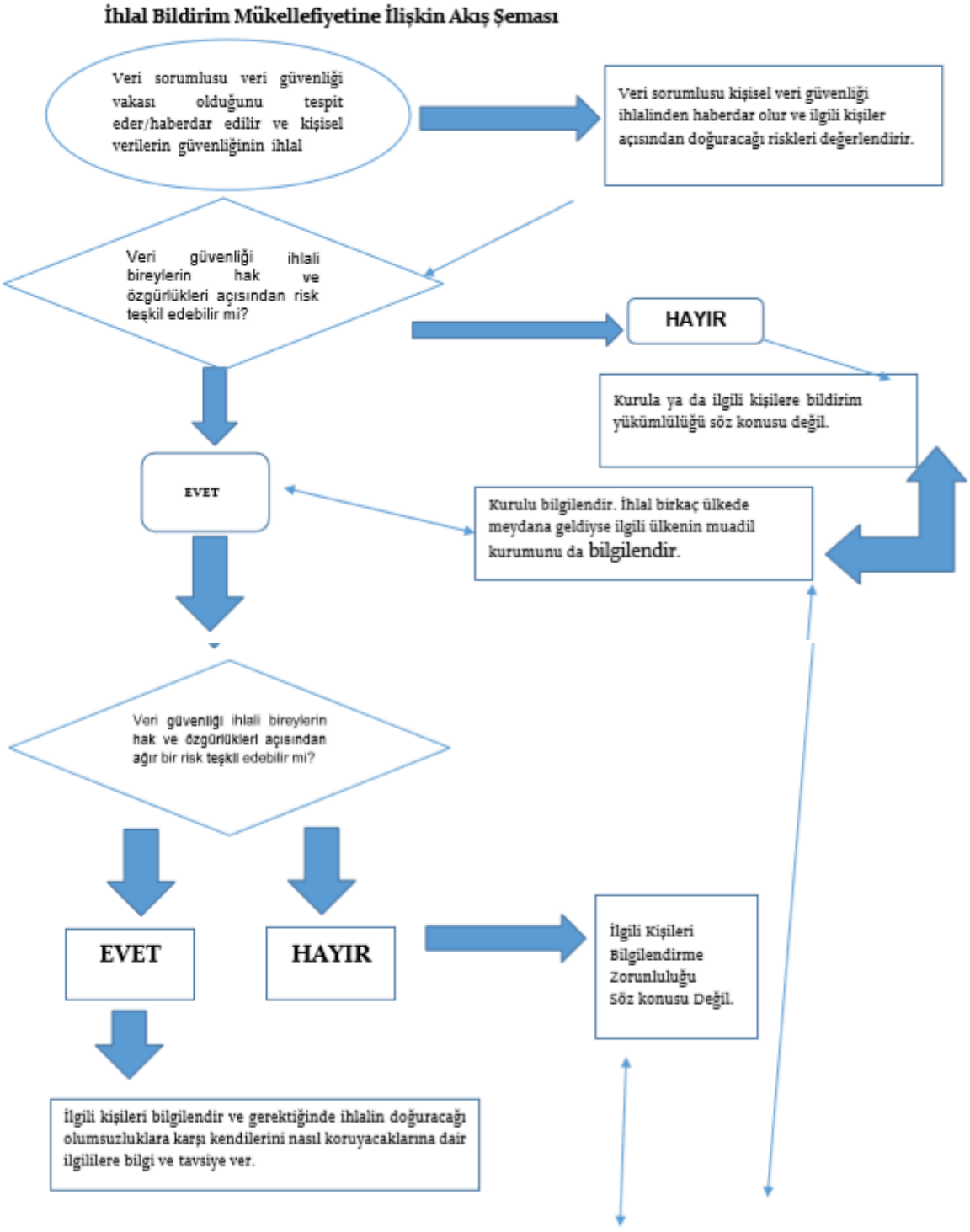
Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

6- İHLAL MÜDAHALE SÜRECİ



Her türlü veri güvenliği ihlali vakası raporlandırılır. (Veri sorumluları kişisel veri ihlallerini kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirir. (GDPR Md.33/5) Her ihlal durumu belgelendirilerek veri sorumlusunca kayıtlar muhafaza altına alınır.

6.1 İHLALE İLİŞKİN ÖN DEĞERLENDİRME

ERKUNT TRAKTÖR nezdinde gerçek veya potansiyel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar durumu **Şirket Avukatına (İrtibat Kişisine)** derhal ve gecikmeksizin bildirmekle yükümlüdür. Bu kapsamda ilgili çalışan veya yöneticisi aşağıdaki hususları içerir bir rapor hazırlayarak, veri ihlali İrtibat Kişisine bildirilir. Bu bildirimde;

• Kişisel veri ihlalinin gerçekleşme tarihi ve saati,

• Kişisel veri ihlalinin tespit edildiği tarih ve saat,

• Kişisel veri ihlali olayına ilişkin açıklamalar,

• Eğer biliniyorsa kişisel veri ihlalinden etkilenen kişi ve veri 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 bilgileri yer almalıdır.

Veri Sorumlusu İrtibat Kişisi (Şirket Avukatı), 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, veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

6.2 ÖNLEME VE KURTARMA ÇALIŞMALARININ YÜRÜTÜLMESİ

ERKUNT TRAKTÖR; 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.

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.

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) Çalışanların 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.

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

Veri ihlalinden etkilenecek kişilerin ve veri türlerinin 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.

6.3 RİSKLERİN DEĞERLENDİRİLMESİ

Kişisel veri ihlalleri, ilgili kişiler adına verilerinin Türk Ceza Kanunu kapsamında düzenlenen suçlara alet edilmesi gibi birçok olumsuz etki oluşturabilir. Bu nedenle ihlalin mevcut ve muhtemel sonuçlarının ilgili kişiler üzerinde ne gibi etkiler oluşturabileceğinin dikkatli bir şekilde değerlendirilmesi ve risklerin ortaya koyulması çok önemlidir.

6.4 BİLDİRİM YÜKÜMLÜLÜKLERİ

Veri ihlalinin gerek hukuki yükümlülük kapsamında, gerekse veri ihlaline ilişkin tedbir alınması, ihlalin olası etkilerinin azaltılması gibi amaçlarla Şirket dışında üçüncü kişilere bildirilmesi gerekmektedir.

6.4.1 Kurul'a Bildirim: Veri Sorumlusu İrtibat Kişisi (Şirket Avukatı) öncelikle kişisel veri ihlalinden haberdar olduğu andan itibaren gecikmeksizin ve en geç 72 saat içerisinde Kurul'a bu durumu bildirmekle yükümlüdür. Bu nedenle, Şirket içerisinde tüm çalışanların herhangi bir veri ihlali durumunu vakit kaybetmeksizin Veri Sorumlusu İrtibat Kişisine bildirmesi, Şirketin 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.

6.4.2 İhlalden Etkilenen Kişilere Bildirim : Şirket, kişisel veri ihlalinden etkilendiği tespit edilen kişilere de en kısa sürede bildirim yapmalıdır. Söz konusu bildirimler, yetkilendirilmiş personelin desteğiyle Veri Sorumlusu İrtibat Kişisi tarafından gerçekleştirilir.

İhlal bildirimi aşağıdaki unsurları içermelidir:

- 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,
- 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.

6.4.3 Diğer Bildirimler: Şirketimiz veri ihlalinin niteliği, büyüklüğü, ihlalin suç teşkil edip etmediği gibi hususlar göz önünde bulundurularak üçüncü kişilere de bildirim yapabilecektir. Bu kişiler, diğer veri sorumluları ya da veri işleyenler, tedarikçiler, adli makamlar, noterler, bankalar olabilir.

6.5 İHLAL SONRASI DURUM TESPİTİ

Şirketimiz 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, 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 aşağıdaki unsurları içerir bir değerlendirme ve iyileştirme raporu hazırlanır.

• Somut olay kapsamında yapılan işlemler,

• Veri ihlalinin çıkış noktasının tespit edilip, zaafın giderilmesi adına yapılan faaliyetler ve zaaf noktasında ilave tedbir gerekip gerekmediği,

• Olası kişisel veri ihlallerinin etkilerini azaltmak için hangi adımların atılması gerektiği

• Kişisel veri ihlali nedeniyle herhangi bir plan, Plan ya da raporlamada iyileştirme gerekip gerekmediği

• Kişisel veri ihlalinin tekrarlanmasını önleyebilmek için ek idari ve/veya teknik tedbirlerin alınmasının gerekli olup olmadığı,

• İhlallere maruz kalmayı ve maliyet etkilerini azaltmak için kaynaklara/altyapıya ek yatırım yapılmasının gerekli olup olmadığı,

• İhlalin tekrarlanmasını önleyecek bir personel farkındalık eğitimi gerekliliği,

7. VERİ İHLALİ MÜDAHALE PLANININ VE İLGİLİ MEVZUATIN UYGULANMASI

Planda değişiklik olması durumunda, Planın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

8. VERİ İHLALİ MÜDAHALE PLANI YÜRÜRLÜĞÜ, GÜNCELLENMESİ VE YÜRÜRLÜKTEN KALDIRILMASI

Plan, yayımı tarihinde yürürlüğe girmiş sayılır. Bu Plan yılda bir kez rutin olarak gözden geçirilir ve kayıt altına alınır. Mevzuatta meydana gelen değişiklikler derhal Plana işlenir. Mevzuattaki değişikliklerin uygulanması için, değişikliğin Plana eklenmesi beklenmez, mevzuata uygun hareket tarzı ne ise güncelleme yapılana dek o yol takip edilir.

9. YÜRÜTME

Planın uygulanmasından ve yürütmesinden veri sorumlusu tüm organizasyonu ile birlikte sorumludur.

10. DAĞITIM

İşbu Veri İhlali Müdahale Planı, Şirket internet sitesinde yayınlanarak, üçüncü taraflara ve Şirket çalışanlarına duyurulur.