ARTRON TASARIM ÜRETİM ELEKTRONİK TİCARET A.Ş.

KİŞİSEL VERİ İHLALİ HALİNDE KRİZ YÖNETİMİ PROSEDÜRÜ

1. AMAÇ

6698S. Kişisel Verilerin Korunması Kanunu'nun ("Kanun") "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12. maddesinin 5. 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 havi olup, Kanun uyarınca Veri Sorumlusu konumunda olan **ARTRON TASARIM ÜRETİM ELEKTRONİK TİCARET ANONİM ŞİRKETİ** ("Şirket"), kendi bünyesinde bir Veri İhlali durumu yaşandığında, ihlal durumunun Kişisel Veriler Koruma Kurulu'na ("Kurul")bildirimine dair Şirket içinde izlenmesi gereken prosedürü ve ihlal gerçekleştikten sonra yapılması gereken iş ve işlemleri işbu Kişisel Veri İhlali Halinde Kriz Yönetimi Prosedürü ("Prosedür") ile belirlemeyi amaçlamaktadır.

2. KAPSAM

Şirket bünyesinde bir Veri İhlali veya Potansiyel Veri İhlali yaşanması durumunda uygulanacak iş ve işlemler Prosedür kapsamında açıklanmış olup herhangi bir ihlal halinde bu Prosedür'de açıklanan yönetim süreci uygulama alanı bulur.

3. KISALTMALAR VE TANIMLAR

Bu prosedür özelinde, aşağıdaki ifadeler aşağıda kendilerine verilen anlamlarda kullanılmaktadır:

- Çalışan: Şirket personelini;
- Form: Kişisel Veriler Koruma Kurulu'nun 24.01.2019 tarihli 2019/10 sayılı kararı ile yayınlanan "kişisel veri ihlali bildirim formunu";
- Kanun: 6698 Sayılı Kişisel Verilerin Korunması Kanununu;
- Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi;
- Kurul: Kişisel Verileri Koruma Kurulunu;
- Kurum: Kişisel Veriler Koruma Kurumunu;
- 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;
- Prosedür: Veri İhlali Halinde Kriz Yönetimi Prosedürünü;
- Potansiyel Veri İhlali: Çalışanlar tarafından Şirket bünyesinde potansiyel olarak Veri İhlali riski yaratan durumu;
- Veri İhlali: Şirket'in hakimiyet alanında olan Kişisel Verilerin, Şirket içinden veya dışından "hukuka aykırı olarak işlenmesi", "hukuka aykırı olarak erişilmesi", "hukuka aykırı olarak elde edilmesi" veya "Kişisel Verilerin muhafazasını sağlama, amacıyla

Şirket tarafından alınan ve güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirlerin yetkisiz kişilerce aşılması" durumu;

- Veri İhlali Müdahale Planı: Şirket nezdinde Veri İhlali yaşanması durumunda yürütülecek prosedürü;
- Veri İlgilisi: Kişisel verisi işlenen ve Veri İhlaline uğrayan gerçek kişiyi.
- Veri Sorumlusu: Artron Tasarım Üretim Elektronik Ticaret Anonim Şirketi'ni ifade eder.

4. SORUMLULUK VE GÖREV DAĞILIMLARI

Potansiyel Veri İhlalinin veya Veri İhlalinin değerlendirilmesi, veri ihlalinin olası sonuçlarının değerlendirilmesi, ihlale ilişkin Şirket nezdindeki sorumluluğun kimde olduğuna dair değerlendirmenin yapılması ve Veri İhlali durumunda Şirket nezdinde raporlamayı yapacak Şirket birim ve Çalışanları ile bu kişilerin görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Şirket Nezdinde Veri İhlaline İlişkin Raporlama Yapılması

UNVAN	BİRİM	GÖREV	İHLALE İLİŞKİN RAPORLAMA YAPILACAK BİRİM VE ÇALIŞAN
Yönetici	Kalite ve Konfigürasyon Yönetim Müdürlüğü	Potansiyel Veri İhlalinin değerlendirilmesi, veri ihlalinin olası sonuçlarının değerlendirilmesi, ihlale ilişkin Şirket nezdindeki sorumluluğun kimde olduğuna dair değerlendirmenin yapılması ve Veri İhlali durumunda Kurul ile Veri İlgilisi'ne yapılacak bildirimlerin gerçekleştirilmesi	Kalite ve Konfigürasyon Yönetim Müdürlüğü - Müdür

5. VERİ İHLALİ DURUMUNDA KRİZ YÖNETİMİ

Şirket nezdine bir Veri İhlali veya Potansiyel Veri İhlali yaşanması durumunda, prosedür, Kurul'un 24.01.2019 tarihli 2019/10 sayılı kararına uygun olarak hazırlanmıştır. Herhangi bir ihlal olduğu zaman, Prosedürün "Sorumluluk ve Görev Dağılımları" başlıklı 2. maddesinde açıklanan birim ve Çalışanlar aşağıdaki süreçleri yürüteceklerdir:

- Şirket sorumlu birimine bildirim yapılması;

- Şirket içerisinde araştırma yapılması ve Veri İhlali Müdahale Planı'nın harekete geçirilmesi;
- Veri İhlalinin kaynağının tespiti;
- İhlalin ne zaman gerçekleştiği ve ne zaman tespit edilmesi;
- Etkilenen kişisel veri kategorilerinin ve kişi sayısının tespit edilmesi;
- Veri İhlaline ilişkin mevcut risk ve tehditlerin belirlenmesi;
- Kurul'a ''Kişisel Veri İhlal Bildirim Prosedürü'' çerçevesinde Veri İhlaline ilişkin bildirim yapılması;
- Kurul'a Veri İhlali bildirimi sonrası yedeklenen verilerin faaliyete geçirilmesi.

6. VERİ İHLALİ'NE İLİŞKİN UYGULANMASI GEREKEN PROSEDÜR VE VERİ İHLALİ MÜDAHELE PLANI

Şirketin tüm birimleri ve çalışanları, Şirket bünyesinde bir Veri İhlali veya Potansiyel Veri İhlali olduğunda uygulanacak yöntemler açısından işbu Prosedür ve Şirket'in yetkili birim ve çalışanları tarafından verilecek talimatlara uyacaklardır.

Şirket Sorumlu Birimine Bildirim ve Şirket Nezdinde Araştırma Yapılması

Çalışanlar, Şirket içinde yaşanan Veri İhlali veya Potansiyel Veri İhlali konularında sorumlu birimlere ihlali, derhal açıklamak suretiyle yazılı olarak bilgi verir.

Veri İhlali tespit edildiği anda kim tarafından tespit edildiği önemli olmaksızın Prosedürde açıklanan Veri İhlali Müdahale Planı devreye sokulur. Tablo:1'de yer alan kişiler kendilerine yapılan bildirim akabinde ihlale ilişkin araştırma yapılmasına başlarlar. Yapılacak araştırmada; ''Veri İhlalinin kaynağının tespiti, ihlalin ne zaman gerçekleştiği ve ne zaman tespit edilebildiği, etkilenen kişisel veri kategorilerinin tespit edilmesi, Veri İhlaline ilişkin mevcut risk ve tehditlerin belirlenmesine'' ilişkin aksiyonlar alınır. Olası risk ve tehditler belirlenirken aşağıdaki hususlara dikkat edilmesi gerekmektedir:

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı;
- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği;
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

Bu risklerin tanımlanması ve önceliğinin belirlenmesine ilişkin raporlama yapılır. Söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik Veri İhlali Müdahale Planı'nda açıklanan ve aşağıda yer alan önlemler uygulamaya konulmalıdır:

A. Siber Güvenliğin Sağlanması: Kişisel veri içeren bilgi teknoloji sistemlerine gelen izinsiz erişim tehditlerine karşı ilk savunma hattı olacaktır. Herhangi Potansiyel Veri İhlali veya Veri İhlali yaşanması durumunda;

- Yetkisiz erişim/saldırının şirket içinden mi yoksa şirket dışından mı yapıldığının belirlenmesi sağlanacaktır,
- Şirket sistemlerine yetkisiz erişim/saldırının halen devam edip etmediğinin belirlenmesine çalışılacaktır,
- İhlalin sebebi araştırılacaktır,
- İhlalin yaşandığı dijital ortamda, ağda yer alan dosyaların Şirket virüs programları vb. programlar vasıtasıyla taranması sağlanacaktır,
- İhlalin Şirket nezdinde yaratabileceği iş sürecine ilişkin potansiyel sorunların belirlenmesine ilişkin çalışma yapılacaktır.
- Yama yönetimi ve yazılım güncellemeleri gerçekleştirilip yazılım ve donanımların düzgün bir şekilde çalışması sağlanacaktır,
- Güvenlik duvarı yapılandırması gözden geçirilecektir,
- İhlal ile alakalı olduğu düşünülen kısımlara ilişkin şifreler ile erişim yetki ve kontrol matrisinde gerekli değişiklikler yapılacak ve gerekirse erişim yetkileri sınırlandırılacaktır.
- İhlale konu olan veya suça konu veya aracı olduğu düşünülen cihazlar muhafaza edilir ve acil müdahale gerektirmeyen durumlarda üzerinde gerekli hukuki tespitler yapılıncaya kadar kullanılmamalıdır.

B. Fiziksel Veri Güvenliğinin Sağlanması: Şirket nezdinde yaşanan Veri İhlali veya Potansiyel Veri İhlali'nin fiziksel ortamlarda meydana gelmesi halinde;

- Kişisel veri barındıran dokümanların, harddisk, Usb gibi depolama cihazlarının, diğer elektronik cihazların Şirket içinde herkese açık alanda bulunduğunun anlaşılması veya çalınması halinde sorumlu birim tarafından bu evraklar sahibi/ilgilisi tespit edilene kadar sorumlu birim nezdinde üzerindeki bilgiler okunamayacak şekilde zarf veya kutu gibi kapalı bir ortamda muhafaza edilir. Muhafaza altına alınan eşyanın doküman olması durumunda bu dokümanın sahibi/ilgilisi tespit edilemediği taktirde 1 ay sonra doküman imha edilir.
- Şirket içinde kapalı olarak tutulması gereken dolap, kutu vb. gibi ortamların herkese açık şekilde bulunduğunun anlaşılması halinde bu dolap ya da kutuların sahibi/ilgilisi tespit edilene kadar sorumlu birim tarafından güvenliği temin edilir.
- Şirket içinde kişisel veri barındıran herhangi bir ortamda veya bu ortamların yakınında yangın vb. gibi kişisel veri barındıran doküman yahut cihazların yok olmasına, zarar görmesine sebep olabilecek herhangi bir durum görülmesi halinde ivedilikle Şirket'in ilgili diğer birimlerine haber verilir.
- İhlalin yaşandığı ortama ilişkin varsa kamera kayıtları incelenir, konu hakkında bilgi ve görgüsü olabilecek Şirket'in diğer çalışanları ile görüşülür. Gerekli görülmesi halinde konuya ilişkin bilgi ve gerekli dokümanlar avukatlar gibi Şirket danışmanlarıyla paylaşılır, hukuki aksiyon alınır.

Veri İhlaline İlişkin Unsurların Kayıt Altına Alınması

Yaşanan Veri İhlaline ilişkin ihlal kaynağının tespiti, ihlalin ne zaman gerçekleştiği ve ne zaman tespit edildiği, etkilenen kişisel veri kategorilerinin tespiti kayıt altına alacak ve Kurul'un incelemesine hazır halde bulunduracaklardır.

Kurula Veri İhlali Bildirimi Yapılması

Şirket bünyesinde bir Veri İhlali yaşanması durumunda Kanun uyarınca Kurul'a 72 saat içerisinde bildirim yapılması sağlanmalıdır.

Yedeklenen Kişisel Verilerin Faaliyeti Geçirilmesi

Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir.

7. PROSEDÜR'ÜN YAYINLANMASI VE SAKLANMASI

Prosedür, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, **www.artron.com.tr** adresli web sayfasında kamuya açıklanır. Basılı kağıt nüshası da Şirketin Kalite ve Konfigürasyon Yönetim Müdürlüğü'nde muhafaza edilen ilgili dosyasında saklanır.

8. PROSEDÜR'ÜN GÜNCELLENME PERİYODU

Prosedür, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir. İstenildiği zaman Prosedür'ün en güncel haline **www.artron.com.tr** adresli web sayfasından ulaşılabilir.

9. PROSEDÜRÜN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Prosedür, Şirketin web sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

Yürürlükten kaldırılmasına karar verilmesi halinde, Prosedür'ün ıslak imzalı eski nüshaları Şirket Yönetim Kurulu Kararı ile Şirketin Kalite ve Konfigürasyon Yönetim Müdürlüğü tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Şirketin Kalite ve Konfigürasyon Yönetim Müdürlüğü tarafından saklanır.