VERİ İHLALİ MÜDAHALE PLANI

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." hükmünü amirdir.

İşbu "Kişisel Veri İhlali Müdahale Planı" **(Plan**), 24.01.2019 Tarih ve 2019/10 Sayılı Kişisel Verileri Koruma Kurulu kararı (Karar) uyarınca Vargonen Teknoloji ve Bilişim Sanayi Ticaret A.Ş.("**Şirket**") tarafından hazırlanmıştır.

2. KAPSAM

Kişisel veri ihlali; iletilen, saklanan veya sair şekilde 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 dokümanların 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 Şirketin sahip olduğu ya da Şirketimizce yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Plan uygulanır.

3. TANIM VE KISALTMALAR

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

İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Müşteriler, ziyaretçiler, çalışanlar ve çalışan adayları.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örn: ad-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 işlem.
VERİ İŞLEYEN:	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişidir.
VERİ SORUMLUSU:	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder.
KVK KANUNU:	7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
KVK KURUMU:	Kişisel Verileri Koruma Kurumu.
KVK KURULU:	Kişisel Verileri Koruma Kurulu.

4. 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;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin

etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

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.

Buna göre, İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, Şirket söz konusu veri ihlalini, en kısa sürede (en geç 72 saat) Kurul'a ve söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip makul olan en kısa süre içerisinde ilgili kişiye bildirmelidir.

İlgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa Şirketin kendi internet sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmalıdır.

Veri sorumlusu tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak;

- İhlalinin 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 web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları unsurlarına yer verilmesi gerekir.

Kurula yapılacak bildirimde yine Kurul'un belirlediği ve web sitesinde yayınladığı KVK Kurulu Veri İhlal Bildirim Formu doldurularak Kurula iletilir. Şirket tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanması gerekmektedir.

Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak sağlanmalıdır.

Şirket tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulması sağlanmalıdır.

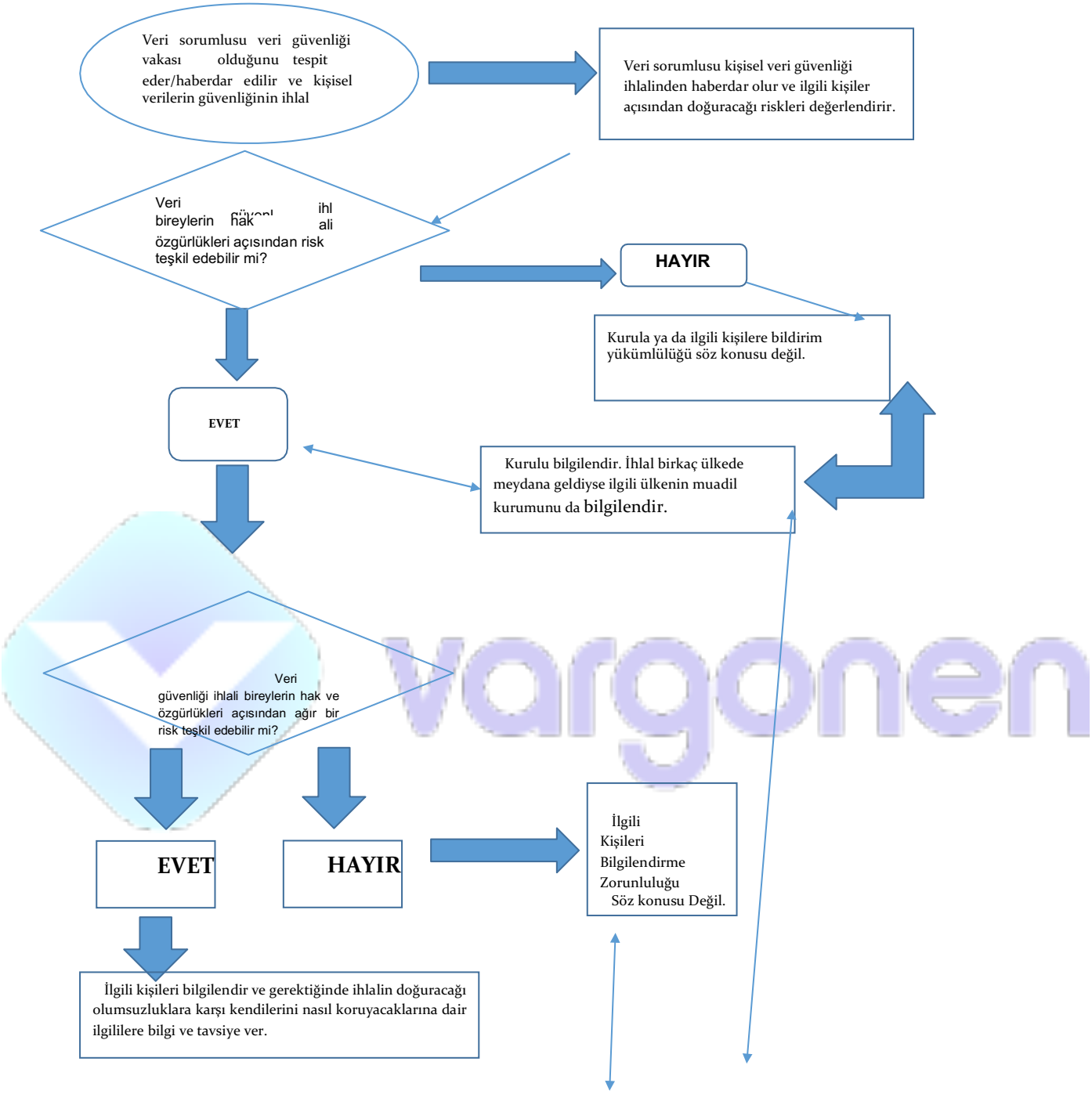
Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyen bu konuda herhangi bir gecikmeye yer vermeksizin Şirket'e bildirimde bulunmalıdır.

Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmalıdır.

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 plan gözden geçirilmelidir.

5. İHLAL MÜDAHALE SÜRECİ

İhlal Bildirim Mükellefiyetine İlişkin Akış Şeması



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.

Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin işbu Planın 1. bölümünde belirtilen Karar uyarınca, Şirket'in kişisel veri ihlalini öğrendiği tarihten itibaren **gecikmeksizin ve en geç 72 saat içinde ihlali** Kurul'a bildirmesi ve veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de **makul olan en kısa süre içerisinde** ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa Şirket'in kendi internet sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması gerekmektedir.

Söz konusu yükümlülüklerin yerine getirilebilmesi için, bir veri ihlali durumunda öncelikle Şirket içerisinde belirli adımlar takip edilecektir:

- İhlale ilişkin ön değerlendirme,
- Önleme ve kurtarma çalışmalarının yürütülmesi,
- Risklerin değerlendirilmesi,
- Bildirim,
- İyileştirme Çalışmaları.

6. İHLALE İLİŞKİN ÖN DEĞERLENDİRME

Merkezimiz nezdinde gerçek veya potansiyel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar Veri Sorumlusu İrtibat Kişisine derhal ve gecikmeksizin durumu bildirmekle yükümlüdür. Bu kapsamda ilgili çalışan veya yöneticisi aşağıdaki hususları içerir bir rapor hazırlayarak, veri ihlalini Veri Sorumlusu ve İrtibat Kişisine bildirir. 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, 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.

7. ÖNLEME VE KURTARMA ÇALIŞMALARI

Veri ihlalinin merkez ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için önleme ve kurtarma çalışmaları veri sorumlusu gözetiminde yürütülür. Bu kapsamda öncelikle veri ihlalinden haberdar edilmesi gereken birimler tespit edilir ve bu kişilere ihlalin kontrol edilebilmesi, mümkünse engellenebilmesi ve zararların azaltılabilmesi için atılması gereken adımlara ilişkin rehberlik edilir.

Akabinde 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.

8. RİSK DEĞERLENDİRMESİ

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.

Veri sorumlusu tarafından riskler değerlendirilirken, ihlalden etkilenen kişisel verilerin niteliği, hassasiyeti ve miktarı ile etkilenen bireylerin sayısı ve kişi gruplarının kimler olduğu, veri ihlalinin Şirket'in faaliyetleri ile itibarına olan etkisi, veri ihlalinin etkisinin azaltılmasında alınan önlemler ve ihlalin olası sonuçları ayrı ayrı ele alınmalıdır. Bunların sonucuna göre veri ihlalleri aşağıdaki şekilde sınıflandırılabilir.

- **1. Kademede İhlal:** İhlalin yarattığı etkiler, ilgili kişiler üzerinde kişisel verilerinin hukuka aykırı olarak elde edilmesi dışında somut bir zarara neden olmamaktadır.
- **2. Kademede İhlal:** İhlal ilgili kişiler üzerinde olumsuz etkilere neden olabilecek niteliktedir. Ancak ihlalden etkilenen veri sayısı, çeşidi ve boyutu düşünüldüğünde bu etki büyük değildir.
- **3. Kademede İhlal:** İhlal boyutu, niteliği, etkili olduğu kişisel verilerin türü, sayısı gibi etmenler değerlendirildiğinde ihlalden etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere ve somut zararlara neden olabilecek seviyededir.

* Kişisel Verileri Koruma Kurumu'na göre: "Gerçekleşen veri ihlalinin düzeyinin belirlenmesinde ilgili kişiler üzerinde ne kadar bir potansiyel etkiye neden olduğunun değerlendirilmesi gerekmektedir. Söz konusu potansiyel etkinin değerlendirilmesinde ise ihlalin niteliği, ihlalin nedeni, ihlale maruz kalan verinin türü, ihlalin etkisinin azaltılmasında alınan önlemler ile ihlalden etkilenen ilgili kişi kategorileri göz önünde bulundurulmalıdır."

2. ve 3. kademedeki ihlallere ilişkin veri sorumlusu üst yönetimine bilgi verilir. İhlalin 3. kademede olduğunun değerlendirildiği durumlarda bu bildirim hiç gecikmeksizin yapılır.

* Kişilerin sadece ad soyad bilgilerinin yer aldığı bir katılım listesinin yetkisiz kişiler tarafından görülmesi durumunda **1. kademede ihlal olduğu** değerlendirilebilir.

İhlalin ilgili kişiler üzerinde olumsuz etkileri bulunması ancak etkisinin büyük olmaması **2. kademede ihlal** kabul edilebilir. Örneğin ilgili kişilerin önemli olarak değerlendirilebilecek verilerinin ihlale maruz kaldığı bir olayda veri sorumlusunun ihlal akabinde aldığı güvenlik tedbirleri ile ihlalin etkilerinin önemli ölçüde azaltmış olması bu kademeye örnek verilebilir.

Özellikle ihlalden etkilenen kişilerin ve/veya kayıtların sayısal olarak çok olması, ihlale konu verilerin içerisinde özel nitelikli veriler olması ya da kredi kartı bilgileri gibi kişilerin önemli bilgilerinin yer alması durumunda ihlalin yüksek düzeyde risk taşıdığı ve **3. kademede ihlal** olduğu değerlendirilebilir.

Ancak Kurum'un risk değerlendirmesi konusu hakkındaki açıklamaları ve kararları takip edilmelidir.

9. BİLDİRİM

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

KURUL'A BİLDİRİM

Veri Sorumlusu İrtibat Kişisi, 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.

İHLALDEN ETKİLENEN KİŞİLERE BİLDİRİM

Şirket, kişisel veri ihlalinden etkilen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa uygun yöntemlerle (örneğin internet sitesi üzerinden duruma ilişkin bir duyuru yayınlanması) bildirim yapmalıdır. Söz konusu bildirimler, yetkilendirilmiş personelin desteğiyle Veri Sorumlusu İrtibat Kişisi tarafından gerçekleştirilir.

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı uyarınca Şirket tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak aşağıdaki unsurları içermesi gerekir:

- 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.

10. İHLAL SONRASI DURUM TESPİTİ

Merkez 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,

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

Plan, Şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

Yürürlükten kaldırılmasına karar verilmesi halinde, Planın ıslak imzalı eski nüshaları Kurul Kararı ile Veri sorumlusu tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Veri sorumlusu tarafından saklanır.

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.

Tarih:

Versiyon:


vargonen