1. GİRİŞ

1.1. AMAÇ

İşbu Kişisel Veri İhlali Müdahale Planı ***("Plan"),*** Kişisel Verileri Koruma Kurulu'nun ***("Kurul")*** 24.01.2019 tarih ve 2019/10 sayılı kararı doğrultusunda; **ULUSOY RAYLI SİSTEMLER ANONİM ŞİRKETİ** ("***Şirket***") olarak tarafımızca işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde Şirket bünyesinde yapılması gerekli iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

1.2. KAPSAM

Şirket bünyesinde ortaya çıkabilecek her tür kişisel veri ihlali, işbu Plan kapsamındadır.

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 (siber saldırı vb.) 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 örnek olarak yer verilen durumlar ve sair şekillerde ortaya çıkabilecek kişisel veri ihlallerinde işbu Plan'da belirtilen şekilde aksiyon alınması gereklidir.

2. İHLAL MÜDAHALE SÜRECİ

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 ve kişisel veri ihlalinin etkilerinin en aza indirgenmesi amacıyla, olası bir veri ihlali durumunda aşağıda yer verilen sürecin takip edilmesi gerekmektedir:

2.1. İhlalin İlk Tespiti ile İrtibat Kişisinin Bilgilendirilmesi

Kişisel verilerin korunmasına dair aldığı eğitimler doğrultusunda Şirket bünyesinde gerçek veya potansiyel bir kişisel veri ihlali tespit eden çalışan, söz konusu ihlali aynı iş günü içinde bağlı olduğu birim sorumlusuna ve İrtibat Kişisine bildirmekle yükümlüdür. İhlalin İrtibat Kişisine bildirilmesi üzerine, veri ihlali tespit eden çalışan ve birim sorumlusu, İrtibat Kişisine sunulmak üzere bir Kişisel Veri İhlali Tespit Raporu hazırlar. Anılan raporda asgari olarak;

- Kişisel veri ihlalinin gerçekleşme tarihi ve saati,
- Kişisel veri ihlalinin tespit edildiği tarih ve saat,
- Somut kişisel veri ihlaline ilişkin açıklamalar,

- Eğer biliniyorsa kişisel veri ihlalinden etkilenen kişi ve veri sayısı,
- Kişisel veri ihlalinin tespit edildiği tarihte varsa atılan adımlara ve alınan önlemlere ilişkin açıklamalar,
- Raporu hazırlayan çalışanların adı, soyadı ve rapor tarihi

hususlarına yer verilir.

Bu kapsamda hazırlanan Kişisel Veri İhlali Tespit Raporu gecikmeksizin ve en geç ihlalin tespit edildiği andan itibaren 24 saat içinde İrtibat Kişisine sunulur.

2.2. İhlale İlişkin Ön Değerlendirme ve Toplantıya Çağrı

Kişisel veri ihlali tespit eden veya Kişisel Veri İhlali Tespit Raporunu teslim alan 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 ve oluşabilecek etkilerini de göz önünde bulundurarak, İnsan Kaynakları Birimi ile birlikte veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

İrtibat Kişisi tarafından eş zamanlı olarak, İnsan Kaynakları Birimi ve ihlalin gerçekleştiği birim sorumlusu veri ihlaline ilişkin gerçekleştirilecek toplantıya çağrılır. Gerekli görülmesi halinde Bilgi İşlem Sorumlusu ve Hukuk Danışmanı da toplantıya katılır. Aşağıda yer verilen tüm süreçler, toplantıya katılım gerçekleştiren çalışanlar tarafından birlikte yürütülür.

2.3. Önleme ve Kurtarma Çalışmalarının Yürütülmesi

Veri ihlalinin Şirket ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için önleme ve kurtarma çalışmaları İrtibat Kişisinin 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.

Eş zamanlı olarak, veri ihlalinden etkilenebilecek kişilerin ve veri türlerinin neler olduğu tespit edilmeye çalışılır, veri ihlalinden etkilenebilecek kişilerin iletişim bilgileri belirlenir, veri ihlali nedeniyle haberdar edilmesi gereken başka kurum ya da kuruluşlar olup olmadığı değerlendirilir.

2.4. Risklerin Değerlendirilmesi

İrtibat Kişisi ve İnsan Kaynakları Birimi tarafından kişisel veri ihlalinin mevcut ve muhtemel sonuçları ve ilgili kişiler üzerinde oluşturabileceği etkilere ilişkin olarak risk değerlendirmesi yapılır. Risklerin değerlendirilmesinde, ihlalden etkilenen kişisel verilerin niteliği, hassasiyeti ve miktarı ile etkilenen bireylerin sayısı ve kişi gruplarının kimler olduğu, veri ihlalinin Şirket faaliyetleri ile itibarına olan etkisi, veri ihlalinin etkisinin azaltılmasında alınan önlemler ve ihlalin olası sonuçları dikkate alınır. Bu doğrultuda yapılan değerlendirme neticesinde, kişisel veri ihlalinin kaçıncı kademe ihlal niteliği taşıdığı belirlenir;

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.

2. ve 3. kademedeki ihlallere ilişkin olarak İrtibat Kişisi tarafından gecikmeksizin Şirket üst yönetimine bilgi verilir.

2.5. Bildirim

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

2.5.1. Kurul'a Bildirim

Kişisel veri ihlali, Şirket'in bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içerisinde Kurul'a bildirilir. Anılan bildirim İrtibat Kişisi tarafından gerçekleştirilir.

Kurul'a yapılacak bildirimde Kişisel Verileri Koruma Kurumu'nun ***("Kurum")*** internet sitesinde yayımlanmış olan Kişisel Veri İhlali Başvuru Formu kullanılır. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak da sağlanabilir.

Haklı bir gerekçe ile 72 saat içerisinde Kurul'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenleri de Kurul'a açıklanır.

2.5.2. İhlalden Etkilenen Kişilere Bildirim

Şirket, kişisel veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa internet sitesi üzerinden duyuru yayımlanması gibi uygun yöntemlerle bildirim yapar. Söz konusu bildirimler, İrtibat Kişisi tarafından gerçekleştirilir.

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin Kurul'un 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;

- 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

unsurlarını içermesi gerekmektedir.

2.5.3. Diğer Bildirimler

Yukarıda yer verilen bildirimlerin yanı sıra, veri ihlalinin niteliği, büyüklüğü, ihlalin suç teşkil edip etmediği gibi hususlar göz önünde bulundurularak Şirket tarafından diğer veri sorumluları ya da veri işleyenler, tedarikçiler, müşteriler, adli makamlar, noterler, bankalar vb. gibi üçüncü kişilere de bildirim

yapılması gerekebilir. İrtibat Kişisi ve İnsan Kaynakları Birimi, böyle bir gereklilik olup olmadığını ayrıca değerlendirir ve gerekli ise bildirimleri yapar.

2.6. İhlal Sonrası Durum Tespiti

Şirket tarafından kişisel veri ihlallerine ilişkin tüm bilgiler, etkiler ve alınan önlemler kayıt altına alınır ve Kurul'un incelemesine hazır halde bulundurulur. İrtibat Kişisi ve İnsan Kaynakları Birimi, 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 İnsan Kaynakları Birimi desteği ile İrtibat Kişisi, aşağıdaki unsurları içerir bir değerlendirme ve iyileştirme raporu hazırlar:

- Somut olay kapsamında yapılan işlemler,
- Veri ihlalinin çıkış noktası, 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 prosedür, politika, 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 bulunup bulunmadığı.

3. KİŞİSEL VERİ İHLALİ KONTROL LİSTESİ

Kişisel veri ihlaline ilişkin olarak yürütülen süreçlerde gerçekleştirilmesi gerekli iş ve işlemlerin takibi adına, işbu Plan ekinde yer alan Kişisel Veri İhlali Kontrol Listesinden yararlanılır.

4. UYGULAMA

İşbu Plan'ın uygulanması ve yürütülmesinden İrtibat Kişisi ve İnsan Kaynakları Birimi sorumludur.

Veri ihlaline ilişkin Şirket bünyesinde yürütülen süreçlerde tüm çalışanlar İrtibat Kişisine ve İnsan Kaynakları Birimi gerekli tüm yardım ve desteği sağlamakla yükümlüdür.

5. PLANIN SAKLANMASI

İşbu Plan, ıslak imzalı (basılı kağıt) ve internet sitesinde olmak üzere iki farklı ortamda yayımlanır. Basılı kağıt nüsha İnsan Kaynakları Birimi tarafından saklanır.

6. PLANIN YÜRÜRLÜĞÜ VE GÜNCELLEME PERİYODU

İşbu Plan, .../.../... tarihi itibariyle yürürlüğe girmiştir.

İşbu Plan, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

No	Versiyon	Tarih	Hazırlayan	Değişiklik
1	1.0	.....	İrtibat Kişisi	.....

EK: KİŞİSEL VERİ İHLALİ KONTROL LİSTESİ

NO	KONTROL LİSTESİ	Tamamlandığında işaretleyiniz
1	Kişisel verilere ilişkin herhangi bir ihlal yaşandı mı veya ihlal yaşandığından şüpheleniliyor mu?	
2	İhlal halen devam etmekte mi?	
3	İhlalin nasıl tespit edildiği kayıt altına alındı mı?	
4	İhlali tespit eden kişi veya sistem kayıt altına alındı mı?	
5	İhlale ait ilk tespitin tarih ve saati kayıt altına alındı mı?	
6	İhlal hakkında temel bilgiler kayıt altına alındı mı?	
7	İhlalle ilgili aksiyonları alacak kişiler bilgilendirildi mi?	
8	Kişisel veri ihlaline ilişkin toplantı yapıldı mı?	
9	İhlal tespit eden ve ihlalden etkilenen çalışanlarla mülakatlar yapılıp onlardan ihlalle ilgili mümkün olduğunca detaylı bilgi alındı mı?	
11	İhlale dahil olan kişilerin veya sistemlerin konumu kayıt altına alındı mı?	
12	Hangi kişilerin, kişisel verilerin ve sistemlerin etkilendiği kayıt altına alındı mı?	
14	Etkilenen sistemler kurum ağından izole edildi mi?	
15	Hedef olan sistemlerin; adı, iletişim sistemi, IP adresi, ağ üzerindeki konumu, fiziksel konumu ve kullanım amacı kayıt altına alındı mı?	
16	Halen tehlike altında olan sistemler veya veriler var ise bunlar kayıt altına alındı mı?	
19	İhlalin nedenlerinin ve kaynaklarının soruşturulması sırasında Bilgi İşlem incelemesi yapıldı mı? Bilgi işlem notları:	
20	Elde edilen verilerin sadece erişim yetkisi olan kişilerin ulaşabildiği, giriş-çıkışları kontrol altında olan bir alanda tutulması sağlandı mı?	
21	İhlalin Şirkette yol açtığı genel ve finansal etkiler tespit edildi mi?	
22	İhlalden kişisel veriler etkilendiyse, etkilenen veriler ve verileri etkilenen kişiler tespit edildi mi?	
23	İhlalin tekrarlanmaması için alınacak önlemler belirlendi mi?	
24	Etkilenen sistemler ihlal öncesindeki sağlıklı yapıya döndürüldü mü?	

25	Veri ihlalinin engellenmesi adına Şirket politikaları/prosedürlerinde güncelleme yapılması gerekliliği bulunmakta mı? Cevap “evet” ise yapılması gerekli güncellemelere ilişkin notlar:	
26	Veri ihlalinin engellenmesi adına Şirket sistemlerinde iyileştirme yapılması gerekliliği bulunmakta mı (sistem, yazılım, anti-virüs yazılımı güncellemeleri, şifrelere ilişkin iyileştirmeler vb. gibi)? Cevap “evet” ise yapılması gerekli iyileştirmelere ilişkin notlar:	
27	Veri ihlalinin engellenmesi adına, kişisel veri işlenen sistemlerin korunması için fazladan tedbir alınması gerekmekte mi? Cevap “evet” ise alınması gerekli ek tedbirler:	
28	İhlal nedeniyle kişisel veriler kanuni olmayan yollarla başkaları tarafından elde edildi mi? Cevap “evet” ise;	
28.1	Durumun Şirket tarafından öğrenildiği tarihten itibaren en geç 72 saat içinde Kurul’a bildirim yapıldı mı?	
28.2	Veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere makul olan en kısa süre içerisinde bildirim yapıldı mı?	
29	Veri ihlaline ilişkin üçüncü kişilere bildirim yapılması gerekmekte mi? Cevap “evet” ise gerekli bildirimler yapıldı mı?	