SERTRANS ULUSLARARASI NAKLİYAT VE TİCARET A.Ş.
KİŞİSEL VERİ İHLALİ MÜDAHALE PROSEDÜRÜ

1. Prosedürün Amacı

6698 sayılı Kişisel Verilerin Korunması Kanunu*'nun ("**Kanun**") 12. maddesinin 5. fıkrasına göre veri sorumlusu olan **Sertrans Uluslararası Nakliyat ve Ticaret Anonim Şirketi ("Şirket")** işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi, başka bir ifadeyle "Kişisel Veri İhlali" gerçekleşmesi halinde, bu durumu en kısa sürede ilgilisine ve "Kişisel Verileri Koruma Kurulu"na ("Kurul") bildirmekle yükümlüdür.

İşbu **"Kişisel Veri İhlali Müdahale Prosedürü"** ("**Prosedür**"), kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde diğer bir deyişle, kişisel veri ihlali gerçekleşmesi durumunda nasıl müdahale edileceği ve atılacak adımların neler olduğu konusunda izlenecek prosedürü belirlemek amacıyla hazırlanmıştır.

2. Tanımlar

Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel Verilerin İşlenmesi	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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
KVKK/Kanun	7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
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	Kişisel Veri İhlali Müdahale Prosedürü
Şirket	Sertrans Uluslararası Nakliyat ve Ticaret Anonim Şirketi
KVK Üst Kurulu/Birimi	Şirket nezdinde kurulmuş olan ve işbu Prosedür'ün yürütülmesinden ve takibinden sorumlu olan Kurul/Birim
KVK Komitesi/Birimi	Şirket nezdinde oluşturulan Kişisel Verileri Koruma Komitesi/Birimi
Veri İşleyen	Veri sorumlusunun vermiş olduğu yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi.
Veri Sahibi/İlgili Kişi/İlgili Kişiler	Kişisel verisi işlenen gerçek kişi/kişiler

Veri Sorumlusu	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, (İşbu Prosedür içerisinde İşbu Prosedür kapsamında **Sertrans Uluslararası Nakliyat ve Ticaret Anonim Şirketi** olarak ifade edilecektir.)
Çalışan	Sertrans Uluslararası Nakliyat ve Ticaret Anonim Şirketi personeli
Kişisel Veri İhlali Müdahale Ekibi	Kişisel Verileri Koruma Komitesi, Üst Kurul Üyeleri ve İhlalin Meydana Geldiği Departmanın Yöneticisinden oluşan Ekip
Karar	Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun 24.01.2019 Tarih ve 2019/10 Sayılı Kararı

3. Prosedürün Uygulanmasında Sorumluluk

İşbu Prosedür'ün uygulanmasından 21/02/2020 tarihli 2020/ 01__ tarihli Yönetim kararıyla belirlenen "Kişisel Verileri Koruma Komitesi Üst Kurul Üyeleri" sorumludur. Prosedür'e aykırı hareket eden çalışanlar Sertrans Uluslararası Nakliyat ve Ticaret Anonim Şirketi Disiplin Yönetmeliği" hükümlerine tabi olacaktır.

4. Kişisel Veri İhlali Tanımı

Kişisel veri ihlali, Kanun'un 12. maddesinin 5. fıkrasında yer alan haliyle *"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi"* anlamına gelmektedir. Kişisel verilerin kanuna aykırı bir şekilde elde edilmesi, hukuka aykırı bir şekilde kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin sehven veya kasten yetkisiz kişilere açıklanması, kişisel verilerin hukuka aykırı bir şekilde silinmesi, değiştirilmesi veya bütünlüğünün bozulması gibi durumlarda ortaya çıkmaktadır.

Aşağıda yer alan durumlar genel olarak kişisel veri ihlali olarak değerlendirilir;

- Kişisel veri içeren fiziki dokümanların veya elektronik cihazların çalınması veya kaybolması,
- Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi,
- Gizli bilgilerin hukuka aykırı şekilde ifşası,
- Kişisel veri ve/veya gizli bilgi içeren e-postaların sehven veya kasten şirket dışında ilgisiz kişilere iletilmesi, gönderimi,
- IT ekipmanlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin siber saldırı) gerçekleşmesi suretiyle kişisel verilere hukuka aykırı erişim sağlanması.

Yukarıda belirtilen durumlar sınırlı sayıda olmayıp benzer durumlarda da işbu Prosedür'de belirtilen şekilde hareket edilmelidir.

5. Kişisel Veri İhlali Müdahale Ekibi

Kişisel veri ihlali durumunda oluşan veya oluşabilecek duruma müdahale etmek ve Kanun kapsamında öngörülen yükümlülükleri yerine getirmek için aşağıda sıralanan katılımcıların dahil edileceği bir **"Kişisel Veri İhlali Müdahale Ekibi" ("Ekip")** oluşturulur:

- Kişisel Veri Komitesi Üst Kurul Üyeleri
- İhlalin Meydana Geldiği Departmanın Yöneticisi

6. Kişisel Veri İhlali Müdahale Süreci

"Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun 24.01.2019 Tarih ve 2019/10 Sayılı Kararı" ("Karar") uyarınca, veri sorumlusu olan Şirket'in kişisel veri ihlalini öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurul'a bildirmesi ve veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde 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 aşağıda belirlenen adımlar takip edilecektir;

- Gerçekleşen veri ihlaline ilişkin ön değerlendirme,
- Engelleme ve kurtarma çalışmalarının yürütülmesi,
- Risklerin değerlendirilmesi,
- Bildirim,
- Değerlendirme ve İyileştirme.

6.1. İhlale İlişkin Ön Değerlendirme

Şirket nezdinde gerçek veya potansiyel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar Kişisel Verileri Koruma Komitesi Üst Kurul Üyeleri'ne derhal ve gecikmeksizin durumu bildirmekle yükümlüdür. Bu kapsamda ilgili çalışan aşağıdaki hususları içerir bir rapor hazırlayarak, veri ihlalini Kişisel Verileri Koruma Komitesi Üst Kurulu'na bildirir.

- Kişisel veri ihlalinin gerçekleşme tarihi ve saati,
- Kişisel veri ihlalinin tespiti tarihi ve saati,
- Kişisel veri ihlali olayına ilişkin açıklamalar,
- Kişisel veri ihlalinden etkilenen kişisel veri kategorileri ve kişi grupları,
- Kişisel veri ihlalinin kaynağı[1],
- Eğer biliniyorsa kişisel veri ihlalinden etkilenen kişi ve kayıt 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.

Kişisel Verileri Koruma Komitesi Üst Kurulu, kendisine iletilen 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, Ekip ile birlikte veri ihlalinin araştırılması için kapsamlı bir araştırma ve soruşturma başlatır.

6.2. Engelleme ve Kurtarma Çalışmalarının Yürütülmesi

Veri ihlalinin Şirket ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için engelleme ve kurtarma çalışmaları Ekip'in gözetiminde yürütülür. Bu kapsamda öncelikle veri ihlalinden haberdar edilmesi gereken departmanlar 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 kayıtların 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.

---

[1] Kişisel veri ihlalinin kaynağı, kişisel verilerin yanlış alıcılara gönderilmesi, belge/cihaz hırsızlığı veya kaybolması, verilerin güvensiz ortamlarda depolanması, zararlı yazılımlar, sosyal mühendislik, sabotaj, kaza/ihmal gibi durumlar olabilir.

6.3. Risklerin Değerlendirilmesi

Ekip tarafından riskler değerlendirilirken, ihlalden etkilenen kişisel verilerin niteliği, hassasiyeti ve hacmi 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 ihlali "düşük düzeyde, orta düzeyde veya yüksek düzeyde risk"[2] olarak nitelendirilir:

- **Düşük düzeyde risk:** İhlal ilgili kişiler üzerinde olumsuz herhangi bir etkiye neden olmamakta ya da bu etki ihmal edilebilir düzeyde kalmaktadır./İhlal neticesinde, herhangi bir etkinlik kaybı söz konusu değil ya da çok düşük bir etkinlik kaybı var ve şirket tarafından tüm kullanıcılara tüm önemli hizmetler sunulabilmektedir./İhlal neticesinde, herhangi bir etkinlik kaybı söz konusu değil ya da çok düşük bir etkinlik kaybı var ve şirket tarafından tüm kullanıcılara bilgi sistemleri aracılığıyla verilen hizmetler sunulabilmektedir.
- **Orta düzeyde risk:** İhlal ilgili kişiler üzerinde olumsuz etkilere neden olabilir fakat bu etki büyük değildir./İhlal neticesinde, şirket tarafından bazı kullanıcılara önemli bir hizmet sunma yetisi kaybedilmiştir./İhlal neticesinde, şirket tarafından bazı kullanıcılara bilgi sistemleri aracılığıyla verilen hizmetleri sunma yetisi kaybedilmiştir.
- **Yüksek düzeyde risk:** İhlal etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere neden olmaktadır/ İhlal neticesinde, şirket tarafından tüm kullanıcılara her türlü önemli hizmeti sunma yetisi kaybedilmiştir./İhlal neticesinde, şirket tarafından tüm kullanıcılara bilgi sistemleri aracılığıyla verilen hizmetleri sunma yetisi kaybedilmiştir.

Orta ve özellikle yüksek düzeyde risk olarak tanımlanan veri ihlallerine ilişkin Yönetim'e Üst Kurul tarafından bilgi verilir.

6.4. 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.

6.4.1. Kurul'a Bildirim

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 Kişisi'ne bildirmesi, Şirket'in 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.

---

[2] Kişilerin sadece ad soyadı, telefon bilgilerinin yer aldığı bir katılım listesinin ihlale konu olması durumunda düşük düzeyde risk taşıdığı değerlendirilebilir.
İhlalin ilgili kişiler üzerinde olumsuz etkileri bulunması ancak etkisinin büyük olmaması orta düzeyde risk kabul edilebilir. Her ne kadar kişilerin önemli bilgileri ihlale konu olsa da, veri sorumlusunun ihlal akabinde aldığını güvenlik tedbirleri ile ihlalin etkilerinin önemli ölçüde azaltmış olması bu risk türüne 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 değerlendirilebilir.
Ancak Kurum'un risk değerlendirmesi konusu hakkındaki açıklamaları ve kararları takip edilmelidir.

6.4.2. İhlalden Etkilenen Kişilere Bildirim

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, Üst Kurul Üyelerinin desteğiyle gerçekleştirilir.

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, "Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarih ve 2019/271 sayılı Kararı" uyarınca, Şirket tarafından ilgili kişiye yapılacak olan ihlal bildirimi açık ve sade bir dille yapılır ve asgari olarak aşağıdaki unsurları içerir;

- 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 internet sayfasının tam adresi, çağrı merkezi vb. iletişim yolları unsurlarına yer verilmesi.

6.4.3. Diğer Bildirimler

Şirket'in hukuken yapması zorunlu olan bildirimlerin yanı sıra, veri ihlalinin niteliği, büyüklüğü, ihlalin suç teşkil edip etmediği gibi hususlar göz önünde bulundurularak üçüncü kişilere de bildirim yapılması gerekebilir. Bu kişiler, diğer veri sorumluları ya da veri işleyenler, dış danışmanlar, adli makamlar, bankalar olabilir. Ekip, böyle bir gereklilik olup olmadığını ayrıca değerlendirir ve gerekli ise bildirimleri yapar.

6.5. Değerlendirme ve İyileştirme

Şirket tarafından kişisel veri ihlallerine ilişkin tüm bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurul'un incelemesine hazır halde bulundurulması gerekmektedir. Kişisel Veri Koruma Komitesi Üst Kurulu, 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 Ekip, aşağıdaki unsurları içerir bir değerlendirme ve iyileştirme raporu hazırlar.

- Olası kişisel veri ihlallerinin etkilerini azaltmak için hangi adımların atılması gerektiği,
- Kişisel veri ihlali nedeniyle herhangi bir politika, prosedür ya da raporlamada iyileştirme gerekip gerekmediği,
- Kişisel veri ihlalinin tekrarlanmasını önleyebilmek için ek bir idari ve/veya teknik tedbir alınmasının gerekli olup olmadığı,
- İhlalin tekrarlanmasını önleyecek bir personel farkındalık eğitimi gerekliliği,
- İhlallere maruz kalmayı ve maliyet etkilerini azaltmak için kaynaklara/altyapıya ek yatırım yapılmasının gerekli olup olmadığı

7. İlgili Politika ve Prosedürler

Bu Prosedür, Şirket nezdinde kişisel verilerin korunması ve işlemesine ilişkin yürürlüğe konmuş tüm politika ve prosedürler ile birlikte ele alınmalıdır.

8. Güncelleme

Bu Prosedür kurumsal ya da yasal kaynaklı içeriklerindeki değişiklik gereksinimlerine bakılmaksızın yılda bir kez gözden geçirilerek kayıt altına alınır. Prosedür güncellenmemiş olsa bile, mevzuatta meydana gelen değişiklikler derhal uygulanacaktır.


SERTRANS
LOGISTICS