ZORLU GRAND HOTEL İŞLETMELERİ ANONİM ŞİRKETİ VERİ İHLALİ BİLDİRİM ve KRİZ SÜREÇ YÖNETİM POLİTİKASI

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 halinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve kurula bildirir. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."
Bu kapsamda Veri İhlali Bildirim ve Kriz Süreç Yönetim Politikası ("Politika"), Zorlu Grand Hotel İşletmeleri Anonim Şirketi ("Şirket") İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, Şirket tarafından benimsenecek ve uygulamada dikkate alınacak faaliyetleri belirlemek amacıyla hazırlanmıştır.

2. KAPSAM

Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamında olup Şirket'in sahip olduğu ya da yönettiği kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

3.TANIMLAR VE KISALTMALAR

Şirket Veri İhlali Bildirim ve Kriz Süreç Yönetim Politikasında kullanılan ve önem teşkil eden tanımlar aşağıda yer almaktadır:

İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi Örneğin: Tedarikçiler, misafirler, ziyaretçiler, çalışanlar ve çalışan adayları.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Örneğin: 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 hale 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. Örneğin, Şirket'in verilerini tutan bulut bilişim firması, acente, kanal yöneticisi vb.
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 Resmi Gazetede 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. SORUMLULUKLAR

Şirket politikanın tüm şirkette işleyiş, faaliyet ve süreçlerinde ve uygulanmasında, hukuki yönden risklerin ve yakın tehlikenin önlenmesinde Şirket genelinde tüm çalışanlarımız, paydaşlarımız, misafirler, ziyaretçiler ve ilgili üçüncü kişiler iş birliği yapmakla yükümlüdür. Şirket'in tüm birimleri Şirket Veri İhlali Bildirim ve Kriz Süreç Yönetim Politikasının uygulanmasından sorumludur.

5. VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

KVKK'nın 12. Maddesinde, İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, 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. KİŞİSEL VERİ İHLALİ

Kişisel veri ihlali, kişisel verilerin kanuna aykırı bir şekilde elde edilmesi, hukuka aykırı bir şekilde kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin yanlışlıkla/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,
- Kişisel veri içeren elektronik belgelerin, donanım veya yazılımlar aracılığıyla şirket dışına çıkarılması,
- 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 yanlışlıkla şirket dışında ilgisiz kişilere iletilmesi, gönderimi,
- Bilgi Teknolojileri (IT) ekipmanlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin; siber saldırı) gerçekleşmesi suretiyle kişisel verilere hukuka aykırı erişim sağlanması.

7. KRİZ MÜDAHALE EKİBİ

Kişisel veri ihlali durumunda oluşan veya oluşabilecek kriz durumuna müdahale etmek ve Kanun kapsamında öngörülen yükümlülükleri yerine getirmek için aşağıdaki departmanlardan belirlenen katılımcıların dahil edileceği bir Kriz Müdahale Ekibi oluşturulur. Bu ekip aşağıdaki katılımcılarla oluşturulmaktadır.

▪ Veri Sorumlusu İrtibat Kişisi

▪ Veri Sorumlusu Üst Yöneticisi (Genel Müdür)

▪ İhlalin Meydana Geldiği Departmanın Yöneticisi

▪ KVK Komitesi

▪ KVK Konusunda Veri Sorumlusu'nun Yetkilendirdiği Üst Yöneticiler

8. KRİZ MÜDAHALE SÜRECİ

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve kurula bildirir. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

Şirket'in kişisel veri ihlalini öğrendiği tarihten itibaren gecikmeksizin ve en geç yetmiş iki (72) saat içinde 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 olan www.zorlugrand.com üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapması gerekmektedir.

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

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

9. KRİZE İLİŞKİN ÖN DEĞERLENDİRME

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

- Kişisel veri ihlalinin gerçekleşme tarihi ve saati,
- Kişisel veri ihlalinin tespiti tarihi ve saati,
- Kişisel veri ihlali olayına ilişkin açıklamalar,
- 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.

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, İşletme içerisinde tanımlı KVK Üst Birimi ve KVK Kurul Üyeleri ile birlikte veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

10. ENGELLEME VE KURTARMA ÇALIŞMALARININ YÜRÜTÜLMESİ

Veri ihlalinin, Şirket ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için engelleme ve kurtarma çalışmaları Şirket içerisinde belirlenmiş olan KVK Üst Birim ve KVK Kurul Üyeleri 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.

11. RİSKLERİN DEĞERLENDİRİLMESİ

Kişisel veri ihlalleri, ihlalden etkilenen kişiler üzerinde kimlik hırsızlığı, hakların kısıtlanması dolandırıcılık, finansal kayıp, itibar kaybı, kişisel verilerin güvenliğinin kaybı, ayrımcılık gibi birçok olumsuz etki oluşturabilir. Bu nedenle kişisel veri ihlalinin olası sonuçlarının Şirket ve ihlalden etkilenen kişiler üzerinde ne gibi etkiler oluşturabileceğinin dikkatli bir şekilde değerlendirilmesi ve risklerin ortaya koyulması çok önemlidir.

Veri Sorumlusu İrtibat Yetkilisi, Şirket içerisinde belirlenmiş KVK Üst Birimi ve KVK Kurul Üyeleri 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 alınır. Bunların sonucuna göre veri ihlali "düşük düzeyde, orta düzeyde veya yüksek düzeyde risk" olarak nitelendirilir:

- Düşük düzeyde risk: İhlal ilgili kişiler üzerinde olumsuz herhangi bir etkiye neden olmamakta ya da bu etki ihmal edilebilir düzeyde kalmaktadır.

- Orta düzeyde risk: İhlal ilgili kişiler üzerinde olumsuz etkilere neden olabilir fakat bu etki büyük değildir.

- Yüksek düzeyde risk: İhlal etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere neden olmaktadır.

Orta ve özellikle yüksek düzeyde risk olarak tanımlanan veri ihlallerine ilişkin Veri Sorumlusu İrtibat yetkilisi Üst Yönetime, KVK Üst Birimine, KVK Kurul üyelerine ivedilikle bilgi vererek toplantıya davet eder ve riskin değerlendirme raporlarına ve ihlalin gerçekleşme ayrıntısına göre tüm süreçlerin koordinasyonunda görev alır.

12. 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.

13. KURULA BİLDİRİM

Veri Sorumlusu İrtibat Yetkilisi, öncelikle kişisel veri ihlalinden haberdar olduğu andan itibaren gecikmeksizin şirket içerisinde belirlenen KVK Üst Birimine, KVK Kurul Üyelerine ve en geç yetmiş iki (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 Yetkilisi'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 yetmiş iki (72) saat içerisinde Kurul'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenleri de Kurul'a açıklanır.

14. 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 bu bildirimler, Şirket içerisinde belirlenen KVK Üst Birimi ve KVK Kurul üyeleri ile Veri Sorumlusu İrtibat Kişisi tarafından belirlenen yöntem içerikle gerçekleştirilir.

Veri sorumlusu tarafından ilgili kişiye yapılacak olan ihlal bildirimi açık ve sade bir dille yapılır ve asgari olarak aşağıdaki bilgileri 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 web sayfasının tam adresi, çağrı merkezi, telefonla iletişim bilgileri vb. iletişim yollarına yer verir.

15. DİĞER BİLDİRİMLER

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. Şirket içerisinde belirlenen KVK Üst Birimi ve KVK Kurul üyeleri ile Veri Sorumlusu İrtibat Kişisi, böyle bir gereklilik olup olmadığını ayrıca değerlendirir ve gerekli ise bildirimleri yapar.

16. DEĞERLENDİRME VE İYİLEŞTİRME

Şirket 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 Yetkilisi Şirket içerisinde belirlenen KVK Üst Birimi ve KVK Kurul Üyeleri ile birlikte 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 hazırlar:

- Oluşan bu durumdan sonra 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,
- İhlallerin maliyet etkilerini gösteren raporu setlerinin hazırlanması.

17.POLİTİKANIN YÜRÜRLÜĞÜ, GÜNCELLENMESİ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirket'in internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

Yürürlükten kaldırılmasına karar verilmesi halinde, kurul kararı ile KVK Kurul üyeleri tarafından iptal edilerek karar defterinde KVK Kurul üyelerinin imzalarıyla birlikte imza altına alınır.

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler KVK Kurul üyeleri ile birlikte alınan kararlarla güncellenir.

18-YÜRÜTME

Dokümanın yürütme sorumluluğunu, Şirket KVK Kurul Üyelerine aittir.

19-DAĞITIM

Politika, Şirket internet sitesi http://www.zorlugrand.com ve Şirket intraneti http://zghintranet yayınlanarak, üçüncü taraflara ve Şirket çalışanlarına duyurulur.

EK-1: KVK Kurulu Veri İhlal Bildirim Formu

Kurul tarafından yayınlanmış olan Veri İhlali Bildirim Formuna aşağıdaki linkten erişebilirsiniz.
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e0413853-cd8c-428f-9315-2e8b3d874b46.pdf