

KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASI

1. AMAÇ

İşbu Kişisel Verilerin Saklanması ve İmhası Politikası'nın ("Politika") amacı; **YAZICI TURİZM MARMARİS İŞLETMELERİ A.Ş.** ("**Grand Yazıcı Club Turban**" veya "**Veri Sorumlusu**" tarafından işlenen kişisel verilerin işlenme sürelerinin belirlenmesi ve işleme süresi sona eren ve/veya işleme amacı ortadan kalkan kişisel verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesine ilişkin kriter ve yöntemlerin ortaya konulması ve bu süreçlerde görev alacak kişilerin rol ve sorumluluklarının tanımlanmasıdır.

İşbu Politika'da 28 Ekim 2017 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi hakkındaki Yönetmeliğin 6'ncı maddesinde yer alan veri güvenliğini sağlamak için alınmış teknik ve idari tedbirlere de yer verilmektedir. 30 Aralık 2017 tarihli Veri Sorumluları Sicili Hakkında Yönetmelik hükümleri ile Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi de bu çerçevede dikkate alınmıştır.

2. KAPSAM

İşbu Politika; 6698 Sayılı Kişisel Verilerin Korunması Kanununun ("KVKK") 7'nci maddesi uyarınca "veri sorumlusu" sıfatıyla **Grand Yazıcı Club Turban**'ın tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollar ile işlediği, elektronik ve/veya kağıt ortamda yer alan ve işleme şartları sona ermiş tüm kişisel verileri silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerini kapsamaktadır.

3.TANIMLAR

Bu dokümanda yer verilen özel tanımlardan:

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

Grand Yazıcı Club Turban

/ Veri Sorumlusu: Yazıcı Turizm Marmaris İşletmeleri A.Ş.'yi

Anonim Hale Getirme: Kişisel Verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

Silme : Kişisel Verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini,

Yok etme: Kişisel Verilerin kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesini,

İmha: Kişisel Verilerin silinmesini, yok edilmesini veya anonim hale getirilmesini,

Kanun: 6698 sayılı "Kişisel Verilerin Korunması Kanunu"nu,

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

İlgili Kişi: Kişisel Verileri işlenen gerçek kişiyi,

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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

Kurul: Kişisel Verileri Koruma Kurulu'nu,

Kişisel Veri İşleme

Envanteri: Veri Sorumlusu'nun iş süreçlerine bağlı olarak gerçekleştirmekte olduğu Kişisel Verileri İşleme faaliyetlerini; Kişisel Verileri İşleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve Kişisel Verileri İşleme amaçları için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen Kişisel Verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandığı envanteri,

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 verilerini,

Üçüncü Kişi: Yurtiçinde veya yurtdışında Kişisel Verilerin aktarıldığı şirket dışındaki üçüncü gerçek veya tüzel kişiyi,

Veri Sorumlusu

İrtibat Kişisi:

Veri Sorumlusu tarafından atanmış Kanun kapsamında oluşturulmuş süreçlerin idari takibini yapan gerçek kişiyi, ifade eder.

4. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN HUKUKİ, TEKNİK YA DA DİĞER SEBEPLERE İLİŞKİN AÇIKLAMA

Grand Yazıcı Club Turban, bünyesindeki departmanlar tarafından iş tanımları doğrultusunda yürütülen iş süreçleri ve bu süreçlere bağlı faaliyetleri gerçekleştirebilmek amacıyla çalışan, çalışan adayı, tedarikçi/taşeron, ziyaretçi, çevrimiçi ziyaretçi ve müşterilerine ait kişisel verileri işlemektedir. Bu kişisel verileri mevzuatta öngörülen veya ilgili departman tarafından kişisel veri işleme amacı çerçevesinde belirlenen süreler boyunca saklamaktadır. Tüm bu akış Kişisel Veri İşleme Envanterinde yer almaktadır. İlgili saklama süreleri sona erdiğinde ise, işbu Politika'da belirlenen silme, yok etme veya anonim hale getirme yöntemleri ile işleme amacı ortadan kalkan kişisel veriler imha edilmektedir.

5. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Bu kısımda Grand Yazıcı Club Turban tarafından alınan teknik ve idari tedbirlere yer verilmektedir. Grand Yazıcı Club Turban, kişisel verileri amacına uygun olarak ve belirlenen süreler boyunca kağıt ve elektronik ortamında kilit altında saklamaktadır.

Kişisel verilere yalnızca Grand Yazıcı Club Turban tarafından yetkilendirilmiş kişiler erişebilmekte olup, işbu yetki kişisel verilerin işlenmesine göre derecelendirilmiştir.

6. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Grand Yazıcı Club Turban bünyesinde saklanan Kişisel Veriler, yasal düzenlemeler saklı kalmak kaydı ile işleme amacının ortadan kalması durumunda, tabi olunan yasal düzenlemelerde öngörülen yasal saklama süresi, işleme amacının gerekli kıldığı sürenin sona ermesi halinde veya İlgili Kişi'nin talebi üzerine verilerin gizliliği göz önünde bulundurularak silme, yok etme ya da anonimleştirme süreçlerine tabi tutularak imha edilir.

Kişisel Veri İşleme Envanteri üzerinde yer alan tüm verilerin saklanma süreleri Veri Sorumlusu tarafından ilgili kanunlar ve yasal düzenlemeler dikkate alınarak belirlenir. Saklama süreleri ve Kişisel Verilerin imhasından İnsan Kaynakları Departmanı sorumludur. İnsan Kaynakları Departmanı kişisel verilerin silinmesini, sadece ilgili kullanıcılar tarafından kişisel verinin işlenebileceği, ilgisi olmayan diğer tüm bölümler için verinin işlenemeyeceği şekilde sağlar. Elektronik ortamdaki kişisel veriler için

gerekli olduđu ölçüde maskeleye yöntemleri kullanılır. Kağıt ortamdaki kişisel veriler için silme işlemi, silinmesi gereken kişisel verilerin karartılması şeklinde gerçekleştirilir.

Verilerin imha edilmesinde aşağıdaki yöntemlerden biri veya birkaçı kullanılır:

6.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

6.1.1. Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

6.1.2. Kişisel Verilerin Silinmesi Yöntemleri

a) Hizmet Olarak Uygulama Türü Bulut Çözümleri

Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

b) Kağıt Ortamında Bulunan Kişisel Veriler

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

c) Merkezi Sunucuda Yer Alan Ofis Dosyaları

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının

kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

d) Taşınabilir Medyada Bulunan Kişisel Veriler

Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

e) Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

İşleme amacı tamamen ortadan kalkan kağıt ve elektronik ortamdaki kişisel veriler, Kişisel Verileri Koruma Kurumu tarafından yayımlanan Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Rehberine uygun olarak yok edilir veya yine bu Rehber’de öngörülen yöntemlerle anonim hale getirilir. İnsan Kaynakları Departmanı tarafından gerçekleştirilen tüm silme, yok etme veya anonim hale getirme işlemleri elektronik ortamda zaman damgası ile loglanarak kayıt altına alınır. Kağıt ortamdaki kişisel veriler bakımından ise bu işlemlerin gerçekleştirildiğine ilişkin tutanak düzenlenir ve İnsan Kaynakları Departmanı tarafından muhafaza edilir. Elektronik ve kağıt ortamdaki kişisel verilere ilişkin silme, yok etme veya anonim hale getirmeye ilişkin kayıtlar üç yıl süre ile saklanır. Grand Yazıcı Club Turban ; kişisel verileri saklama süreleri boyunca sadece ilgili departmanların bu verilere erişimini sağlayacak şekilde “silme” yöntemini kullanır. Saklama sürelerinin bitmesi ve kişisel verinin saklanmasını gerektirecek herhangi bir başka amacın mevcut olmaması halinde ise anonim hale getirme yöntemini kullanır.

6.2.Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Grand Yazıcı Club Turban; kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

6.2.1.Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir:

a) Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.

- i) **Fiziksel Yok Etme:** Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.
- ii) **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

b) Çevresel Sistemler

Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

- i) Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- ii) Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, SSD, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- iii) Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- iv) Veri kayıt ortamı çıkartılabilir olan yazıcı gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- v) Veri kayıt ortamı sabit olan yazıcı, gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

c) Kağıt Ortamlar

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

d) Bulut Ortamı

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrlenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

- i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,
- ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

- iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması,

gerekir.

6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

Veri sorumlusu, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin anonim hale getirilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıdaki yöntemlerle gerçekleştirilir.

7. VERİLERİN İMHA SÜREÇLERİ

7.1.SAKLAMA VE İMHA SÜRELERİ TABLOSU

Veri türlerine göre saklama süreleri Kişisel Veri Envanteri'ndedir. İlgili temel mevzuattaki saklama süreleri ise belirtilenlerle sınırlı olmamak üzere **EK:** Saklama Süreleri Tablosu'ndadır. Ancak, Saklama Süreleri Tablosu'nda belirtilen ilgili mevzuatta değişiklik olması halinde güncel yeni mevzuat dikkate alınacaktır.

7.2. Periyodik İmha Süresi

Grand Yazıcı Club Turban; saklama süresi sona eren ve kişisel verinin saklanmasını gerektirecek başka herhangi bir veri işleme amacı mevcut olmayan kişisel verileri, saklama süresinin sona ermesini takiben 6 (altı) ay içerisinde siler/yok eder/anonim hale getirir. Periyodik imha süreci kapsamında İnsan Kaynakları Departmanı tarafından takip edilir.

7.3. İlgili Kişinin talep etmesi durumunda kişisel verilerin imha edilmesi

İlgili kişi, Grand Yazıcı Club Turban'a başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

- a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Grand Yazıcı Club Turban, talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Grand Yazıcı Club Turban, ilgili kişilerin silme veya yok etme taleplerini en geç "**otuz gün**" içinde sonuçlandırır.
- b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa; Grand Yazıcı Club Turban, bu durumu üçüncü kişiye bildirerek söz konusu kişisel verilerin silinmesi veya yok edilmesini talep eder.
- c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Grand Yazıcı Club Turban tarafından Kişisel Verilerin Korunması Kanunu'nun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç "**otuz gün**" içinde yazılı olarak ya da elektronik ortamda bildirilir.

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİNDE YETERLİ ÖNLEMLERE İLİŞKİN POLİTİKA

1 GİRİŞ

"YAZICI TURİZM MARMARİS İŞLETMELERİ A.Ş. ("Grand Yazıcı Club Turban" veya "Şirket") departmanları tarafından ilgili kişisel veri işleme süreç ve faaliyetleri kapsamında 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") md. 6 anlamında özel nitelikli kişisel veri işlenmektedir. Şirket'in işlediği bu özel nitelikli kişisel veriler; veri işleme amaçları ve şartları ışığında kişisel veri işleme envanterinde yer almaktadır. KVKK md. 6 özel nitelikli kişisel verilerin işleme şartlarını ikinci ve üçüncü fıkralarında düzenlemiştir. Dördüncü fıkra ise; özel nitelikli kişisel verilerin işlenmesinde KVKK md. 12 uyarınca alınması gerekli her türlü teknik ve idari tedbirin yanı sıra, KVK Kurulu ("Kurul") tarafından belirlenecek yeterli önlemlerin de alınmasının zorunlu olduğunu vurgulamaktadır. KVKK md. 6/f.4'ün atıf yaptığı bu Kurul kararı 7.3.2018 tarihli Resmi Gazete'de yayımlanmıştır.

Politikanın Amacı ve Kapsamı

İşbu Politika, Kurul kararı uyarınca; Grand Yazıcı Club Turban'ın işlediği özel nitelikli kişisel veriler açısından alması gereken yeterli önlemlerin neler olduğunu, Kişisel Verileri Koruma Kurumu ("Kurum") tarafından yayımlanan Kişisel Veri Güvenliği ile ilişkilendirerek açıklamaktadır.

Bu Politika özel nitelikli kişisel verinin işlendiği elektronik ve kağıt ortamları kapsamaktadır.

Politika Çerçevesi

1. Özel Nitelikli Kişisel Verilerin İşlenmesi Süreçlerinde Çalışanlara ve Müşterilere Yönelik Olarak Alınan Aksiyonlar

- a. **Eğitim:** KVKK ve ilgili ikincil mevzuat ile Kurul Kararları ve Rehberleri Doğrultusunda Özel Nitelikli Kişisel verilerin güvenliğine ilişkin olarak düzenli olarak çalışanlara eğitimler verilmelidir.
- b. **Gizlilik Sözleşmesi veya Taahhütnamesi:** Özel nitelikli kişisel verilere erişim yetkisi olan çalışanlarla, iş sözleşmesi dışında ayrıca spesifik olarak özel nitelikli kişisel veriler kapsamında gizlilik sözleşmesi veya taahhütname yapılması. Gerek iş sözleşmesi gerek gizlilik sözleşmesi veya taahhütnamesi içinde kişisel verilere ilişkin süresiz sır saklama yükümlülüğü getirilmelidir. Gizlilik anlaşmalarının ihlali durumunda yapılan ihlallerin raporlanması için bir süreç ve bu sürecin detaylarının verildiği prosedür ve gizlilik anlaşmasının ihlal edilmesi durumunda gerekli işlemler yapılmalıdır. Grand Yazıcı Club Turban, bilgi varlıklarının koruması için kritik bilgi varlıklarına erişim hakkı verilen tüm tedarikçilerle, üçüncü partilerle, sözleşmeli çalışanlarla ve tedarikçilerin alt işverenleri ile gizlilik anlaşmaları imzalanmalıdır.
- c. **Erişim Yetki ve Kontrolleri:** Özel nitelikli kişisel verilere erişim yetkisi olan çalışanların, yetki kapsamalarının ve sürelerinin net olarak tanımlanması gerekmektedir. Ayrıca bu yetkilerin periyodik olarak kontrollerinin yapılması gerekmektedir. Bu amaçla KVK Kurumu tarafından yayımlanan Veri Güvenliği Rehberi çerçevesinde erişim yetki ve kontrol matrisi oluşturulmalıdır. İşten ayrılan veya görev değişikliği gerçekleşen çalışanların, özel nitelikli kişisel veriye erişim yetkileri derhal kaldırılmalı ve üzerine kayıtlı elektronik ekipmanların iade alınması sağlanmalıdır. Organizasyon yapısındaki rol ve sorumluluklar tanımlanırken, mümkün olan her durum için görevler ayrılığı ve en düşük erişim hakkı ilkeleri göz önünde bulundurulmalıdır. Bu yapı ile birlikte, birbiriyle uyuşmayan roller aynı kişiye atanmamalıdır. Grand Yazıcı Club Turban çalışanlarına sorumluluklarının değişmesi durumunda yeni sorumluluklara göre yeni/ek yetkiler tayin edilmeden önce mutlaka eski yetkilerinde değişiklikler gerçekleştirilmelidir. Grand Yazıcı Club Turban, 3. parti çalışanlar için işten çıkarmaların düzenli bir biçimde yapılmasını ve bunun için Grand Yazıcı Club Turban içinde ilgili sorumlulukların tanımlanmasını sağlamalıdır. İşten veya projeden çıkarılan 3. parti çalışanlar ile görüşme yapılmadan önce işten ayrılan çalışanın bütün erişim hakları kaldırılmalı, sonrasında kişi üzerinde Grand Yazıcı Club Turban'a ait olan bütün varlıklar geri alınmalıdır. 3. parti çalışanları kendilerinde

bulunan Grand Yazıcı Club Turban varlıklarını işten ayrılma durumunda veya sözleşme sürelerinin sonunda ilgili Grand Yazıcı Club Turban personeline teslim etmelidir. Özel nitelikli kişisel veri barındıran bilişim sistemlerine ve hizmetlerine ait tüm erişimler, erişim verilmeden önce erişim hakkının onaylanmasını sağlayan bir kullanıcı kayıt prosedürü üzerinden sağlanmalıdır. Bilişim sistemlerine ve hizmetlerine erişimlerin kaldırılmasına yönelik otomatik veya zamanında bildirmeyi de sağlayacak bir erişim silme süreci izlenmelidir. Üçüncü tarafların özel nitelikli kişisel veri barındıran bilişim sistemlerine erişimi, bu gereksinimin detaylı bir analizi yapıp içerdiği riskler değerlendirildikten sonra sağlanmalıdır.

2. Özel Nitelikli Kişisel Verilerin İşlendiği, Muhafaza Edildiği ve Erişildiği Elektronik Ortamlarda Alınması Gerekli Yeterli Önlemler

- a. Özel nitelikli kişisel verilerin bulunduğu elektronik ortamların kriptografik yöntemler kullanılarak saklanması sağlanmalıdır.
- b. Bu amaçla kullanılan anahtarların güvenliğini sağlamak amacıyla, farklı ve güvenli ortamlarda muhafaza edilerek anahtar güvenliğinin sağlanması gereklidir.
- c. Özel nitelikli kişisel veriler üzerinde gerçekleştirilen tüm işlem hareketlerinin ve kayıtların loglanmasıdır. Kullanıcı faaliyetleri, istisnalar ve güvenlik olaylarının denetim izleri tutulmalı ve izlenmelidir. Denetim izleri aşağıdakileri içermelidir:
 - Başlangıç ve bitiş zamanları
 - Sistem hataları veya aksaklıkları ve alınan düzeltici önlemler
 - Veri dosyalarının ve sistem çıktılarının doğrulanması ve doğru bir şekilde işlenmesi
 - Denetim izi tutulan kişinin adı veya kullanıcı ismi

Erişim düzeyi yüksek (sistem yöneticileri ve sistem operatörleri gibi ayrıcalıklı kullanıcılar) kullanıcıların aktiviteleri kayıt altına alınmalı ve bağımsız biri tarafından düzenli olarak gözden geçirilmelidir.

Özel nitelikli kişisel veriler içeren uygulamalara erişimler ile Grand Yazıcı Club Turban ağına erişimler herhangi bir güvenlik ihlaline karşı izlenmelidir. Bu gibi durumlar için uygun mekanizmalar kurulmalıdır. Uzaktan erişim ancak sınırlı olarak sağlanmalı ve sistemler üzerinden verilen yetkiler doğrultusunda gerçekleştirilmelidir.

Denetim izleri, kayıt tutma ve saklama ihtiyaçlarına göre tutulmalıdır. Denetim izi tutma mekanizmaları ve denetim izleri yetkisiz erişimlere karşı korunmalıdır.

- d. Özel nitelikli kişisel verilere bir yazılım aracılığıyla erişilen hallerde veya bu verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi gerekir. Gerekli güvenlik testlerinin periyodik olarak yapılması veya yaptırılması ve sonuçların kayıt altına alınarak gerekli aksiyonların planlanması gereklidir.
- e. Bu verilere uzaktan erişim gereken hallerde en az iki faktörlü kimlik doğrulama sisteminin kullanılması gerekmektedir.

f. İşlenen özel nitelikli kişisel verinin biyometrik veri, sağlık verisi ve genetik veri olduğu durumlarda **"VERİ KORUMASI ETKİ ANALİZİ"** yapılması önemlidir.

3. Özel Nitelikli Kişisel Verilerin İşlendiği, Muhafaza Edildiği ve Erişildiği Fiziksel Ortamlarda Alınması Gerekli Yeterli Önlemler

- a. Özel nitelikli kişisel verinin bulunduğu ortam arşiv veya veri merkezi ise bu ortamların teknik ve fiziksel güvenliğini sağlamak amacıyla gerekli güvenlik önlemlerinin alınması gereklidir.
- b. İçlerinde barındırdıkları özel nitelikli kişisel veriye göre ofisler, odalar ve tesisler için fiziksel güvenlik kontrolleri tasarlanmalı ve uygulanmalıdır.
- c. Bu ortamlara yetkisiz giriş çıkışların engellenmesi gerekmektedir.

4. Özel Nitelikli Kişisel Verilerin Aktarımında Alınması Gereken Yeterli Önlemler

- a. Bu verilerin e-posta yoluyla aktarılması gereken durumlarda, mutlaka şifreli olarak kurumsal e-posta adresi ile veya KEP adresi kullanılarak aktarılması gerekmektedir. Ayrıca yine bu kapsamda olmak üzere; özel nitelikli kişisel veri içeren e-postaların kurumsal olarak "gizli" veya "hassas & gizli" olarak adlandırılan veri sınıfları ile etiketlenerek gönderilmesi sağlanmalıdır.
- b. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gereken hallerde, kriptografik yöntemlerle şifrelenmesi ve anahtarların farklı ortamlarda tutularak anahtar yönetiminin ve güvenliğin sağlanması.
- c. Farklı fiziksel ortamlardaki sunucular arasında aktarım yapılacak ise, VPN kurularak veya benzeri yöntemlerle aktarımın gerçekleştirilmesi.
- d. Kağıt ortam yoluyla aktarım gerekiyorsa, evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın gizlilik dereceli bilgiler çerçevesinde gönderilmesi gerekir.

** İşbu politikanın hazırlanmış olduğu Türkçe dilindeki hali ile herhangi bir çeviri hali arasında bir uyumsuzluk çıktığı hallerde, Türkçe metin dikkate alınmalıdır.

** İşbu politika Grand Yazıcı Otel İşletmeleri Anonim Şirketi'nin yazılı izni olmaksızın çoğaltılıp dağıtılamaz