KINGFISHER PLC

Veri Koruma Standardı

Belge Sorumlusu:	Grup Veri Koruma Sorumlusu
Belgenin muhatabı:	Tüm Kingfisher Şirketleri
İlgili Politika	Veri Koruma Politikası
Yeni inceleme tarihi:	9 Ocak 2019
İlgili Politika Belgeleri:	Veri Koruma Politikası, Belge Saklama ve Kayıt Tutma Politikası, Belge Saklama ve Kayıt Tutma Standartları Bilgi Güvenliği Politikası, Kabul Edilebilir Kullanım Politikası

İçindekiler

1. Özet ve amaçlar

Bu Politika Standardının amacı, veri koruma ve gizlilik kanunlarına uymayı sağlamak ve müşterilerimizin, çalışanlarımızın ve tedarikçilerimizin bilgilerinin Kingfisher Grup Şirketlerinin faaliyet gösterdiği tüm yargı bölgelerinde her zaman uygun şekilde toplandığından ve kullanıldığından emin olmaktır.

Bu Politika Standardında, "**Kişisel Veri**", tek başına ya da başka bilgilerle birlikte alınan ve bir kişinin ("**Birey**") tanımlanmasına olanak sağlayan bilgi anlamına gelir. Bu bilgiler, örneğin bir bireyin iş e-posta adresini, posta adresi veya doğum tarihiyle birlikte adını, bir bireyin fotoğrafını vb. içerir.

Kişisel Veri güvenli tutulmalı ve adil, şeffaf bir şekilde ve her zaman kanunlara uygun olarak işlenmelidir.

Her Grup Şirketi, faaliyet gösterdiği bölgelerde geçerli olan düzenleme çerçevesi hakkında bilgi sahibi olmalıdır.

- Avrupa Birliği'nde, AB Genel Veri Koruma Tüzüğü (GDPR) [2016/679 Sayılı Tüzük (AB)], gizlilikle ilgili diğer kanunlar veya yerel veri koruma kuralları ile birlikte 25 Mayıs 2018 tarihinden itibaren geçerli olacaktır;
- Avrupa Birliği dışında, Grup Şirketinin faaliyetleri için geçerli olan tüm yerel veya bölgesel kanunlara uyulmalıdır.

Grup Veri Koruma Sorumlusu, Kingfisher'ın faaliyet gösterdiği her bir ülkede veri koruma sorularından sorumlu olan kişinin ("**Veri Koruma Ülke Temsilcisi**") desteği ile etkili uyumluluk prosedürleri oluşturacak ve uygulayacaktır.

2. Sorumluluk ve yönetim

2.1 GRUP VERİ KORUMA SORUMLUSU bu Politika Standardından ve bunun Grup genelinde uygulanmasından sorumludur.

Veri Koruma Sorumlusunun rolü ve sorumlulukları şu şekildedir:

- Yönetim Kuruluna veri koruma sorumlulukları, riskleri ve sorumlulukları hakkında güncel bilgiler vermek;
- tüm veri koruma prosedürlerini ve politikalarını düzenli bir şekilde incelemek ve onaylamak;
- prosedürlere, politikalara ve geçerli veri koruma ve gizlilik kanunları ile uyumluluğu izlemek;
- tüm personel ve bu politikada bahsedilenler için veri koruma eğitimi ve tavsiyesi ayarlamak;
- personelden, kurul üyelerinden ve diğer paydaşlardan veri korumayla ilgili gelen soruları yanıtlamak;

- kendileri hakkında hangi bilgilerin saklandığını öğrenmek isteyen müşteriler ve çalışanlar gibi bireylere yanıt vermek ve şirketin verilerini ele alan üçüncü taraflarla veri işlemeye ilişkin tüm sözleşmeleri veya anlaşmaları kontrol etmek ve onaylamak;
- gizlilik etki değerlendirmelerini denetlemek ve incelemek;
- ana denetleyici kurum için irtibat noktası olarak hareket etmek ve yerel denetleyici kurumlarla işbirliği yapmak.

Veri Koruma Sorumlusu ile şu adresten iletişime geçilebilir: dpo@kingfisher.com

Tüm Kingfisher şirketlerinin ve Grup dahilindeki tüm fonksiyonların Veri Koruma Sorumlusunun görevini yerine getirmek için makul şekilde ihtiyaç duyabileceği tüm bilgileri gecikmeksizin ifşa etmesi gerektiğini lütfen unutmayın.

2.2 **VERİ KORUMA ÜLKE TEMSİLCİSİ** şunlardan sorumludur:

- Veri Koruma Sorumlusunun, gizliliğe ilişkin yerel yasaları ve Veri Koruma kanunlarını anlamasına yardımcı olmak;
- Veri Koruma Sorumlusunun, Kingfisher Grup Şirketlerinin faaliyet gösterdiği bir ülke veya bölgedeki veri koruma kurallarını ve süreçlerini tanımlamasına yardımcı olmak;
- Veri Koruma Görevlisi ile bir ülkedeki ilgili Kingfisher Grup Şirketleri arasında veri koruma ve gizlilik konularında bağlantı noktası olarak hareket etmek.

Veri Koruma Ülke Temsilcilerinin bir listesi İntranet'te mevcuttur ve güncellemeler İç İletişim Departmanı tarafından düzenli olarak iletilecektir.

2.3 **BT YÖNETİM EKİBİ** Kingfisher ve üçüncü taraf sistemlerinin veri güvenliğini sağlamaktan sorumludur.

Bir Grup Şirketi tarafından ya da bir üçüncü tarafça veri işlenmesi durumunda her zaman BT Yönetim ekibine danışılmalıdır. BT Yönetim ekibindeki irtibat noktaları İntranet'te ayrıntılı şekilde belirtilmiştir ve güncellemeler İç İletişim Departmanı tarafından düzenli olarak iletilecektir.

BT Yönetim Ekibinin rolü ve sorumlulukları:

- tüm sistemlerin, hizmetlerin, yazılımların ve ekipmanların kabul edilen güvenlik standartlarını karşılamasını sağlamak;
- tüm sistemlerin, hizmetlerin, yazılımların ve ekipmanların; veri koruma politikaları, standartları, süreçleri, ilkeleri ve ilgili ülkelerin kanunları ile uyumluluk sağladığından emin olmak;
- sistem ve bilgi güvenliği politikalarının ve sözleşme belgelerinin taslaklarını hazırlamak;
- üçüncü taraf durum tespitleri yapmak.

3. Grup Minimum standartları

Kingfisher Grup Şirketlerinin faaliyet gösterdiği bir yargı bölgesinin geçerli kanunları daha sıkı bir gereksinimi zorunlu kılmadığı müddetçe (bu durumda daha sıkı olan gereklilikler geçerli olacaktır) çalışanların, müşterilerin ve tedarikçilerin Kişisel Verilerini ele alırken Kingfisher Grubu genelinde her zaman aşağıdaki standartlara uyulacaktır. Daha ayrıntılı ve ülkeye özel kurallar, Veri Koruma Sorumlusu ya da Ülke Veri Koruma Temsilcisi tarafından her bir Kingfisher Grup Şirketine iletilecektir.

3.1 Verilerin toplanması:

Kişisel Veri toplamadan önce:

- yalnızca amaç için gerekli olan en az miktarda Kişisel Veri topladığımızdan emin olmalıyız;
- toplama amacının meşru olduğundan ve bireylerin haklarını ihlal etmediğinden emin olmalıyız;
- Bireyleri Kişisel Verilerini ne şekilde kullanmayı amaçladığımız ve toplama amacımız hakkında açık bir şekilde bilgilendirmeliyiz;
- Kişisel Verilerin güvenli bir şekilde toplanıp saklandığından ve izinsiz erişimi ya da Kişisel Verilerin zarar görmesini veya kaybolmasını önlemek için yeterli güvenlik önlemleri aldığımızdan emin olmalıyız.

3.2 Verilerin kullanılması:

- Kişisel Verilerin bunlara erişimi olmayan kişilerin kullanımına sunulmadığından emin olmalıyız;
- Kişisel Verilerin yalnızca toplandıkları amaçlar için ve ilgili Bireyin makul şekilde bekleyeceği biçimde kullanıldığından emin olmalıyız;
- verilerin güvenli bir şekilde ele alınıp saklandığını ve izinsiz erişime, hasara veya kayba karşı korunduğunu düzenli olarak kontrol etmeli ve doğrulamalıyız;
- aşağıdaki bilgileri tanımlamalı ve her zaman Veri Koruma Sorumlusu tarafından iletilecek bir formatta kaydetmeliyiz: (i) toplanan ve kullanılan verilerin kategorileri, (ii) verileri işlenecek olan Bireylerin kategorileri, (iii) Kişisel Verilerin ifşa edileceği veya ifşa edildiği alıcıların kategorileri, (iv) verilerin saklandığı konumun/konumların adresi.
- Bireyin işteki performansıyla, ekonomik durumlarıyla, sağlığıyla, kişisel tercihleriyle, ilgi alanlarıyla, güvenilirliğiyle, davranışlarıyla, konumuyla veya hareketiyle ilgili belirli yönleri analiz etmek veya tahmin etmek için Bireyin belirli kişisel yönlerini değerlendirmek şeklinde Birey hakkında otomatik kararlar alınmasıyla sonuçlanan herhangi bir otomatik işleme aracı kullanılmadan önce her zaman Veri Koruma Sorumlusu veya Veri Koruma Ülke Temsilcisi ile irtibata geçilmelidir

3.3 Verilerin aktarılması:

Kingfisher Grubu dışındaki herhangi bir işleyiciye Kişisel Veri erişimi (aktarma ya da uzaktan erişim aracılığıyla) sağlamadan önce:

- Kişisel Veri aktardığımız işleyicinin bu Standarda ve geçerli kanunlara uyduğundan emin olmalıyız;
- aşağıdaki bilgileri tanımlamalı ve her zaman kaydetmeliyiz: (i) işleyicinin temsilcisinin ve veri koruma sorumlusunun adı ve irtibat bilgileri, (ii) işlenen verilerin kategorileri, (iv) verileri işlenecek olan Bireylerin kategorileri, (v) verilerin aktarılacağı/verilere erişilecek konumların adresi, (vi) tüm alt işleyicilerin listesi

ve kurumsal bilgileri ve (vi) Kişisel Verilerin ifşa edildiği veya ifşa edileceği alıcıların kategorileri;

- söz konusu ülke veya bölge Bireylerin kişisel verilerin işlenmesine ilişkin haklarıyla ilgili yeterli seviyede koruma sağlamadığı veya taraflar arasında yeterli güvenceyi içeren yazılı bir sözleşme imzalanmadığı (veya geçerli koruma kanunlarına uygun şekilde bu tür güvenceler sağlamak için alternatif düzenlemeler uygulanmadığı) sürece Kişisel Verilerin başka bir ülkeye veya bölgeye aktarılmadığından/Kişisel Verilere başka bir ülkeden veya bölgeden erişilmediğinden emin olmalıyız.

3.4 Verilerin saklanması

Kişisel Veriler, toplanma amacı için gerekli olandan daha uzun süreyle saklanmamalıdır (yukarıdaki madde 3.1). Bu, verilere artık ihtiyaç kalmadığında verilerin şirket sistemlerinden imha edilmesi veya güvenli bir şekilde bertaraf edilmesi gerektiği anlamına gelir.

Örnek: Müşteri, bir elektrikli alet kazanmak için adını, adresini ve telefon numarasını içeren bir form doldurarak bir yarışmaya katıldı ve Grup Şirketi'nden ek iletişim almak istemediğini belirten bir kutucuğu işaretledi. Çekiliş yapıldıktan sonra Grup Şirketi müşterinin formda gönderdiği detayları silmelidir çünkü toplanma amacı için artık bunlara ihtiyaç yoktur.

Kingfisher'ın belge saklamaya ilişkin politikasına ve saklama süresine ilişkin kanunlara uyulmalıdır.

3.5 Bireylerin Hakları

Veriler, Bireylerin haklarına uygun şekilde işlenmelidir. Bireylerin hakları ülkeye göre farklılık gösterir. Avrupa Birliği'nde, Bireyler şu konularda geniş haklara sahiptir:

(a) Kişisel Verilerinin işlenmesi onayını iptal etme (işleme, onaya dayalı olarak yapılıyorsa);
(b) Kişisel Verilerinin işlenmesine itiraz etme (işleme, meşru menfaatlere dayalı olarak yapılıyorsa);
(c) kendileri hakkında tutulan her türlü Kişisel Veriye erişme;
(d) doğru olmayan tüm Kişisel Verileri düzelttirme;
(e) Kişisel Verilerini şirket sistemlerinden sildirme;
(f) kişisel verilerinin başka şirketlere aktarılmasını sağlama;
(g) kendileri ya da başkaları açısından hasara ya da rahatsızlığa yol açma ihtimali olan işlemeleri önleme.

3.6 Şikayet ve ihlaller

Kişisel Verileri etkileyen her türlü güvenlik ihlali dahil olmak üzere her türlü şikayet ve ihlal derhal Veri Koruma Sorumlusuna ve/veya herhangi bir temsilciye bildirilmelidir.

Kişisel Verileri etkileyen her türlü güvenlik ihlali şikayetleri derhal BT Yönetimi Başkanına bildirilmelidir.

Kişisel Verilerin yok olmasına, kaybolmasına, değiştirilmesine, yetkisizce ifşa edilmesine veya Kişisel Verilere erişilmesine yol açan her türlü hırsızlık, kötüye kullanım veya güvenlik ihlali derhal (her durumda en geç 2 saat içinde) Veri Koruma Sorumlusuna ve BT Yönetimi Başkanına bildirilmelidir.

4. İzleme ve Denetim

Bu Politika Standardıyla uyumluluğu sağlamak için bu Politikayla ve Veri Koruma Sorumlusu veya Veri Koruma Ülke Temsilcileri tarafından getirilen veri korumayla ilgili diğer süreçler ve kurallarla uyumluluk, periyodik olarak denetlenmelidir.

Bu Politika Standardının konusuna ilişkin herhangi bir şüpheniz varsa Grup Veri Koruma Sorumlusundan ya da Veri Koruma Ülke Temsilcinizden tavsiye almalısınız.

Endişelerinizi bildirmek için ihbar hattını da kullanabilirsiniz.

5. İzin ve Onayların İncelenmesi

Eylem/durum	İletişim		Kime/kim tarafından?
	(Önceki) Bildirim	Önceki Onay	
Veri İhlali	X		Grup Veri Koruma Sorumlusu* + Yönetim Başkanı
Otomatik karar alma (Profil oluşturma dahil)	X	X	Grup Veri Koruma Sorumlusu + Yönetim Başkanı
Veri sahibi şikayetleri	X		Grup Veri Koruma Sorumlusu
Tüzükle ilgili sorgular	X		Grup Veri Koruma Sorumlusu + Grup Hukuk Direktörü
Düzenleyici yaptırım eylemi	X		Grup Veri Koruma Sorumlusu + Grup Hukuk Direktörü
Veri sahiplerinin haklarının kullanılması	X		Grup Veri Koruma Sorumlusu
Veri Gizliliği Etki Değerlendirmesi gerekliliğini tetikleyen yeni işleme faaliyetleri	X	X	Grup Veri Koruma Sorumlusu + Yönetim Başkanı

*Her durumda, doğrudan ya da ülkedeki Veri Koruma Ülke Temsilcisi aracılığıyla.