Veri Koruma Etki Değerlendirmesi (DPIA) Politikası

1. Amaç

Bu politikanın amacı, Evrensel Ağız ve Diş Sağlığı Ltd. Şti.'nin **("Kurum")** tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinde potansiyel riskleri tespit etmek ve bu riskleri en aza indirmek için GDPR'ye uygun şekilde bir **Veri Koruma Etki Değerlendirmesi (DPIA)**süreci uygulamaktır. DPIA, özellikle yeni teknolojilerin kullanıldığı veya yüksek risk taşıyan veri işleme faaliyetleri için gereklidir.

2. Veri Koruma Etki Değerlendirmesi (DPIA) Nedir?

DPIA, kişisel verilerin işlenmesinin bireylerin hak ve özgürlüklerine yönelik oluşturabileceği riskleri belirleyen ve bu riskleri hafifletmek için alınacak önlemleri içeren bir süreçtir. GDPR'nin 35. maddesi kapsamında, bir veri işleme faaliyeti "yüksek risk" taşıyorsa, bir DPIA yapılması zorunludur.

2.1. Yüksek Riskli Veri İşleme Faaliyetleri

DPIA'nın gerekli olduğu durumlar arasında şunlar bulunabilir:

- Büyük ölçekli, sistematik ve kapsamlı veri işleme faaliyetleri
- Özel nitelikli kişisel verilerin işlenmesi (örneğin, sağlık verileri)
- Kişisel verilerin sistematik olarak izlenmesi (örneğin, gözetim sistemleri)
- Otomatik karar verme ve profil oluşturma faaliyetleri

3. DPIA Süreci

3.1. Hazırlık ve Planlama

DPIA süreci, kişisel veri işleme faaliyetine başlamadan önce gerçekleştirilir. Bu aşamada aşağıdaki adımlar izlenir:

- İlgili veri işleme faaliyeti ve kapsamı belirlenir.
- Hangi kişisel veri türlerinin işleneceği tanımlanır.
- Veri sahiplerinin kimler olduğu ve ne kadar kişinin etkileneceği belirlenir.

3.2. Risklerin Tanımlanması

Veri işleme faaliyeti sırasında bireylerin hak ve özgürlüklerine yönelik potansiyel riskler belirlenir. Bu riskler arasında şunlar yer alabilir:

- Kişisel verilerin yetkisiz erişim veya ifşası
- Verilerin değiştirilmesi veya silinmesi
- Gizlilik ihlali
- Veri sahiplerinin haklarını kullanamaması

3.3. Risklerin Değerlendirilmesi

Her bir riskin olasılığı ve etkisi değerlendirilir. Bu aşamada, riskin ne derece ciddi olduğu ve ortaya çıkma olasılığı göz önünde bulundurulur. Riskler **düşük, orta, yüksek** şeklinde sınıflandırılır.

3.4. Risk Azaltıcı Önlemler

Belirlenen risklere karşı alınacak güvenlik ve koruma önlemleri belirlenir. Bu önlemler şunlar olabilir:

- Veri minimizasyonu (yalnızca gerekli verilerin işlenmesi)
- Verilerin şifrelenmesi ve anonimleştirilmesi
- Yetkisiz erişimlere karşı güvenlik protokollerinin uygulanması
- Düzenli güvenlik denetimlerinin yapılması

3.5. Sonuçların Belgelendirilmesi

DPIA'nın sonuçları belgelenir ve gerektiğinde veri koruma otoritesine sunulmak üzere kayıt altına alınır. Bu belgeler, risk değerlendirmelerini, alınan önlemleri ve değerlendirme sürecini içerir.

3.6. DPIA Sonrası Eylem Planı

Eğer DPIA sonuçlarına göre veri işleme faaliyeti kabul edilebilir bir risk taşıyorsa, veri işleme faaliyetleri başlatılır. Ancak riskler kabul edilemeyecek kadar yüksekse, işleme faaliyetleri gözden geçirilir ve gerekirse durdurulur.

4. Veri Koruma Sorumlusunun (DPO) Rolü

Veri Koruma Sorumlusu (DPO), DPIA sürecinin doğru ve eksiksiz bir şekilde yürütülmesinden sorumludur. DPO, risklerin tespiti, analiz edilmesi ve raporlanması süreçlerinde aktif rol alır. Ayrıca, yüksek riskli durumlar tespit edildiğinde veri koruma otoritesiyle iletişime geçmekten sorumludur.

5. DPIA Gerekliliğinin Değerlendirilmesi

Veri işleme faaliyetinin yüksek risk taşıyıp taşımadığını belirlemek için aşağıdaki sorular sorulur:

- Bu işlem, büyük çaplı kişisel veri işleme içeriyor mu?
- Otomatik karar verme veya profil oluşturma gibi faaliyetler söz konusu mu?
- Hassas veri kategorileri işleniyor mu?
- Veriler üçüncü taraflarla paylaşılıyor mu?

6. Gözden Geçirme ve Güncelleme

Veri işleme faaliyetlerinde değişiklikler olduğunda veya yeni riskler ortaya çıktığında DPIA gözden geçirilir ve güncellenir. Ayrıca, düzenli aralıklarla DPIA süreçlerinin etkinliği değerlendirilir.

7. Dokümantasyon ve Kayıt Tutma

Tüm DPIA değerlendirmeleri, GDPR gereğince belgelendirilir ve denetimler için uygun bir şekilde muhafaza edilir. Kayıtlar, veri işleme faaliyetleri, risk değerlendirmeleri ve alınan önlemlerle ilgili tüm bilgileri içermelidir.

Son Güncelleme: 06.11.2024

Veri Koruma Sorumlusu İletişim Bilgileri:

- İsim: Özge Topuz
- E-posta: info@evrenseldis.com.tr