

VERİ İHLALI MÜDAHALE POLİTİKASI



İçindekiler

İçindekiler
1.AMAÇ VE KAPSAM
2. KAPSAM
3.TANIMLAR VE KISALTMALAR
4. SORUMLULUKLAR
5. Veri güvenliğine ilişkin yükümlülükler
6-POLİTİKA'NIN VE İLGİLİ MEVZUATIN UYGULANMASI
7-REVİZYON VE YÜRÜLÜLÜKTEN KALDIRMA
8-POLİTİKANIN YÜRÜRLÜĞÜ
9-YÜRÜTME
10-DAĞITIM

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 hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri İhlali Müdahale Politikası ("Politika"), DEOSGB İŞ SAĞLIĞI VE GÜVENLİĞİ ANONİM ŞİRKETİ ("Şirket") İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, 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 Şirketimizce yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

3.TANIMLAR VE KISALTMALAR

Şirket Veri İhlali Müdahale Politikası'nda kullanılan ve önem teşkil eden tanımlar aşağıda yer almaktadır:

İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Müşteriler, ziyaretçiler, çalışanlar ve çalışan adayları.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Ör: ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.



KİŞİSEL VERİLERİN İŞLENMESİ:	<i>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 işlem.</i>
VERİ İŞLEYEN:	<i>Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişidir. Örneğin, Şirket'in verilerini tutan bulut bilişim firması, talimatlar çerçevesinde arama yapan call-center firması vb.</i>
VERİ SORUMLUSU:	<i>Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder.</i>
KVK KANUNU:	<i>7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.</i>
KVK KURUMU:	<i>Kişisel Verileri Koruma Kurumu.</i>
KVK KURULU:	<i>Kişisel Verileri Koruma Kurulu.</i>
KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİNE İLİŞKİN YÖNETMELİK:	<i>20 Ekim 2016 tarihli ve 29863 sayılı Resmi Gazete'de yayımlanan, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik.</i>

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 organ ve departmanları Şirket Veri İhlali Müdahale Politikasının uygulanmasından sorumludur.

5. Veri güvenliğine ilişkin yükümlülükler

KVKK'nın 12. Maddesinde, İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu tarafından alınması gereken önlemler tanımlanmıştır.

Veri sorumlusu;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
- Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.*

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

Buna göre, İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, Şirket söz konusu veri ihlalini, en kısa sürede (en geç 72 saat) Kurul'a ve söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip makul olan en kısa süre içerisinde ilgili kişiye bildirmelidir.

İlgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa Şirketin kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmalıdır.



Veri sorumlusu tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak;

- 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 vb. iletişim yolları unsurlarına yer verilmesi gerekir.

Kurula yapılacak bildirimde yine Kurul'un belirlediği ve web sitesinde yayınladığı KVK Kurulu Veri İhlal Bildirim Formu doldurularak Kurula iletilir.

Şirket tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanması gerekmektedir.

Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal vermeksizin aşamalı olarak sağlanmalıdır.

Şirket tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulması sağlanmalıdır.

Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyen bu konuda herhangi bir gecikmeye yer vermeksizin Şirket'e bildirimde bulunmalıdır.

Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmalıdır.

Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu plan gözden geçirilmelidir.

6-POLİTİKA'NIN VE İLGİLİ MEVZUATIN UYGULANMASI

Politika'da değişiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir. Güncelleme tablosu "Doküman Künyesi"nde yer almaktadır.

7-REVİZYON VE YÜRÜLÜKTEN KALDIRMA

İşbu Politika yılda bir defa, ilgili Şirket Hukuk Müşavirliği tarafından gözden geçirilir ve güncellenir.

8-POLİTİKANIN YÜRÜRLÜĞÜ

İşbu Politika, Şirket'in internet sitesinde (<https://deosgb.com.tr/>) yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

9-YÜRÜTME

Dokümanın yürütme sorumluluğunu, Şirket KVK Bölümü'ne aittir.

10-DAĞITIM

Politika, Şirket internet sitesinde ve Şirket intranetinde yayınlanarak, üçüncü taraflara ve Şirket çalışanlarına duyurulur.

EK-1: KVK Kurulu'nun Web Sitesinde yayınladığı Veri İhlal Bildirim Formu

