

DECA BİLGİ TEKNOLOJİLERİ A.Ş.

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI

BÖLÜM 1: AMAÇ VE KAPSAM

1.1. Amaç

Bu politikanın amacı, DECA Bilgi Teknolojileri A.Ş. ("Şirket") tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") ve ilgili mevzuat uyarınca kişisel verilerin hukuka uygun biçimde işlenmesi, korunması ve veri sahiplerinin haklarının güvence altına alınması için benimsenen prensipleri belirlemektir.

1.2. Kapsam

Bu politika; Şirketimizin müşterileri, potansiyel müşterileri, iş ortakları, tedarikçileri, çalışanları, çalışan adayları, stajyerleri, web sitesi ziyaretçileri ve teknoloji/yazılım çözümlerimizden faydalanan diğer tüm üçüncü kişilere ait kişisel verilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesini kapsar.

BÖLÜM 2: KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER

Şirketimiz, kişisel verileri aşağıdaki ilkelere sıkı sıkıya bağlı kalarak işler:

- Hukuka ve dürüstlük kurallarına uygun olma.
- Doğru ve gerektiğinde güncel olma.
- Belirli, açık ve meşru amaçlar için işlenme (Yazılım geliştirme, lisanslama, Ar-Ge ve teknik destek süreçleri vb.).
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma (Sadece projenin veya hizmetin gerektirdiği minimum verinin talep edilmesi).
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

BÖLÜM 3: KİŞİSEL VERİLERİN İŞLENME AMAÇLARI

Bilişim ve teknoloji faaliyetlerimiz kapsamında toplanan kişisel veriler ağırlıklı olarak şu amaçlarla işlenmektedir:

Faaliyet Alanı	İşleme Amaçları
Yazılım ve Teknoloji Hizmetleri	Ürün lisanslamalarının yapılması, kullanıcı hesaplarının oluşturulması, sistem hatalarının giderilmesi (bug-fix), API ve entegrasyon süreçlerinin yönetimi, bulut tabanlı hizmetlerin sunulması.
Ar-Ge ve Proje Geliştirme	TÜBİTAK, KOSGEB, AB fonları ve Teknopark projeleri kapsamında mevzuatsal bildirimlerin yapılması, simülasyon ve yapay zeka eğitim modelleri için veri setlerinin anonimleştirilerek kullanılması.
Ticari Operasyonlar (B2B)	Kurumsal müşterilerle sözleşme süreçlerinin yürütülmesi, faturalandırma, e-fatura/e-arşiv operasyonları, teknik destek (helpdesk) taleplerinin karşılanması ve müşteri ilişkileri yönetimi (CRM).

Faaliyet Alanı	İşleme Amaçları
İnsan Kaynakları	Çalışan ve stajyer adaylarının değerlendirilmesi, özlük dosyalarının oluşturulması, SGK bildirimleri, performans yönetimi ve şirket içi iletişim ağlarının (Slack, Microsoft Teams, e-posta) kurulması.
Bilgi Güvenliği	Şirket ağının, sunucuların ve web sitelerinin siber saldırılara karşı korunması, erişim loglarının (5651 sayılı kanun gereği) tutulması, veri yedekleme operasyonları.

BÖLÜM 4: KİŞİSEL VERİLERİN AKTARILMASI (YURT İÇİ VE YURT DIŞI)

Şirketimiz, kişisel verileri "Bilme İhtiyacı" (Need to Know) prensibine göre aktarır.

Yurt İçi Aktarım: İş süreçlerinin yürütülmesi amacıyla; bağımsız denetim firmalarına, mali müşavirlere, hukuk danışmanlarına, bankalara, e-fatura entegratörlerine, yetkili kamu kurumlarına (SGK, BTK, Teknopark Yönetimleri, TÜBİTAK vb.) ve iş ortaklarımıza yasal sınırlar çerçevesinde veri aktarımı yapılmaktadır.

Yurt Dışı Aktarım: Bilişim sektörünün doğası gereği; kullanılan global bulut altyapıları, sunucu barındırma hizmetleri, kod depoları ve global CRM/iletişim yazılımları nedeniyle kişisel veriler yurt dışına aktarılabilir. Bu aktarımlar, Kurul'un belirlediği güvenli ülkelere veya ilgili kişinin açık rızası/standart sözleşmeler kapsamında gerçekleştirilir.

BÖLÜM 5: VERİ GÜVENLİĞİ İÇİN ALINAN TEKNİK VE İDARİ TEDBİRLER

Şirketimiz, güvenlik standartlarını teknoloji operasyonlarına uyarlayarak aşağıdaki tedbirleri uygular:

Teknik Tedbirler:

- Veri tabanlarında ve sunucularda güçlü şifreleme (encryption) ve kriptografik algoritmaların kullanılması.
- Şirket içi ağlarda güvenlik duvarları (Firewall), Saldırı Tespit ve Engelleme Sistemleri (IDS/IPS) kullanılması.
- Yazılım geliştirme ve test ortamlarında (Test/Dev environments) gerçek kişisel verilerin maskelenmesi veya sentetik veri kullanılması.
- Sistemlere erişimde İki Aşamalı Doğrulama (2FA) ve Rol Bazlı Erişim Kontrolü (RBAC) uygulanması.

İdari Tedbirler:

- Çalışanlarla ve iş ortaklarıyla Gizlilik Sözleşmelerinin (NDA) imzalanması.
- Çalışanlara periyodik olarak siber güvenlik ve KVKK farkındalık eğitimleri verilmesi.
- Veri ihlali durumunda uygulanacak "Siber Olaylara Müdahale Planı"nın hazır bulundurulması.

BÖLÜM 6: SAKLAMA, İMHA VE İLGİLİ KİŞİNİN HAKLARI

6.1. Saklama ve İmha:

Kişisel veriler, işlendikleri amaç için gerekli olan süre veya yasal mevzuatta (örn. Türk Ticaret Kanunu, Vergi Usul Kanunu, İş Kanunu) öngörülen süreler boyunca saklanır. Sürelerin bitiminde veriler;

řirketimizin "Kiřisel Veri Saklama ve İmha Politikası"na uygun olarak periyodik imha sűreçlerinde (silme, yok etme veya anonimleřtirme) geri dűndűrűlemez řekilde sistemlerden temizlenir.

6.2. İlgili Kiřinin Hakları:

Veri sahipleri KVKK'nın 11. maddesi uyarınca; verilerinin iřlenip iřlenmedięini űęrenme, amacına uygun kullanılıp kullanılmadıęını sorgulama, dűzeltme, silme veya yok edilmesini talep etme haklarına sahiptir. Bu talepler decabilgiteknolojileri@hs03.kep.tr adresine KEP űzerinden veya sistemlerimizde kayıtlı info@decateknoloji.com e-posta adresi ile yazılı olarak iletilebilir. Bařvurular en geç 30 (otuz) gűn ierisinde űcretsiz olarak sonulandırılır.