

Creart Soft

Gizlilik, Çerez ve Bilgi Güvenliği Politikası

Yasal Dayanak, Kapsam ve Uyum İlkesi

İşbu doküman, Türkiye Cumhuriyeti mevzuatı esas alınarak hazırlanmıştır. Creart Soft tarafından sunulan her hizmetin hukuki niteliği; hizmetin türüne, müşterinin tüketici/tacir olup olmamasına, hizmetin yazılım geliştirme, SaaS, barındırma, lisans, domain, ödeme entegrasyonu, bakım-destek veya danışmanlık kapsamına göre değişebilir. Bu nedenle aşağıdaki mevzuat hükümleri, ilgili hizmet bakımından uygulanabildiği ölçüde dikkate alınır:

- 6098 sayılı Türk Borçlar Kanunu, 6102 sayılı Türk Ticaret Kanunu ve ilgili ikincil mevzuat.
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun ve Mesafeli Sözleşmeler Yönetmeliği; yalnızca tüketici işlemleri bakımından uygulanacak hükümler saklıdır.
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, Elektronik Ticarete Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik ve Ticari Elektronik İletiler mevzuatı.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu, ilgili Kurul kararları ve kişisel veri güvenliği rehberleri.
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve BTK düzenlemeleri; özellikle barındırma, yer sağlama, trafik/log kayıtları, hukuka aykırı içerik bildirim ve erişim/yer sağlayıcılığına temas eden hizmetlerde uygulanır.
- 5846 sayılı Fikir ve Sanat Eserleri Kanunu; yazılım, tasarım, arayüz, kod, dokümantasyon, logo ve sair fikri ürünler bakımından uygulanır.
- 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun; PayTR üzerinden yürütülen ödeme süreçleri bakımından dikkate alınır.
- Vergi Usul Kanunu, e-fatura/e-arşiv düzenlemeleri, elektronik defter ve saklama yükümlülükleri ile mali mevzuat hükümleri saklıdır.

Hizmetlerin niteliğine göre ilave mevzuat, kamu otoritesi kararları, mahkeme kararları, sektör düzenlemeleri, ödeme kuruluşu kuralları, açık kaynak lisansları ve üçüncü taraf servis şartları ayrıca uygulanabilir.

1. Amaç ve Kapsam

1.1. İşbu Gizlilik, Çerez ve Bilgi Güvenliği Politikası; Creart Soft web sitesi, müşteri paneli, destek sistemi, SaaS hizmetleri, yazılım projeleri, ödeme süreçleri, entegrasyonlar, demo/test ortamları ve iletişim kanalları kapsamında uygulanır.

1.2. Creart Soft, müşterilerin ve ziyaretçilerin gizliliğine önem verir; kişisel verileri yalnızca hukuka uygun, sınırlı, ölçülü ve belirli amaçlarla işler.

1.3. Müşteri tarafından proje, demo veya canlı sistemlere yüklenen ticari veri, kullanıcı verisi, içerik, belge ve veritabanı kayıtları müşterinin sorumluluğundadır. Creart Soft bu verilere ancak teknik destek, bakım, güvenlik, hata giderme veya yasal yükümlülük amacıyla sınırlı erişir.

2. Toplanan Bilgiler

2.1. Kimlik ve iletişim bilgileri: ad, soyad, unvan, e-posta, telefon, adres, vergi bilgileri, fatura bilgileri ve müşteri temsilcisi bilgileri.

2.2. Hesap ve işlem bilgileri: kullanıcı hesabı, sipariş, fatura, ödeme durumu, hizmet paketi, lisans durumu, destek talebi, proje aşaması, teslim ve kabul kayıtları.

2.3. Teknik bilgiler: IP adresi, cihaz bilgisi, tarayıcı bilgisi, oturum kaydı, hata kayıtları, güvenlik logları, API istekleri, işlem zamanı, erişim günlükleri, lisans doğrulama kayıtları ve sunucu logları.

2.4. Ödeme bilgileri: ödeme tutarı, ödeme yöntemi, işlem numarası, maskeleytirilmiş kart bilgisi, ödeme onayı, iade durumu ve PayTR/banka tarafından sağlanan işlem sonucu bilgileri. Kart numarası, CVV/CVC gibi hassas kart bilgileri Creart Soft sistemlerinde saklanmaz.

3. Verilerin Kullanım Amaçları

- 3.1. Hizmetlerin sunulması, sipariş ve üyelik süreçlerinin yönetilmesi, yazılım projesi planlama, geliştirme, test, teslim ve destek süreçlerinin yürütülmesi.
- 3.2. Ödeme alınması, fatura düzenlenmesi, muhasebe kayıtlarının tutulması, iade süreçlerinin yürütülmesi ve PayTR ödeme altyapısı ile işlem güvenliğinin sağlanması.
- 3.3. Lisans doğrulama, hizmet güvenliği, kötüye kullanımın önlenmesi, yetkisiz erişim tespiti, saldırı önleme, hata analizi, yedekleme ve sistem sürekliliğinin sağlanması.
- 3.4. Yasal taleplerin karşılanması, BTK/5651 kapsamında ilgili logların tutulması, KVKK başvurularının yönetilmesi ve yetkili makamlarla zorunlu paylaşım süreçlerinin yürütülmesi.

4. Çerezler ve Benzer Teknolojiler

- 4.1. Web sitesi ve müşteri panelinde oturum yönetimi, güvenlik, tercihlerin hatırlanması, performans ölçümü, hata tespiti ve analitik amaçlarla çerezler kullanılabilir.
- 4.2. Zorunlu çerezler, hizmetin çalışması için gereklidir. Analitik, pazarlama veya tercih çerezleri ise ilgili mevzuat ve rıza yönetimi çerçevesinde kullanılmalıdır.
- 4.3. Kullanıcılar tarayıcı ayarlarından çerezleri yönetebilir. Ancak zorunlu çerezlerin kapatılması halinde müşteri paneli, ödeme, oturum veya güvenlik fonksiyonları çalışmayabilir.

5. Üçüncü Taraflar ve PayTR

- 5.1. Ödeme işlemleri PayTR Ödeme ve Elektronik Para Kuruluşu A.Ş. altyapısı üzerinden yürütülebilir. Bu kapsamda ödeme tutarı, işlem kimliği, fatura bilgisi, iade bilgisi ve ödeme güvenliği için gerekli sınırlı bilgiler PayTR'ye aktarılabilir.
- 5.2. Creart Soft; e-fatura/e-arşiv, muhasebe, SMS, e-posta, barındırma, sunucu, CDN, yedekleme, hata takip, analitik, müşteri destek, proje yönetim, uygulama mağazası ve entegrasyon servislerinden yararlanabilir. Bu servislerle veri paylaşımı hizmetin ifası ve güvenlik amacıyla sınırlıdır.
- 5.3. Üçüncü taraf web siteleri, ödeme ekranları veya entegrasyon servisleri kendi gizlilik politikalarına tabidir. Kullanıcılar, ilgili üçüncü taraf politikalarını ayrıca incelemelidir.

6. Bilgi Güvenliği

- 6.1. Creart Soft; yetkilendirme, erişim kontrolü, şifreleme, güvenli bağlantı, güvenlik duvarı, yedekleme, loglama, güncelleme, zararlı yazılım önlemleri ve güvenli geliştirme uygulamaları dahil makul teknik ve idari tedbirleri uygular.
- 6.2. Müşteri; güçlü şifre kullanmak, iki aşamalı doğrulama varsa aktif etmek, erişim bilgilerini paylaşmamak, kullanıcı yetkilerini doğru tanımlamak, güncel tarayıcı/cihaz kullanmak ve kendi sistemlerinde güvenlik önlemleri almakla yükümlüdür.
- 6.3. E-posta ile gönderilen bilgilerin güvenliği her zaman garanti edilemeyebilir. Hassas erişim bilgileri mümkün olduğunca güvenli kanal, şifre yöneticisi veya süreli erişim yöntemi ile paylaşılmalıdır.

7. Saklama, Silme ve Yedekleme

- 7.1. Veriler; hizmetin devamı, sözleşme, fatura, destek, yasal yükümlülük, uyumsuzluk, güvenlik ve teknik gereklilik süreleri boyunca saklanır.
- 7.2. Hizmetin sona ermesi halinde müşteri verileri, ilgili hizmet türüne göre makul süre içinde silinebilir, anonim hale getirilebilir veya yasal saklama yükümlülükleri kapsamında muhafaza edilebilir.

7.3. Yedekler, teknik altyapı gereği canlı veriden farklı periyotlarda silinebilir. Yedeklerden geri dönüş talebi, hizmet paketinde belirtilmişse destek kapsamında; aksi halde ayrıca ücretli işlem olarak değerlendirilebilir.

8. Politika Değişiklikleri ve İletişim

8.1. Creart Soft, mevzuat, hizmet kapsamı, ödeme altyapısı, teknik altyapı veya iş süreçlerinde değişiklik olması halinde bu politikayı güncelleyebilir.

8.2. Güncel politika web sitesinde veya müşteri panelinde yayımlandığı anda yürürlüğe girer. Önemli değişiklikler için e-posta, panel bildiri veya duyuru kanalları kullanılabilir.

9. Çerez Kategorileri ve Kullanım Detayı

9.1. Zorunlu çerezler; oturum açma, güvenli ödeme yönlendirmesi, kullanıcı doğrulama, panel güvenliği, sepet/sipariş akışı ve tercihlerin teknik olarak çalışması için kullanılır.

9.2. Performans ve analitik çerezleri; sayfa yüklenme süreleri, hata oranları, kullanıcı deneyimi, ziyaret yoğunluğu ve sistem performansının ölçülmesi için kullanılabilir. Bu çerezler kişisel veri işliyorsa KVKK ve ilgili çerez rehberlerine göre rıza yönetimi yapılmalıdır.

9.3. Pazarlama çerezleri; reklam, yeniden hedefleme, kampanya ölçümü ve kullanıcı ilgi alanına göre içerik sunumu için kullanılabilir. Bu tür çerezler açık rıza gerektirebilir ve kullanıcıya reddetme imkanı verilmelidir.

9.4. Güvenlik çerezleri; sahtecilik önleme, bot tespiti, deneme sayısı sınırlandırma, oturum güvenliği ve yetkisiz erişim tespiti için kullanılabilir.

10. Veri İhlali, Olay Yönetimi ve Bildirim

10.1. Creart Soft, kişisel veri veya sistem güvenliği ihlali şüphesi halinde olayı teknik ve idari olarak inceleyebilir, erişimleri sınırlandırabilir, şifre sıfırlama yapabilir, ilgili servisleri geçici olarak durdurabilir ve gerekli kayıtları koruma altına alabilir.

10.2. KVKK kapsamında bildirim gerektiren bir veri ihlali oluşması halinde, yasal süreler ve Kurul kararları dikkate alınarak ilgili kişiler ve Kişisel Verileri Koruma Kurumu nezdinde gerekli değerlendirme yapılır.

10.3. Müşteri kaynaklı ihlallerde müşteri; kendi kullanıcılarını bilgilendirmek, otoritelerle iletişime geçmek, şifreleri değiştirmek, erişimleri kapatmak ve zararın büyümemesi için gerekli tedbirleri almakla yükümlüdür.

11. Müşteri Verileri, Demo Ortamları ve Test Verileri

11.1. Demo ve test ortamlarında gerçek kişisel veri yerine anonim, maskeleştirilmiş veya örnek veri kullanılması esastır. Müşteri gerçek kişisel veri ile test yapılmasını talep ederse bu verilerin hukuka uygun aktarımından sorumludur.

11.2. Müşteri, destek için gönderdiği ekran görüntülerinde kimlik, kart, sağlık, özel nitelikli veri veya gizli ticari bilgi bulunmamasına dikkat etmelidir. Gerekli hallerde bu verileri maskelemelidir.

11.3. Proje tamamlandıktan sonra test hesapları, geçici şifreler, demo erişimleri ve paylaşılmış API anahtarları kapatılmalı veya yenilenmelidir.

12. Kullanıcı Kontrolü ve Veri Taşınabilirliği

12.1. Müşteri, kendi hesabındaki temel bilgileri güncelleme, destek talebi oluşturma, fatura bilgilerini kontrol etme ve hizmet iptal talebi iletilme imkanına sahip olabilir.

12.2. Veri dışı aktarımı, yedek indirme veya kaynak/dokümantasyon teslimi ancak hizmet paketinde veya sözleşmede belirtilmişse ücretsizdir. Aksi halde teknik işlem ve işçilik bedeli ayrıca talep edilebilir.