Güvenlik ve Güven Merkezi

Parselo, arazi profesyonelleri ve mülk sahipleri için güvenli ve yerel öncelikli bir Coğrafi Bilgi Sistemleri (CBS) mimarisi sunar. Verilerinizin mahremiyeti ve sistem güvenliği temel tasarım ilkemizdir.

1. Temel Güvenlik ve Gizlilik Taahhütleri

Portföyünüz ve Aradığınız Parseller Bize Ait Değildir: Girdiğiniz künye ve yüklediğiniz sınır verileri, oluşturduğunuz analizler veya yüklediğiniz saha fotoğrafları ticari amaçla üçüncü taraflarla paylaşılmaz.

Yapay Zeka Eğitilmez: Parselo müşteri verilerini ve arama geçmişini yapay zeka modellerini eğitmek için kullanmaz ve bu amaçla hiçbir sağlayıcıya vermez. Kendi anahtarınızla kullandığınız yapay zeka sağlayıcısının gönderilen içeriği nasıl işlediği, o sağlayıcıyla aranızdaki hesap şartlarına tabidir.

Veri Satışı Yapılmaz: Parselo hiçbir koşulda kullanıcıların arama eğilimlerini, portföy büyüklüklerini veya iletişim bilgilerini veri simsarlarına satmaz.

Kripto-İmha: Pazarlama videoları ve geçici drone simülasyon render dosyaları teslim edildikten sonra sunucularımızdan otomatik olarak güvenli şekilde silinir.

2. Veri İşleme Mimarisi ve Akış Tablosu

Parselo, hesaplamaların büyük bölümünü doğrudan kullanıcının cihazında (istemci tarafı WebAssembly ve Canvas ile) çalıştırarak sunucuya giden veri miktarını en aza indirir.

Yerel Coğrafi Bilgi Sistemleri Motoru (İstemci): Eş yükselti hesaplamaları, eğim analizi ve 3B arazi morfolojisi doğrudan tarayıcınızda veya telefonunuzda işlenir.

Sunucu Tarafı (Bulut): Yalnızca girdiğiniz künye (il/ilçe/mahalle/ada/parsel) ve yüklediğiniz sınır ile şifreli oturum token'ı işlenir.

Harici Sağlayıcılar: Harita altlıkları ve Esri konum servisleri Parselo sunucusu üzerinden çağrılır; Esri anahtarı tarayıcıya gönderilmez. Lisanslı ödeme geçidi (PCI-DSS Seviye 1) bağımsız güvenli kanaldan çalışır.

3. Teknik ve Ağ Güvenliği Önlemleri

Uçtan Uca Şifreleme (TLS 1.3): Tüm veri aktarımı modern kriptografik şifreleme protokolleriyle korunur.

Katı Güvenlik Başlıkları: CSP (İçerik Güvenliği Politikası), HSTS ve XSS/CSRF koruma katmanları aktiftir.

DDoS ve İstemci Koruması: Dağıtık hizmet aksatma saldırılarına karşı akıllı CDN ve hız sınırlama katmanları uygulanır.

4. Sorumlu Zafiyet Bildirimi (Responsible Disclosure)

Parselo altyapısında güvenlik açığı tespit eden bağımsız araştırmacılar, detayları destek@parselo.com.tr adresine iletebilir. Bildirimler en geç 24 saat içinde güvenlik ekibimizce değerlendirmeye alınır.

Son güncelleme: 24 Eylül 2026