

TDV Yurtlar Portalı

GİZLİLİK POLİTİKASI

Hazırlanma tarihi: 08.10.2026 | Sürüm: 1.0 | Mobil uygulama

Yayın öncesi inceleme taslağı

Veri bazında hukuki sebepler, saklama süreleri ve hizmet sağlayıcıların aktarım koşulları kurum tarafından doğrulanmalıdır. Bu politika, faaliyet bazlı KVKK aydınlatma metinlerinin veya gerektiğinde alınacak açık rızanın yerine geçmez.

1. Kapsam ve sorumluluk

Veri sorumlusu: Türkiye Diyanet Vakfı Yurtlar İşletmesi

İletişim: info@tdvyurt.com.tr

Bu politika, TDV Yurtlar Portalı mobil uygulamasındaki öğrenci hesabı, yurt işlemleri, karekodla giriş/çıkış, bildirimler ve hizmet satın alma özellikleri kapsamında kişisel verilerin kullanımını açıklar. İşlenen veriler, kullanıcının yararlandığı hizmete ve kurum kayıtlarına göre değişebilir.

2. İşlenen veri kategorileri

Kimlik ve hesap: T.C. kimlik numarası, ad ve soyad, hesapla ilişkili iletişim ve öğrenci/yurt bilgileri; kurum kayıtlarında bulunan profil fotoğrafı.

Yurt işlemleri: Giriş/çıkış hareketleri, izin ve misafir başvuruları, mesajlar, talep/öneri/şikâyet ve arıza bildirimleri ile bunlara verilen yanıtlar.

Mali işlemler: Borç ve ödeme durumu, seçilen hizmetler ve aylar, tutar ve ödeme işlemine ilişkin sonuç/referans bilgileri.

Teknik veriler: Hesap-cihaz eşleştirmesinde kullanılan cihaz tanımlayıcısı, oturum bilgileri ve bildirim gönderim anahtarı (push token). QR işleminde kullanılan enlem ve boylam da sunucuya iletilir. İşletim ve güvenlik kayıtlarının kapsamı sunucu yapılandırmasına bağlıdır.

3. Verilerin elde edilmesi ve kullanım amaçları

Veriler, kullanıcının uygulamaya girdiği bilgilerden, kurumun öğrenci/yurt kayıtlarından, izin verilen cihaz özelliklerinden ve işlem sırasında oluşan kayıtlardan elde edilir. Hesaba erişim sağlamak, yurt hizmetlerini yürütmek, giriş/çıkış işlemini doğrulamak, başvuruları ve ödemeleri takip etmek, talepleri yanıtlamak, bildirim göndermek ve yetkisiz kullanımı önlemek için kullanılır. Serbest metin alanlarında işlem için gerekli olmayan sağlık bilgileri veya başka kişilerin özel bilgileri paylaşılmamalıdır.

İzinler ve veri paylaşımı

4. Kamera ve konum

Kamera: Karekodun okunması için kullanılır. İncelenen QR akışında kamera görüntüsünü fotoğraf/video olarak sunucuya yükleyen bir işlem bulunmamaktadır; okunan karekod bilgisi işleme alınır.

Konum: QR okutma sırasında cihazın konumu alınarak tanımlı yurt/cihaz konumuna uzaklığı kontrol edilir. Giriş/çıkış isteğiyle enlem ve boylam sunucuya gönderilir. İncelenen QR akışında sürekli arka plan konum takibi bulunmamaktadır.

Kamera veya konum izni verilmezse karekod işlemi tamamlanamayabilir. İzinler cihaz ayarlarından değiştirilebilir. Konum izni vermek, kişisel veri işleme için gereken hukuki dayanağın yerine geçmez.

5. Cihaz eşleştirmesi ve güvenlik kontrolleri

Bir cihazın farklı öğrenci hesaplarıyla kullanılmasını sınırlandırmak için cihaz tanımlayıcısı hesapla ilişkilendirilir. İncelenen Android akışında ANDROID_ID kullanılmaktadır; bu değer IMEI değildir. Cihaz tanımlayıcısının kalıcılığı işletim sistemi, imzalama ve cihaz sıfırlama koşullarına bağlıdır. Uygulamayı kaldırmak, sunucudaki hesap-cihaz eşleşmesini kendiliğinden silmez. Cihaz değişikliği veya hatalı eşleştirme için yurt yönetimine başvurulmalıdır. Sahte konum ve cihaz bütünlüğü kontrolleri QR kullanımını sınırlandırabilir; bu kontrollerin uygulanması platforma göre farklılık gösterebilir.

6. Bildirimler

Desteklenen ve yapılandırılmış sürümlerde bildirimler Google Firebase Cloud Messaging üzerinden iletilir. Bildirim anahtarı hesap/cihazla ilişkilendirilerek ilgili kullanıcıya bildirim gönderilmesini sağlar. Bildirim içeriği, cihaz ayarlarına bağlı olarak kilit ekranında görünebilir. Bildirimler işletim sistemi ayarlarından kapatılabilir. Uygulama içi mesaj veya duyuru kayıtları, bildirim izni kapalı olsa da kurum sisteminde tutulabilir.

7. Ödemeler ve dış bağlantılar

Hizmet satın alma akışında kullanıcı, ödeme sayfasına yönlendirilir veya uygulama içi web görünümünde ödeme yapar. Kart verileri ödeme sayfası ve ilgili ödeme kuruluşu/banka tarafından işlenir; portal tarafında hizmet siparişi ve ödeme sonucu gibi işlem kayıtları kullanılır. Kart verilerinin kim tarafından ve ne kadar süre saklandığı, kullanılan ödeme sağlayıcısı doğrulanarak ayrıca açıklanmalıdır. Sosyal medya ve diğer dış bağlantılarda ilgili hizmetin kendi gizlilik ve çerez politikaları geçerlidir.

8. Verilerin paylaşılması ve aktarılması

Veriler, görevleri ve yetkileri ölçüsünde ilgili yurt/kurum birimleriyle; teknik hizmetin gerektirdiği ölçüde barındırma, bakım, bildirim ve ödeme hizmet sağlayıcılarıyla ve hukuken gerekli durumlarda yetkili kamu kurumlarıyla paylaşılabilir. Firebase ve diğer dış hizmetlerde yurt dışı veri işleme veya aktarım söz konusu olabilir. Alıcılar, ülkeler ve uygulanacak aktarım mekanizması kurum tarafından teyit edilmelidir. Gerekli hukuki koşullar sağlanmadan aktarım yapılmamalıdır.

Saklama ve kullanıcı hakları

9. Hukuki sebepler

Her veri işleme faaliyeti için uygulanabilir hukuki sebep ayrı ayrı belirlenmelidir. Faaliyetin niteliğine göre sözleşmenin kurulması veya ifası, kanuni yükümlülük, bir hakkın tesisi/kullanılması/korunması, temel hak ve özgürlüklere zarar vermeyen meşru menfaat veya gerekli hâllerde açık rıza değerlendirilebilir. Bu sayılan sebepler tüm işlemlere topluca uygulanmaz. Veri kategorisi, amaç, alıcı ve hukuki sebep eşleştirmesi kurumun onaylı aydınlatma metinlerinde açıklanmalıdır.

10. Saklama, silme ve hesap işlemleri

Kişisel veriler yalnızca hizmetin gerektirdiği süre ve geçerli yasal saklama yükümlülükleri kapsamında tutulmalıdır. Öğrenci kayıtları, mali belgeler, hareket kayıtları, konum bilgileri, cihaz eşleştirmeleri ve bildirim anahtarları için süreler ayrı ayrı belirlenmelidir. Bu taslakta doğrulanmamış sayısal bir saklama süresi öngörülmemiştir. İşleme şartları sona erdiğinde veriler ilgili yükümlülükler gözetilerek silinmeli, yok edilmeli veya anonimleştirilmelidir. Çıkış yapmak veya uygulamayı kaldırmak, kurum kayıtlarını ve hesabı otomatik olarak silmez. Hesabın kapatılması ve silme talepleri kurumun resmî başvuru kanalından iletilmelidir.

11. Güvenlik ve kullanıcı tercihleri

Hesap erişimi, oturum bilgileri ve cihaz eşleştirmesi uygulamanın güvenlik mekanizmaları kapsamında kullanılır. Kişisel veri güvenliği için kurumun erişim yetkileri, sunucu güvenliği, kayıt yönetimi ve hizmet sağlayıcı tedbirleri ayrıca doğrulanmalıdır. Hiçbir sistem mutlak güvenlik garantisi vermez. Kullanıcı şifresini paylaşmamalı, ortak cihaz kullanımından kaçınmalı ve kayıp/çalıntı cihazı yurt yönetimine bildirmelidir. Kamera, konum ve bildirim izinleri cihaz ayarlarından yönetilebilir.

12. Kişisel verilere ilişkin haklar ve başvuru

Uygulanabilir mevzuat kapsamında kişisel verilerinizin işlenip işlenmediğini öğrenme, işlenmişse bilgi isteme, amaç ve amaca uygun kullanım hakkında bilgi alma, aktarım yapılan üçüncü kişileri öğrenme, eksik/yanlış verilerin düzeltilmesini isteme, şartları oluştuğunda silme veya yok etme talep etme ve bu işlemlerin alıcılara bildirilmesini isteme haklarınız bulunmaktadır. Münhasıran otomatik analiz nedeniyle aleyhinize doğan sonuçta itiraz edebilir ve hukuka aykırı işleme nedeniyle zararın giderilmesini talep edebilirsiniz.

Başvuru ve iletişim: Türkiye Diyanet Vakfı Yurtlar İşletmesi - info@tdvyurt.com.tr. Kişisel verilerinize ilişkin talepleriniz için bu adresten başvuru usulü hakkında bilgi alabilirsiniz. Başvuruların ilgili mevzuatta öngörülen yöntemlerle yapılması ve kimlik doğrulaması gerekebilir. E-posta ile şifre veya kart bilgisi göndermeyiniz.

13. Güncellemeler

Özellikler, hizmet sağlayıcılar veya veri işleme süreçleri değiştiğinde politika güncellenir. Güncel sürüm uygulamada ve kurumun yayınlayacağı erişilebilir gizlilik sayfasında sunulmalıdır. Bu belgenin hazırlanması, uygulama mağazası veri güvenliği beyanlarını veya kurumsal hukuki incelemeyi kendiliğinden tamamlamaz.

Hazırlık referansı: Kişisel Verileri Koruma Kurumu, "Aydınlatma Yükümlülüğü" ve 08.06.2020 tarihli kamuoyu duyurusu. www.kvkk.gov.tr/Icerik/2033/Aydınlatma-Yukumlulugu | www.kvkk.gov.tr/Icerik/6765