

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

UXR PLAYGROUND

1. BÖLÜM: POLİTİKANIN AMACI, DAYANAĞI VE KAPSAMI

1.1. Amaç ve Veri Sorumlusu

Bu Politika, UXR Playground markası altında faaliyet gösteren ONIT TEKNOLOJİ & YAZILIM LİMİTED ŞİRKETİ ("Şirket") tarafından, veri sorumlusu sıfatıyla hazırlanmıştır. Kişisel verilerin hangi esaslarla saklanacağını, saklama ihtiyacı sona erdiğinde nasıl imha edileceğini ve bu süreçlerin sorumlularını belirler.

Politikanın dayanağı 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun" veya "KVKK") ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir ("Yönetmelik"). Veri işleme amaçları, hukuki sebepleri ve alıcı grupları için KVKK Aydınlatma Metni; çerez süreçleri için Çerez Aydınlatma Metni birlikte değerlendirilir.

1.2. Kapsam ve Geçerlilik Alanı

Politika; web sitesi ziyaretleri, iletişim talepleri, kayıt, satın alma, ödeme ve iade, eğitim, atölye, etkinlik, dijital içerik, katılım ve sertifika, topluluk iletişimi ve etkinlik fotoğrafları kapsamında Şirketin işlediği kişisel verileri kapsar. Bu süreçlerde görev alan eğitmen, iş ortağı ve hizmet sağlayıcıların gerçek kişi iletişim bilgileri de kapsam içindedir.

2. BÖLÜM: TANIMLAR

Bu Politikada kullanılan temel kavramlar aşağıdaki anlamları taşır:

- Silme:** İşlenen kişisel verilerin, ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
- Yok Etme:** Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
- Anonim Hale Getirme:** Kişisel verilerin, başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.
- Kişisel Veri ve İlgili Kişi:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi kişisel veri; bu verinin ait olduğu gerçek kişi ilgili kişidir.
- Periyodik İmha:** Kişisel verilerin işleme şartlarının tamamı ortadan kalktığında, Politikada belirlenen aralıklarla resen yapılan silme, yok etme veya anonim hale getirme işlemidir.
- Kayıt Ortamı ve İlgili Kullanıcı:** Kişisel verilerin bulunduğu elektronik veya fiziki ortam kayıt ortamıdır. Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu kişi veya birim dışındaki, Şirketin yetki ve talimatıyla veri işleyen kişiler ilgili kullanıcıdır.

3. BÖLÜM: SAKLAMA VE KAYIT ORTAMLARI

Kişisel veriler, kullanılan hizmetin niteliğine göre aşağıdaki ortamlarda bulunabilir. Aynı verinin farklı ortamlardaki kopyaları da saklama ve imha değerlendirmesine dahil edilir.

A) Elektronik Ortamlar

- Google hizmetleri ve Airtable: İletişim yazışmaları, başvuru ve kayıt bilgileri, operasyon dosyaları, katılım ve hizmet süreçlerine ilişkin kayıtlar.
- Zoom ve web hizmetleri: Çevrim içi eğitim ve etkinliklerin yürütülmesi için kullanılan katılım bilgileri; web altyapısı, Google Analytics ve Meta Pixel kapsamında işlenen çevrim içi veriler. Eğitim ve etkinliklerde Şirket tarafından ses veya video kaydı alınmaz.
- Ödeme ve görsel içerik ortamları: izyico üzerinden yürütülen işlemlere ilişkin ödeme ve iade kayıtları ile Şirketin kontrolündeki fotoğraf dosyaları ve sosyal medya paylaşımları. Hizmet sağlayıcıların kendi yasal yükümlülükleri kapsamında tuttukları kayıtlar, Şirketin kontrolündeki kopyalardan ayrı değerlendirilir.

B) Elektronik Olmayan (Fiziki) Ortamlar

- Fiziki belge veya kişisel veri içeren çalışma materyali oluşması halinde bunlar da Politika kapsamındadır. Bu belgelerin yalnızca görev gereği erişmesi gereken kişilere açık tutulması ve saklama ihtiyacı sona erdiğinde uygun yöntemle imha edilmesi esastır.

4. BÖLÜM: SAKLAMA VE İMHAYI GEREKTİREN SEBEPLER

4.1. Saklamayı Gerektiren Hukuki ve Operasyonel Sebepler

Kişisel veriler, amaçla bağlantılı, sınırlı ve ölçülü olarak, ilgili veri için geçerli hukuki sebep ve gerekli süreyle saklanır:

- Hukuki yükümlülükler ve hakların korunması: Vergi, muhasebe, ticaret, tüketici ve ilgili diğer mevzuattan doğan belge saklama yükümlülükleri; sözleşmenin, ödemenin ve hizmet ifasının ispatı ile uyuşmazlıklarda hakların tesisi, kullanılması veya korunması.
- Sözleşme ve hizmet süreçleri: Kayıtların yönetimi, eğitim ve etkinliklerin sunulması, ödeme ve iadelerin yürütülmesi, katılım ve sertifika işlemleri ile ilgili taleplerin karşılanması.
- Diğer işleme şartları: Temel hak ve özgürlüklere zarar vermemek kaydıyla bilgi güvenliği ve gerekli operasyonel kontroller için meşru menfaat; açık rıza gerektiren faaliyetlerde ise ilgili amaca yönelik geçerli açık rıza. Bu dayanaklar birbirinin yerine kullanılmaz.

4.2. İmhayı Gerektiren Sebepler

Kanun'un 5 ve 6. maddelerindeki işleme şartlarının tamamı ortadan kalktığında, başvuru beklenmeksizin veya ilgili kişinin talebi üzerine imha yapılır. Bu kapsamda özellikle:

- Saklama amacı veya ilgili hukuki dayanağın sona ermesi ve veriyi tutmayı gerektiren başka bir işleme şartının bulunmaması,
- İlgili saklama süresinin dolması ve daha uzun saklamayı gerektiren somut bir hukuki yükümlülük veya uyuşmazlığın bulunmaması,

- İşlemenin yalnız açık rızaya dayandığı hallerde rızanın geri alınması veya ilgili kişi başvurusunun ya da Kurul kararının imhayı gerektirmesi dikkate alınır. Başka bir hukuki sebeple tutulması gereken kayıtlar, yalnızca o amaçla ve gerekli kapsamda saklanır.

5. BÖLÜM: TEKNİK VE İDARİ TEDBİRLER

Saklama ve imha süreçlerinin operasyonel takibini ilgili UXR Playground yetkilisi yürütür. Bu görev; sürelerin kontrolünü, ilgili sistemlerde işlemlerin yürütülmesini, hizmet sağlayıcılarla gerekli koordinasyonu ve işlem kayıtlarının tutulmasını kapsar. Şirket yönetimi uygulamanın gözetiminden; verilere erişen görevliler ise yetkileri içindeki işlemlerden sorumludur.

5.1. İdari Tedbirler

- Gizlilik ve amaçla sınırlılık: Kişisel verilere erişen kişiler, verileri yalnızca görevleri ve Şirketin talimatları kapsamında kullanmakla, yetkisiz kişilerle paylaşmamakla yükümlüdür. Dış hizmet ilişkilerinde veri erişiminin kapsamı ve gizlilik yükümlülükleri değerlendirilir.
- Farkındalık: Kişisel verilerin korunmasına ilişkin eğitimler alınmakta ve ihtiyaç doğrultusunda tekrarlanmaktadır.
- Yetkilendirme: Erişimin görev için gerekli veriyle sınırlandırılması, görev sona erdiğinde yetkilerin kaldırılması ve saklama süresi dolan kayıtların tespiti bu Politikanın uygulama esaslarıdır.

5.2. Teknik Tedbirler

- Hesap ve paylaşım güvenliği: Kişisel veri içeren hesapların ve paylaşım bağlantılarının erişim ayarları, görev ve ihtiyaç kapsamında kontrol edilir; yetkisiz erişimi önleyecek hesap güvenliği tedbirleri uygulanır.
- İmha güvenliği: İşlemden önce doğru veri, ortam ve kapsam belirlenir; ilgisiz kayıtların kaybı önlenir. Silinen verilerin yedek veya kopyalardan tekrar kullanıma alınmaması için ilgili ortamın silme ve erişim kontrolleri birlikte değerlendirilir.
- Hizmet sağlayıcılar: Şirket adına veri tutulan hizmetlerde, sağlayıcının sunduğu erişim ve silme işlevleri kullanılır; gerektiğinde silme talebi iletilir ve sonuç takip edilir. Şirketin kontrolündeki dışa aktarılmış kopyalar ayrıca işleme alınır.

6. BÖLÜM: KİŞİSEL VERİLERİN İMHA YÖNTEMLERİ

İmha yöntemi; verinin niteliği, bulunduğu ortam ve uygulanabilir teknik imkanlar dikkate alınarak seçilir. İlgili kişinin talebi üzerine seçilen yöntem gerekçesiyle açıklanır.

- Silme: Dijital kayıtlar ilgili uygulamadan silinir veya erişim ve kullanım yetkileri kaldırılarak ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz hale getirilir. Fiziki belgelerde gerektiğinde geri döndürülemeyen karartma uygulanır.
- Yok Etme: Fiziki belgeler okunamaz ve geri getirilemez biçimde parçalanır. Şirketin kontrolündeki dijital ortamlarda, ortamın niteliğine uygun güvenli silme veya fiziksel imha yöntemi kullanılır. Bulut hizmetlerinde sağlayıcının silme süreci takip edilir.

- Anonim Hale Getirme: Gerektiğinde istatistik ve değerlendirme sonuçları toplulaştırılır; doğrudan ve dolaylı tanımlayıcılar giderilerek başka verilerle eşleştirilse dahi kişinin belirlenememesi sağlanır. Yalnızca ad ve soyadın çıkarılması anonimleştirme için yeterli sayılmaz.

7. BÖLÜM: PERİYODİK İMHA VE SAKLAMA SÜRELERİ

Saklama süreleri; mevzuat, hizmetin niteliği, ispat ihtiyacı ve ölçülülük birlikte değerlendirilerek uygulanır. Aşağıdaki süreler bütün veri dosyasının gereksiz ayrıntılarıyla tutulması anlamına gelmez. Saklama amacı sona eren fazla veya mükerrer veriler ayklanır.

- Periyodik imha aralığı en fazla 6 aydır. İşleme şartlarının tamamı ortadan kalkan dijital kayıtlar, saklama süreleri ve hukuki saklama istisnaları kontrol edilerek takip eden ilk periyodik imhada otomatik olarak silinir. Fiziki kayıtlar ve otomatik silmenin uygulanamadığı ortamlardaki veriler, aynı süre içinde yetkili kişilerce silinir, yok edilir veya anonim hale getirilir. İşlemlerin tamamlanması ve istisnalar operasyon sorumlusu tarafından takip edilir. İlgili kişi başvuruları bu takvim beklenmeden yasal süre içinde sonuçlandırılır. İmha işlemleri kayıt altına alınır; işlem kayıtları en az 3 yıl saklanır.

Saklama ve İmha Süreleri:

Somut bir dava, inceleme, talep veya başka bir kanuni saklama yükümlülüğü varsa yalnızca bunun için gerekli kayıtlar, ilgili süreç ve uygulanabilir süreler tamamlanıncaya kadar erişimi sınırlandırılarak tutulur.

Aşağıdaki tabloda hukuki saklama zorunluluğu bulunmayan süreçler için belirtilen süreler, Şirketin amaç ve ihtiyaçla sınırlı azami saklama süreleridir. Daha erken sona eren işleme amacı veya geri alınan rıza ayrıca değerlendirilir.

Süre sonunda başka bir işleme şartı bulunmuyorsa ilk periyodik imhada işlem yapılır. Kişinin silme veya yok etme talebi varsa 8. bölümdeki süre uygulanır.

Kayıt / süreç	Saklama süresi ve başlangıcı
Fatura, muhasebe ve ticari işlem belgeleri	İlgili belgenin oluştuğu takvim yılının bitiminden itibaren 10 yıl; özel mevzuatta daha uzun süre öngörülmüşse o süre.
Sözleşme, kayıt, ödeme/iade ve hizmetin ifasını kanıtlayan asgari katılım/sertifika kayıtları	Hizmet ilişkisinin sona ermesinden itibaren 10 yıl; yalnız sözleşmenin ve ifanın ispatı ile hakların korunması için gerekli kayıtlar. Ticari belge niteliğindeki verilerde ilgili yasal başlangıç esas alınır.
Satışa dönüşmeyen iletişim ve bilgi talepleri	Talebin sonuçlanmasından veya son iletişimden itibaren en fazla 2 yıl.
Eğitim/etkinlik çalışma dosyaları ve kişisel veri içeren geri bildirimler	Programın tamamlanmasından itibaren en fazla 1 yıl; ispat için gerekli asgari kayıtlar ayrı tutulur. Kişisel veri içermeyen anonim sonuçlar bu sınıra tabi değildir.

Kayıt / süreç	Saklama süresi ve başlangıcı
Etkinlik fotoğrafları ve tanıtım amaçlı görseller	İlgili tanıtım amacı ve geçerli işleme şartı devam ettiği sürece, çekimden itibaren en fazla 2 yıl. Yalnız açık rızaya dayanan kullanımda rızanın geri alınması ayrıca değerlendirilir.
Bülten/topluluk iletişimi ve ticari elektronik ileti kayıtları	İletişim için kullanılan bilgiler geçerli izin/işleme şartı süresince; ticari ileti onay kayıtları onayın sona ermesinden, diğer ticari ileti kayıtları kayıt tarihinden itibaren 3 yıl. Ret sonrası bu kayıtlar yeni gönderim amacıyla kullanılmaz.
Web sitesi, çerez ve çevrim içi ölçüm verileri	Çerez Aydınlatma Metni'nde açıklanan süre ve esaslar; Şirketin ayrıca tuttuğu teknik erişim/güvenlik kayıtlarında kayıt tarihinden itibaren en fazla 1 yıl. Aynı yasal saklama yükümlülükleri saklıdır.
KVKK başvuru ve cevap kayıtları	Başvurunun sonuçlandırılmasından itibaren 3 yıl; devam eden inceleme veya uyuşmazlıkta gerekli kayıtlar süreç ve ilgili hukuki süreler tamamlanıncaya kadar.
İmha işlem kayıtları	İşlem tarihinden itibaren en az 3 yıl; daha uzun saklama gerektiren başka bir hukuki yükümlülük yoksa bu sürenin sonunda ilk periyodik imha.

8. BÖLÜM: BAŞVURULAR VE POLİTİKANIN UYGULANMASI

İlgili kişiler, KVKK kapsamındaki taleplerini hello@uxrplayground.com üzerinden iletebilir; usul ve diğer başvuru yolları için sitedeki KVKK Başvuru Formu'ndan yararlanabilir. Yazılı başvuru adresi: Çınar Mahallesi Yeşiltepe Sokak, Nidapark Küçükyaşı / Kınalı Etabı, A2/50, Maltepe/İstanbul. Başvurularda mevzuattaki kimlik ve başvuru koşulları uygulanır.

Silme veya yok etme talepleri en geç 30 gün içinde sonuçlandırılır ve başvuru sahibine bilgi verilir. İşleme şartları sürüyorsa ret gerekçesi açıklanır. Talep kabul edildiğinde, verilerin aktarıldığı üçüncü kişilere gerekli bildirim yapılarak Yönetmelik kapsamındaki işlemlerin yapılması temin edilir. Politika ihlallerinde erişimin sınırlandırılması, sözleşmesel ve hukuki tedbirler değerlendirilir; Şirketin sorumlulara karşı kanundan ve sözleşmeden doğan talep ve rücu hakları saklıdır.

9. BÖLÜM: YÜRÜRLÜK VE GÜNCELLEME

Politika, Şirket yönetimince onaylanarak yayımlandığında yürürlüğe girer. Mevzuat, kullanılan hizmetler veya veri işleme süreçleri değiştiğinde gözden geçirilir; sürüm ve değişiklik kayıtları saklanır. Güncel metin UXR Playground internet sitesinde yayımlanır. Emredici mevzuat hükümleri saklıdır.