

AI Eğitim/Log Verisi Anonim/Pseudo & Maskeleye Planlama Şablonu — Yazılım / AI KVKK (v1.0)

Asset Amaç: Bu şablon, yapay zeka (AI/ML) modellerinin eğitim verisinde ve model çalıştırma/izleme (*logging*) süreçlerinde kişisel veri (PII) ihlali risklerini sistematik olarak azaltmak için alan bazlı bir dönüşüm planı sunar. Loglar, web formları ve CRM sistemlerinden gelen veri alanlarını sınıflandırarak silme (*drop*), maskeleye (*mask*), takma adlandırma (*pseudo-ID*) veya toplulaştırma (*aggregate*) kararlarını standardize eder. Otel ve B2B senaryolarında makine öğrenimi süreçlerine hızlıca entegre edilebilir teknik bir gizlilik dönüşüm (*privacy transform*) mimarisi sağlar.

Kim Kullanır?: Veri / ML Ekipleri, Platform / Altyapı Mimarları ve KVKK / Uyum Sorumluları.

Nasıl Kullanılır?

- Model eğitimi veya izleme için kullanılacak veri kaynaklarını ve veri alanlarını (*log, form, CRM vb.*) çıkararak envantere alın.
- Her alan için risk durumuna göre teknik dönüştürme aksiyonunu (*Drop / Mask / Pseudo-ID / Toplulaştır*) belirleyin.
- Model çıktı izleme (*logging*) şemasını PII verilerden tamamen arındırılmış biçimde tasarlayın; TTL, örnekleme (*sampling*) ve denetim kurallarını aktif edin.

TEMPLATE — AI Eğitim & Log Verisi Gizlilik Planlama Şablonu

A) Kaynak ve Alan Envanteri

Kaynak Sistem (Log / Form / CRM / Feedback)	Veri Alanı	Risk Tipi (PII / Serbest Metin / Tanımlayıcı)	AI Kullanım Amacı (Feature / Monitoring / Debug)	Uygulanacak Aksiyon (Drop / Mask / Pseudo / Toplulaştır)	Notlar / Dönüşüm Mantiğı
Müşteri Formu	TCKN / Pasaport No	Doğrudan Tanımlayıcı (PII)	Kullanılmıyor	[] Drop	Eğitim setinden tamamen çıkarılmalı
Resepsiyon Logu	Müşteri Ad-Soyad	Doğrudan Tanımlayıcı (PII)	Debug / İzleme	[] Mask	A*** K*** şeklinde maskeleye

CRM Veritabanı	Müşteri ID / E-posta	Dolaylı Tanımlayıcı	Feature Eng. / Seg.	☐ Pseudo-ID	Hash (SHA-256) + Salt ile takma ad
Konaklama / Harcama	Harcama Tutar & Tarih	Davranışsal Veri	Model Eğitimi	☐ Toplulaştır	Günlük/Aylık ortalama segmente dönüştürme
Chatbot / Destek	Serbest Metin (Prompt)	Yüksek PII Riski (Serbest metin)	Model Eğitimi / Fine-Tuning	☐ PII Redaction	Otomatik Regex/NER süzgeciyle maskeleyme

B) Privacy Transform (Gizlilik Dönüşüm) Kuralları (v1.0)

- Drop (Tamamen Çıkarılacak) Listesi: _____ (Örn: TCKN, Pasaport, Kredi Kartı, Tam Açık Adres)
- Mask (Maskelenecek) Listesi: _____ (Örn: Telefon +90 532 *** ** 12, E-posta a***@gmail.com)
- Pseudo-ID (Takma Adlaştırma) Yaklaşımı: _____ (HMAC-SHA256 anahtarlama mimarisi; tuzlama/salt kullanımı)
- Toplulaştırma (Aggregation) Kurgusu:
 - Tarih: Kesin zaman damgası yerine [Yıl-Ay] veya [Haftanın Günü] olarak ölçekleme.
 - Lokasyon: İlçe/Sokak bilgisi yerine [İl] veya [Bölge] seviyesine genelleştirme.

C) Model Logging (İzleme) Şeması

- Loglanacak Model Alanları: _____ (Prompt tokens, Model ID, Latency, Confidence Score, Feature Vectors)
- PII Redaction (Anlık Maskeleyme Filter): ☐ Evet (Aktif) | ☐ Hayır
- Sampling (Örnekleme) Oranı: % _____ (Debug/Monitoring için üretilen logların saklanma oranı, Örn: %5)
- TTL / Retention (Saklama Süresi): _____ Gün (Model loglarının otomatik silinme periyodu, Örn: 30 gün)
- Erişim Roller (RBAC): _____ (Sadece yetkili ML/Platform mühendisleri)
- Audit Trail (Erişim & Sorgu Kaydı): ☐ Evet | ☐ Hayır (Log veritabanına atılan tüm sorguların kullanıcı bazlı kaydı)

D) Kontrol Listesi (Checklist)

- [] **Eğitim Setinde PII Arındırma:** Eğitim verisindeki tüm doğrudan ve dolaylı PII alanları drop edildi veya maskelendi.
- [] **İzole Pseudo-ID Eşleşme Tablosu:** Pseudo-ID dönüşüm haritası (*mapping table*) ana veritabanından tamamen ayrı, kilitli ve yetkili erişimli bir ortamda tutuluyor.
- [] **PII-Free Model Logging:** Modelin canlı ortamdaki girdi/çıkış loglarında PII bulunmuyor; PII Redaction filtresi aktif.
- [] **TTL & Sampling Yapılandırması:** Log veritabanı için zaman aşımı (TTL) ve sampling kuralları teknik olarak konfigüre edildi.
- [] **Export & Erişim Denetimi:** Eğitim seti indirmeleri, log dışı aktarımları ve erişimler silinemez audit sunucusuna kaydediliyor.
- [] **180 Günlük Periyodik Yenileme Planı:** AI veri işleme süreçleri ve gizlilik maskeleye kuralları 6 ayda bir gözden geçiriliyor.

Deliverables (Teslim Edilecek Çıktılar)

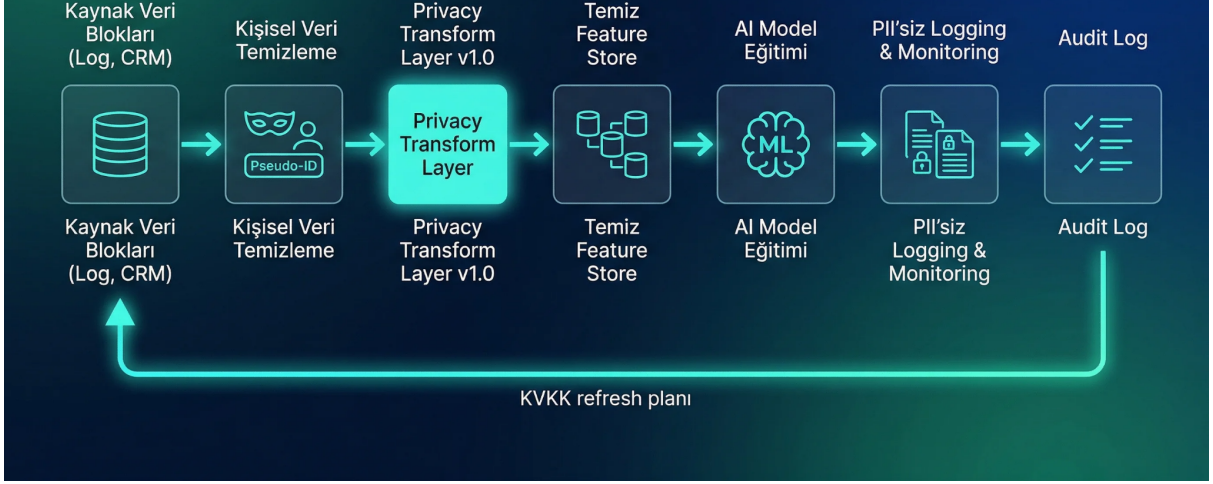
- **AI Data Classification & Privacy Transform Matrisi (v1.0):** Model eğitimi öncesi veri arındırma ve maskeleye kuralları rehberi.
- **Pseudo-ID & Salt Management Mimarisi:** Güvenli takma adlaştırma ve erişimi izole eşleşme veritabanı standartları dokümanı.
- **PII-Redacted Model Logging & Monitoring Şeması:** Canlı AI modellerinde kişisel veri sızdırmayan log altyapısı kılavuzu.
- **AI Veri Yönetişimi 180 Günlük Audit & Refresh Takvimi:** Periyodik veri kümesi denetim ve temizlik takvimi.



[Checklist / Framework Card]

AI/ML mühendisleri, veri mimarları ve KVKK uyum sorumluları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir AI Veri Hazırlık & Privacy Checklist Kartı. Koyu karbon gri zemin üzerine yerleştirilmiş; yapay zeka nöron ağı simgeleri, kilitli veri kalkanı, PII maskeleye gözü ve TTL zamanlayıcısı. Kartın üzerinde; "AI Training Set Privacy Transform: Drop, Mask & Pseudo-ID", "Isolated Salt/Mapping DB for Pseudo-Identifiers", "PII-Free Live Model Logging with Active Redaction", ve "Retention Control: Strict TTL, Sampling & 180-Day Refresh" teslimat kalemi başlıkları, yanlarında yeşil onay rozetleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.

KVKK UYUMLU AI EĞİTİM PIPELINE DİYAGRAMI



[Diagram / Flow]

Ham veri kaynaklarından (Log, Form, CRM) başlayıp KVKK Privacy Transform katmanına (Drop/Mask/Pseudo/Aggregate), oradan PII'siz temiz eğitim veri kümesine (Training Dataset), AI Model Eğitime ve PII-Redacted Model Logging/Monitoring hattına uzanan 16:9 formatında yüksek çözünürlüklü bir AI Pipeline Mimarisi Diyagramı. Koyu şık zemin üzerinde; mor, mavi ve yeşil veri akış hatları, Regex/NER filtreleme düğümleri, izole Pseudo-ID kasası ve kilitli denetim izi (Audit Trail) simgeleri profesyonel bir sistem şeması olarak sergileniyor.