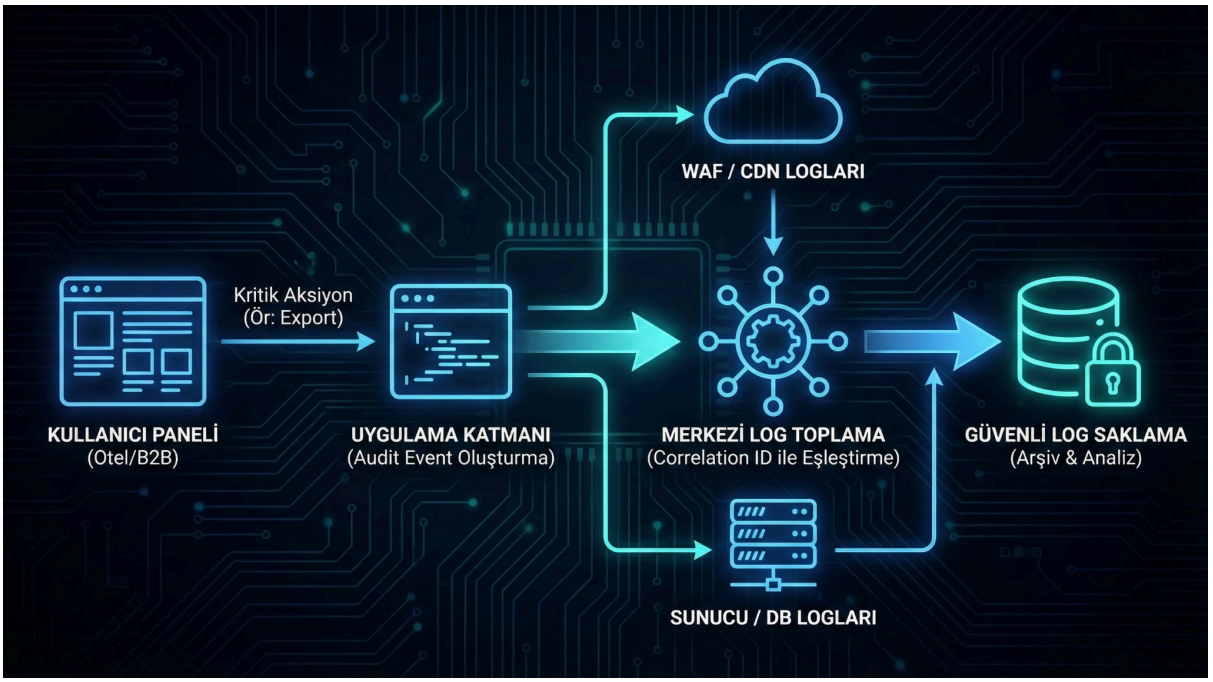
# Erişim & Loglama KVKK Teknik Tedbir Checklist’i (v1.0)

**Asset Amacı:** Panel ve sunucu katmanındaki RBAC (Rol Tabanlı Erişim Kontrolü) ve loglama kurgusunu tek bir standart checklist’e indirger. "Kim, ne zaman, hangi veriye erişti?" sorusuna yanıt verecek audit (denetim) kapsamını belirler; log güvenliği ve saklama (retention) adımlarını planlar. Özellikle otel ve B2B kurumlarda KVKK uyumu, denetime hazırlık ve ihlal analiz hızını artırmayı hedefler.

**Kim Kullanır?:** IT/Yazılım ekipleri, operasyon yöneticileri ve otel/B2B projelerinden sorumlu ajans teknik liderleri.




## Nasıl Kullanılır? (3 Adım)

1. **Matris Oluşturma:** Rol-yetki matrisini doldurarak ekran ve aksiyon bazlı (View/Edit/Export) izinleri netleştirin.
2. **Kapsam Belirleme:** Audit kapsamını seçin; özellikle login hareketleri, yetki değişimleri ve kritik veri görüntülemelerini (view) dahil edin.
3. **Güvenlik Sprinti:** Veri maskeleme (masking), log bütünlüğü ve erişim kısıtlamalarını 14 günlük plana bağlayarak yayına alın.

## Ölçüm & Önceliklendirme Checklist’i

- [ ] **RBAC Tanımı:** Rol setleri (Admin/Editör/Operatör/Viewer) net olarak tanımlandı mı?
- [ ] **Aksiyon İzinleri:** Ekran bazlı "Görüntüleme/Düzenleme/Silme/Dışa Aktarma" izinleri ayrıştırıldı mı?
- [ ] **Export Kontrolü:** Veri dışa aktarma (Export) izinleri tüm roller için varsayılan olarak kapalı mı?
- [ ] **Audit Kaydı:** Yetki değişiklikleri ve login (başarı/başarısızlık) hareketleri loglanıyor mu?
- [ ] **View Loglama:** Kritik müşteri verilerinin görüntülendiği ekranlarda "View" aksiyonu kayıt altına alınıyor mu?
- [ ] **Değişim İzleme:** Değişiklik loglarında "Eski Veri → Yeni Veri" (Diff) farkı tutuluyor mu?
- [ ] **Maskeleme:** Hata loglarında ve sistem çıktılarında PII (Kişisel Veri) maskeleme yapılıyor mu?
- [ ] **Log Güvenliği:** Log erişimi RBAC ile sınırlı mı ve log bütünlüğü (değiştirilemezlik) korunuyor mu?

## Problem → Kök Neden → Çözüm Tablosu

| Problem | Kök Neden | Çözüm |
|---|---|---|
| **Viewer veri dışa aktarabiliyor** | Export izni ayrı bir yetki değil | Export iznini role ayır + Audit zorunluluğu getir |
| **Hata loglarında PII görünüyor** | Payload loglama filtresiz açık | Masking + Log seviyeleri + Test süreci |
| **"Kim yaptı" bulunamıyor** | View logları ve Correlation ID yok | Audit event şeması + Correlation ID zorunluluğu |

## 14 Günlük Teknik Tedbir Sprint Planı

- **Gün 1–4:** Kritik ekranların listelenmesi, rol-yetki matrisinin oluşturulması ve Export izinlerinin kapatılması.
- **Gün 5–8:** Login ve yetki değişikliği audit kayıtlarının merkezi sisteme bağlanması; hata loglarında masking (maskeleme) uygulaması.

- **Gün 9–12:** Log saklama (retention) politikalarının aktifi edilmesi, WAF/CDN log akışının sağlanması ve Correlation ID entegrasyonu.
- **Gün 13–14:** Log yedekleme/bütünlük (immutability) kontrolü ve 365 günlük refresh (yenileme) planının raporlanması.


## Öncesi/Sonrası KPI Tablosu

| KPI | Önce | Sonra |
|---|---|---|
| **Incident Analiz Süresi** | Saatler | Dakikalar |
| **Audit Kapsam Oranı** | % Belirsiz | %100 Kritik Aksiyon |
| **PII Masking Oranı** | Düşük | Tam Uygulama |
| **Log Erişimi Yetkili Sayısı** | Dağınık | Kısıtlı & Denetimli |

## Deliverables (Teslim Edilecekler)

- Final Rol-Yetki Matrisi.
- Log Aksiyon Kapsam Tablosu.
- Panel + Sunucu Log Akış Diyagramı.
- Retention & Masking Uygulama Notları.
- Kapanış Raporu Şablonu.