Mobil Uygulama + WebView Veri Haritası & KVKK Checklist Şablonu — Yazılım / Mobile Hybrid (v1.0)

Asset Amaç: Bu asset, mobil uygulama (native app) ve WebView hibrit yapılarda toplanan verileri tek bir veri haritasında birleştirmenizi sağlar. Kullanıcı izin türleri, çerezler, device_id, push_token gibi teknik tanımlayıcılar (*identifiers*) ve backend erişim logları için kontrol noktalarını standardize eder. Mobil, web ve altyapı ekipleri için ortak bir teknik çalışma ve KVKK uyum zemini sunar.

Kim Kullanır?: Mobil Uygulama Ekibi, Web Geliştirme Ekibi, Backend/IT Ekibi ve Ürün/Operasyon Yöneticileri (Otel ve B2B Sektörleri).

Nasıl Kullanılır?

1. Mobil uygulama içerisinde WebView formatında açılan web sayfalarını (rezervasyon, ödeme, portal vb.) ve native app SDK'larını eksiksiz envantere işleyin.
2. İzin/consent olaylarını (*events*) ve tüm teknik tanımlayıcıları (device_id, push_token, web_cookie_id) veri haritasına bağlayın.
3. Arka plan log/audit ve veri saklama (*retention*) kurallarını tanımlayarak 14 günlük sprint planı çerçevesinde projeye entegre edin.

TEMPLATE — Mobil + WebView Veri Haritası & KVKK Denetim Matrisi

1) Ölçüm & Önceliklendirme Checklist'i

Hibrit mobil mimarilerde veri güvenliği, KVKK uyumu ve teknik entegrasyonu doğrulayan denetim listesi:

- [ ] **WebView Sayfa Envanteri Çıkarıldı:** Mobil uygulama içinden çağrılan tüm web sayfaları (Örn: Rezervasyon adımları, ödeme ekranı, kullanıcı profili) tespit edildi mi?
- [ ] **Native App SDK Envanteri Tanımlandı:** Uygulama içinde çalışan üçüncü taraf SDK'lar (Analitik, crash raporlama, push bildirim, pazarlama araçları) listelendi mi?
- [ ] **WebView Etiket/Çerez Tespiti Yapıldı:** WebView içinde yüklenen web sayfalarındaki tüm takip çerezleri ve script etiketleri (GTM/Pixel) haritalandı mı?
- [ ] **CMP / Consent Mekanizması Entegre Edildi:** Rıza Yönetim Platformu'nun (CMP) WebView ekranlarında sorunsuz çalıştığı doğrulandı mı?
- [ ] **Consent Sonrası Tetikleme Mekanizması Kuruldu:** WebView içindeki pazarlama ve analitik etiketlerinin yalnızca kullanıcı çerez izni verdikten sonra tetiklenmesi sağlandı mı?
- [ ] **ID Sözlüğü Hazırlandı:** Sistem genelindeki teknik kimlikler (app_user_id, device_id, push_token, web_cookie_id, session_id) standart tanımlara bağlandı mı?
- [ ] **App–WebView ID Eşleme Kuralları Sınırlandırıldı:** Kullanıcı takibi için native taraf ile web tarafındaki kimlik birleştirme kuralları yalnızca hukuki dayanak ve veri minimizasyonu sınırında tutuldu mu?
- [ ] **Push Token & İzin Event'leri Kayıt Altına Alındı:** Push bildirim izin değişiklikleri ve token oluşturma/yenileme olayları tarih ve izin durumuyla loglanıyor mu?

- [ ] **Backend Erişim ve Hata Logları Maskelendi:** Sunucu tarafındaki erişim ve hata kayıtlarında yer alan hassas veriler (şifre, kart no, T.C. No vb.) otomatik olarak maskeleniyor mu?
- [ ] **Log Saklama ve Erişim Yetkileri (RBAC & Retention):** Loglara erişim Rol Bazlı Erişim Kontrolü (RBAC) ile kısıtlandı ve veri imha/retention periyotları belirlendi mi?
- [ ] **App Store & Google Play Gizlilik Beyanı Hizalandı:** Mağaza panellerindeki kişisel veri ve takip bildirimleri (*Privacy Nutrition Labels*) uygulamadaki gerçek veri akışıyla birebir eşleştirildi mi?

2) Problem $\rightarrow$ Kök Neden $\rightarrow$ Çözüm Matrisi

Hibrit mobil uygulamalarda sık karşılaşılan veri sızıntısı/uyum sorunları ve teknik çözüm adımları:

Problem	**Kök Neden**	**Çözüm**
WebView'de reklam/analitik etiketleri kullanıcı onayı (*consent*) öncesinde tetikleniyor	Web tarafındaki CMP ve GTM izin kurallarının WebView ortamında özel olarak test edilmemiş olması	Mobil CMP sinyali entegrasyonu + Consent sonrası GTM tetikleme mimarisi + Ağ (*network*) testi
App ve Web katmanlarında aynı kullanıcı farklı kimliklerle (ID) kontrolsüz şekilde birleşiyor	Ortak bir ID sözlüğünün ve açık bir eşleme (*mapping*) kuralının bulunmaması	Bütünleşik ID sözlüğü oluşturulması + Minimum veri eşleme prensibi + Teknik dökümantasyon
Push bildirimlerinde (Push Notification) kilit ekranda kişisel veya hassas veri görünüyor	Bildirim içeriğinin cihaz kilit ekranına düşeceği düşünülmeden jenerik tasarlanması	Kilit ekranda genel bilgilendirme metni gösterimi + Detaylı içeriğin uygulama içine taşınması

3) 14 Günlük Hibrit Entegrasyon Sprint Planı

- **Gün 1: Sayfa & SDK Envanter Tespiti:** Mobil uygulama içinde açılan tüm WebView adresleri ile native katmanda kullanılan tüm SDK'lar (Crashlytics, Firebase, OneSignal vb.) haritalandırılır.
- **Gün 2: WebView Çerez & Etiket Analizi:** WebView sayfalarında yüklenen tüm çerezler ve JavaScript etiketleri tespit edilerek veri işleme amaçları çıkarılır.
- **Gün 3: CMP / Consent Davranış Doğrulaması:** Mobil arayüzden WebView katmanına rıza sinyallerinin (*consent state*) doğru aktarıldığı kontrol edilir.

- **Gün 4: Consent Sonrası Tetikleme Mimarisi:** İzin verilmeyen durumlarda WebView içi etiketlerin çalışmasını engelleyen GTM tetikleme kuralları yapılandırılır.
- **Gün 5: ID Sözlüğü ve Eşleme Kuralları:** app_user_id, device_id ve web_cookie_id arasındaki ilişkinin sınırları çizilir, dokümante edilir.
- **Gün 6: Push Token & İzin Event Tasarımı:** Kullanıcının bildirim izni verme/kaldırma eylemlerini ve token güncellemelerini takip eden veri şeması kurgulanır.
- **Gün 7: Backend Log Kapsamı & Maskeleme:** Sunucu seviyesindeki veri akışlarında kişisel verilerin maskelenmesi (*data anonymization/masking*) sağlanır.
- **Gün 8: Retention & Rotation Tasarımı:** Log verilerinin ve süresi dolan push token'larının veri tabanından otomatik temizlenme periyotları tanımlanır.
- **Gün 9: Aydınlatma Metni Tutarlılık Denetimi:** Mobil uygulama içi aydınlatma metinleri ile WebView formlarındaki metinlerin hukuki tutarlılığı kontrol edilir.
- **Gün 10: Mağaza Gizlilik Beyanı Hizalaması:** iOS App Store ve Android Google Play panellerindeki veri beyanları uygulamadaki teknik haritayla eşleştirilir.
- **Gün 11: Çoklu İşletim Sistemi QA Testleri:** Farklı iOS ve Android sürümlerinde WebView izin mekanizmaları ve veri akışları test edilir.
- **Gün 12: Performans ve Uyum KPI Ölçümü:** Başlangıç seviyesi izin kabul oranları ve etiket çalışma doğruluk yüzdeleri kaydedilir.
- **Gün 13: Canlıya Alma (Publish) & İzleme:** Yeni hibrit veri mimarisi uygulama güncellenerek canlıya alınır ve log akışları denetlenir.
- **Gün 14: Kapanış Raporu & Yıllık Yenileme Planı:** Sprint çıktıları dökümante edilir ve 365 günlük periyodik kontrol takvimi kilitlenir.

4) Öncesi / Sonrası Operasyonel KPI Tablosu

Mobil + WebView veri haritalama ve KVKK iyileştirmelerinin teknik performans çıktıları:

KPI Metriği	**Önce (Eski Durum)**	**Sonra (Hibrit Uyum Hedefi)**	**Stratejik Açıklama**
İzin kabul oranı (Push / Konum)	Düşük / Bilinmiyor	↑ **Artar** *(Şeffaf İletişim)*	Doğru zamanda ve şeffaf gerekçelerle istenen izinlerde kabul oranları yükselir.
WebView consent uyumu (Tag firing)	%0 – %40 (Kontrolsüz tetiklenme)	**%100** *(Tam Uyum)*	Çerez izni alınmadan hiçbir analitik veya reklam etiketi WebView'de çalışmaz.

SDK / Vendor sayısı	Yüksek (Gereksiz/Atıl SDK'lar)	↓ **Düşer** *(Minimizasyon)*	Kullanılmayan üçüncü taraf SDK'lar kaldırılarak uygulama boyutu ve güvenlik riski azaltılır.
Log denetlenebilirlik kapsama oranı	Kısmi / Düzensiz	**%100** *(Tam Audit)*	Tüm erişim, işlem ve izin değişiklikleri RBAC kısıtlı ve maskeli olarak loglanır.
Şikâyet / İtiraz sayısı	Yüksek (İzinsiz push/takip riski)	↓ **Düşer** *(Açık Rıza)*	Bildirim ve veri işleme süreçleri kontrol altına alındığı için kullanıcı itirazları düşer.

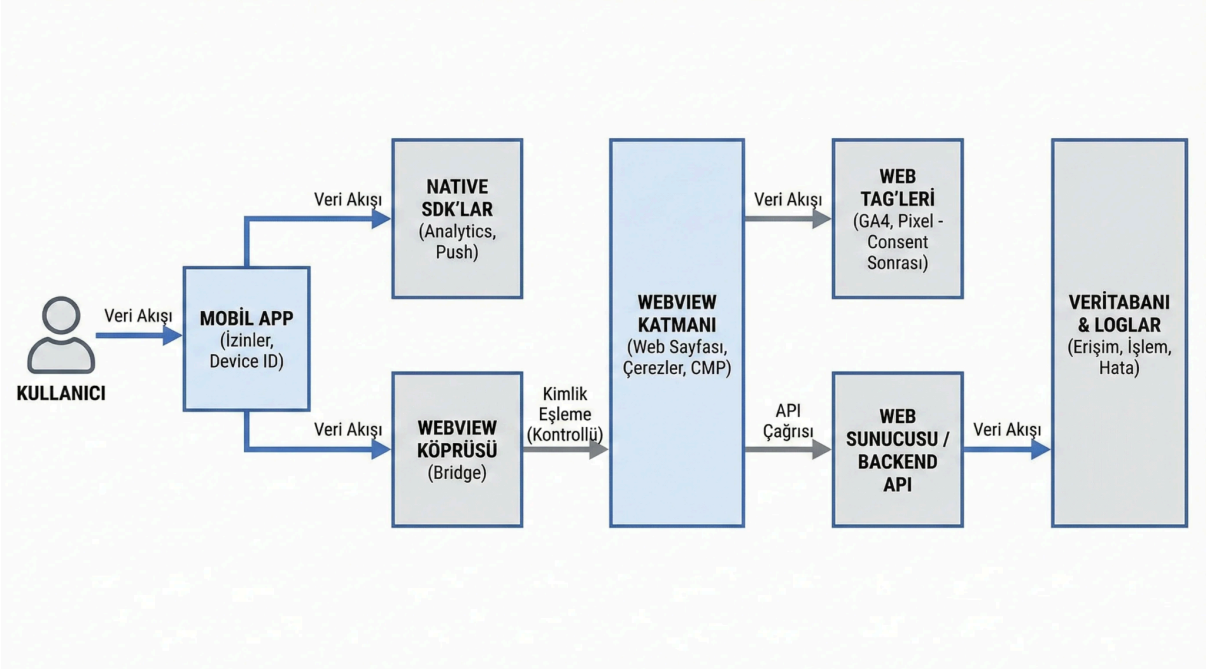
5) Nasıl Uygulanır? (5 Hibrit Mobil Kuralı)

1. **Rıza Sinyallerini App'ten WebView'e Doğrudan Aktarın:** Kullanıcı native uygulamada bir çerez/veri izni verdiyse, bu rıza parametresini WebView açılırken sorgu parametresi (*query string*) veya JavaScript Bridge aracılığıyla dataLayer'a iletin; kullanıcıya tekrar tekrar çerez banner'ı göstermeyin.
2. **Kişisel Verileri Push Notification Payload'ına Koymayın:** Sunucudan gönderilen push bildirim veri paketinde (payload) kullanıcının adı, rezervasyon kodu veya özel verilerini açık metin olarak taşımayın. Bildirimi jenerik tutup detay veriyi uygulama açıldığında güvenli API'den çekin.
3. **SDK'ların Arka Plan Veri Toplamasını Kısıtlayın:** Analitik veya hata izleme SDK'larının varsayılan olarak topladığı cihaz kimlikleri (IDFA, GAID) ve konum verilerini, ilgili izinler alınmadığı sürece SDK başlatma (*initialization*) ayarlarından kapalı tutun.
4. **WebView Formlarında Autocomplete/Autofill Güvenliği Sağlayın:** WebView içinde açılan form alanlarında hassas verilerin (kredi kartı, T.C. No) cihaz hafızasına kaydolmasını önlemek için HTML autocomplete="off" parametrelerini aktif edin.
5. **ID Eşleştirmelerini Backend Katmanında Anonimleştirin:** Mobil kullanıcı kimliği (app_user_id) ile web çerez kimliğini (web_cookie_id) birleştirirken ham verileri tutmak yerine, veritabanında tek taraflı hash algoritmalarıyla eşleme tablosu oluşturun.

Deliverables (Teslim Edilecek Çıktılar)

- **Hibrit Veri Akış Diyagramı:** Mobil Uygulama $\leftrightarrow$ WebView $\leftrightarrow$ Backend arasındaki veri transferlerini ve güvenlik kapılarını gösteren mimari şema.

- **İzin ve Veri Türleri Tablosu:** Uygulamada toplanan her bir veri tipinin (Konum, Push Token, Device ID) hukuki gerekçesini ve izin türünü belirten matris.
- **Bütünleşik ID Sözlüğü Dokümanı:** Sistemde kullanılan tüm teknik kimliklerin tanımlarını ve kullanım sınırlarını belirten teknik rehber.
- **Consent Tetikleme Test Checklist'i:** WebView ve mobil katmanda rıza durumlarına göre etiketlerin çalışmasını doğrulayan test senaryoları belgesi.
- **Log & Retention Politikası Notu:** Log saklama sürelerini, imha süreçlerini ve 14 günlük sprint uygulama planını içeren proje kapanış raporu.



[Diagram / Flow]

Mobil uygulama (native app) ve WebView hibrit mimarisinde verilerin, izin sinyallerinin ve teknik kimliklerin (ID) güvenli geçişini gösteren, 1920x1080px (16:9) Full HD çözünürlükte mimari akış diyagramı. Koyu gece mavisi ve antrasit zemin üzerinde, sol taraftaki "Native App Katmanı (Push Token / Device ID)" ve ortadaki "WebView Katmanı (Cookie / GTM Tag)" kutularından çıkan veri hatları, merkezdeki "CMP Sinyal Köprüsü & Consent Validator" katmanına ulaşıyor. Buradan onaylanan veriler, en sağdaki "Maskeli Backend Loglama & Güvenli CRM/PMS" düğümüne parlak turkuaz, mor ve elektrik yeşili akış oklarıyla bağlanarak "clarity at a glance" felsefesiyle görselleştiriliyor.

[Checklist / Framework Card]

Mobil geliştiriciler, web yazılımcıları, IT yöneticileri ve uyum sorumluları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir operational kontrol kartı. Koyu karbon gri ve siber mavi tonlarındaki teknolojik arka plan üzerinde parlayan neon yeşili mobil cihaz ve veri kalkanı ikonları yer alıyor. Kartın üzerinde; "Native App SDK Envanter Tespiti", "WebView CMP Sinyal Aktarımı", "App-Web ID Eşleme Sınırlandırması" ve "Kilit Ekranı Push Notification Maskelemesi" maddeleri, yanlarında parlak onay işaretleriyle scannable ve kurumsal bir checklist formatında sergileniyor.