Ürün & Web Geliştirme İçin Privacy by Design Checklist Şablonu — Yazılım / SDLC Privacy (v1.0)

Asset Amaç: Bu asset, Privacy by Design ve Privacy by Default ilkelerini yazılım ve ürün geliştirme yaşam döngüsüne (SDLC: Discovery → Design → Dev → Test → Release) entegre etmek için aşama bazlı teknik ve operasyonel bir kontrol seti sunar. Veri toplama formları, açık rıza / consent kurguları, loglama şemaları, erişim yetkileri ve üçüncü taraf entegrasyon kararlarını daha tasarım aşamasındayken almayı standardize eder. Otel, B2B ve yazılım projelerinde KVKK ve GDPR kaynaklı canlıya geçiş öncesi/sonrası son dakika revizyonlarını ve yazılım gecikmelerini sıfıra indirmeyi hedefler.

Kim Kullanır?: Product Owner (PO), UX/UI Designers, Software Engineers / Developers, QA / Test Engineers ve IT/BT Sorumluları.

Nasıl Kullanılır?

1. SDLC'nin her aşamasında (Discovery'den Release'e) sorulması gereken KVKK/GDPR uyum sorularını ve aşama çıktılarını doldurun.
2. Definition of Done (DoD) kriterlerine privacy maddelerini ekleyin ve her sprint'te en az 1 privacy task'ı etiketiyle (*backlog tag*) planlayın.
3. Canlıya çıkış (*release*) öncesinde "Privacy Smoke Test" uygulayın; release sonrasında ise 30–90 günlük periyodik inceleme ve 365 günlük refresh takvimini çalıştırın.

CHECKLIST & SPRINT PLAN — SDLC Privacy by Design & Default Control Set

A) Ölçüm & Önceliklendirme Checklist'i (Aşama Bazlı)

1. Discovery (Keşif & Kapsam)

- [ ] **Feature Amaç Tanımı:** Geliştirilecek özelliğin (*feature*) iş ve veri işleme amacı net ve yazılı olarak tanımlandı.
- [ ] **Data Whitelist (Alan Listesi):** Sadece özelliğin çalışması için şart olan veri alanları belirlendi (*Data Minimization*).
- [ ] **Gereksiz Alan Yasağı:** İşleme amacı olmayan ("ileride lazım olur" denilen) veri alanları karartıldı/çıkarıldı.
- [ ] **Vendor & Entegrasyon İhtiyacı:** Özellik kapsamında kullanılacak 3. parti SDK, API, script veya entegrasyonlar tespit edildi.
- [ ] **Retention / Backup / Log Notu:** Verinin saklanma süresi, yedekleme stratejisi ve loglama ihtiyacı ürün isterlerine eklendi.

2. Design (Tasarım & UX/UI)

- [ ] **Form Alanı Minimizasyonu:** Formlardaki alanlar minimize edildi; zorunlu ve opsiyonel alanlar kullanıcıya açıkça ayırt ettirildi.

- [ ] **Ayrıştırılmış Rıza & Varsayılan Kutular:** Açık rıza (*consent*) onay kutuları pazarlama metinlerinden ayrıldı ve asla önceden işaretlenmiş (*pre-checked*) olarak sunulmadı.
- [ ] **Görünür Aydınlatma Metni:** Katmanlı aydınlatma metni linkleri, form ve veri giriş alanlarının hemen altında erişilebilir yapıldı.
- [ ] **Logging Şeması:** Hangi eylemlerin loglanacağı ve logların kişisel veri içermeyeceği UI/UX tasarım dokümantasyonuna eklendi.
- [ ] **Privacy by Default Ayarları:** Varsayılan profil, veri paylaşımı ve pazarlama ayarları en gizli/en kısıtlı seviyede kurgulandı (*Export/Tracking kapalı*).

3. Dev (Geliştirme & Mimari)

- [ ] **RBAC & Admin MFA:** Veri tabanı ve admin paneli erişimleri Role-Based Access Control (RBAC) ile kısıtlandı; MFA zorunlu kılındı.
- [ ] **Veri Şifreleme (TLS + At-Rest):** Veri aktarımda TLS 1.3 ve veritabanında saklamada AES-256 şifreleme uygulandı.
- [ ] **Log Redaction / Masking:** Uygulama loglarında TC Kimlik No, e-posta, kart verisi gibi PII alanlarını otomatik maskeleyen (*redaction*) kütüphaneler aktif edildi.
- [ ] **Secrets Manager Kullanımı:** Veritabanı şifreleri ve API anahtarları kaynak kod içinde hardcoded bırakılmadı; KMS/Secrets Manager'a taşındı.
- [ ] **Consent-Driven Script Triggering:** İzleme pikselleri ve analitik etiketleri, yalnızca kullanıcının rıza vermesi durumunda tetiklenecek şekilde mimariye eklendi.

4. Test (QA & Güvenlik)

- [ ] **Consent Reddi Testi:** Rıza verilmeyen senaryoda hiçbir pazarlama ve üçüncü taraf etiketinin (*tag/script*) çalışmadığı doğrulandı.
- [ ] **PII Log Masking Testi:** Uygulama ve hata logları incelenerek log dosyasında açık PII bulunmadığı test edildi.
- [ ] **Kısıtlı Export / Dışa Aktarım:** Dışa veri aktarma yetkisi role bağlandı; varsayılanda tüm hesaplar için kapatıldı.
- [ ] **Test Verisi Anonimleştirme:** Staging ve test ortamlarında gerçek müşteri verisi kullanılmadı; maskelenmiş veya sentetik veri kullanıldı.
- [ ] **Backup / Log Heartbeat Kontrolü:** Veritabanı yedeklerinin şifreliliği ve log akışının kesintisizliği doğrulandı.

5. Release & Post-Release (Yayın & Takip)

- [ ] **Privacy Smoke Test:** Canlıya geçiş onayından hemen önce 5 maddelik kritik gizlilik smoke testi tamamlandı.
- [ ] **30–90 Gün Review Takvimi:** Canlıya alınan özelliğin veri akışları için 30 ve 90 günlük periyodik gözden geçirme takvime işlendi.
- [ ] **Vendor / Script Değişiklik Gate'i:** Uygulamaya eklenecek yeni script ve SDK'lar için otomatik onay kapsama kapısı kuruldu.
- [ ] **365 Günlük Checklist Güncelleme:** SDLC Privacy Checklist dokümanının yılda bir kez yeni KVKK/GDPR kararlarına göre güncellenmesi planlandı.

B) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm
KVKK/GDPR uyum revizyonları canlıya çıkışın son gününe kalıyor.	Discovery ve Design aşamalarında veri koruma ve gizlilik sorularının sorulmaması.	**Aşama Bazlı Checklist & DoD:** Gizlilik gereksinimlerini Definition of Done (DoD) kriteri yapmak ve tasarımdan itibaren Privacy Gate uygulamak.
Uygulama ve sunucu loglarında açık PII/kişisel veri sızıyor.	Logging mimarisinin tasarlanmaması, log maskeleme (*redaction*) mekanizmasının olmaması.	**Logging Şema Standardı & Otomatik Masking:** Loglama standardı oluşturmak ve PII verileri loga düşmeden anonimleştiren kütüphaneleri devreye almak.
Kullanıcı rızayı reddetmesine rağmen pazarlama etiketleri arka planda çalışıyor.	Etiket yöneticisi (*Tag Manager*) tetikleyicilerinin rıza durumuna göre kurgulanmaması ve QA testinin yapılmaması.	**Consent-Driven Firing & Otomatik QA Testi:** Tag'leri rıza parametresine bağlamak ve her sprintte Consent Reddi otomasyon testlerini çalıştırmak.

C) 14 Günlük Sprint Planı (Gün 1–14) — "SDLC Privacy Kurulum"

[Gün 1–4: Mimari, Whitelist & Design Gate] ──► [Gün 5–8: Log, Secrets & Test Masking] ──► [Gün 9–11: Smoke Test & Pilot Sprint] ──► [Gün 12–14: Eğitim, Review & Refresh]

- **Gün 1:** SDLC Privacy Checklist v1.0 dokümanının yayınlanması, PO, UX, Dev ve QA liderleriyle sahipliklerin paylaşılması.
- **Gün 2:** Data Whitelist şablonunun oluşturulması ve Discovery sprint toplantılarına entegre edilmesi.
- **Gün 3:** Design Review süreçlerine "Privacy Gate" aşamasının eklenmesi (Form minimizasyonu ve rıza kutusu kontrolü).
- **Gün 4:** Merkezi Logging Şema Standardının ve PII maskeleme kurallarının geliştiricilere tanımlanması.
- **Gün 5:** Rıza yönetimi (*Consent Management*) için QA ve otomasyon test senaryolarının yazılması.
- **Gün 6:** Tüm API anahtarları ve veritabanı bağlantıları için Secrets Manager / KMS standardının oturtulması.

- **Gün 7:** Admin panelleri ve sunucu erişimleri için RBAC ve zorunlu MFA kontrol listesinin uygulanması.
- **Gün 8:** Staging ve test ortamlarındaki veritabanları için otomatik maskeleme ve anonimleştirme planının devreye alınması.
- **Gün 9:** Canlıya çıkış öncesi kullanılacak 5 maddelik "Privacy Smoke Test" setinin oluşturulması.
- **Gün 10:** Uygulamaya eklenecek yeni SDK, kütüphane ve 3. parti script'ler için teknik onay kapısının (*Gate*) kurulması.
- **Gün 11:** Aktif geliştirme sprintinde en az 1 privacy görevinin (*Privacy Task/Backlog Tag*) pilot olarak yürütülmesi.
- **Gün 12:** SDLC Uyum KPI'larının belirlenmesi ve dashboard üzerinden takibinin başlatılması.
- **Gün 13:** Yazılım ve ürün ekipleri için SDLC Privacy by Design dokümantasyon eğitimi düzenlenmesi.
- **Gün 14:** 30–90 günlük canlı sonrası review takviminin işlenmesi ve 365 günlük checklist güncelleme planının onaylanması.

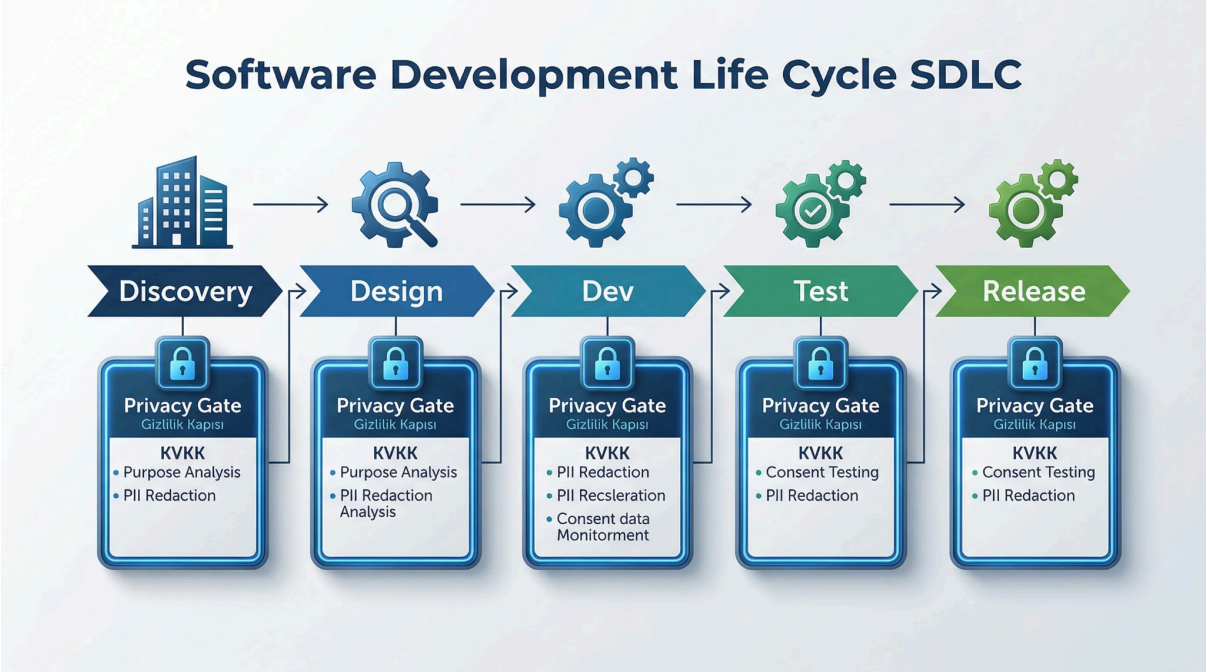
D) Öncesi / Sonrası KPI Tablosu

Ölçüm Metriği / KPI	**Öncesi (Geleneksel SDLC)**	**Sonrası (Privacy by Design SDLC)**	**Hedef Değer**
KVKK Kaynaklı Son Dakika Revizyon Sayısı	Sprint başına 4 – 6 engelleyici revizyon	0 (Discovery ve Design'da çözülüyor)	**0 Revizyon**
Privacy Kaynaklı Release Gecikmesi	5 – 10 Gün erteleme	0 Gün (DoD kriteri ile eşzamanlı)	**0 Gün**
Loglarda Taraf Edilen PII Sızıntı Sayısı	Yüksek (Açık e-posta/tel logları)	0 (Otomatik Redaction & Masking)	**0 Sızıntı**
Consent Reddi / Tag Tetikleme Uyumsuzluğu	%30 – %40 Oranında kaçak	%0 (Consent-Driven Tag Firing)	**%100 Uyum**

Sprint Başına Privacy Task Oranı	%0 (Proje sonuna ertelenir)	Sprint başına en az 1 etiketli görev	**≥ 1 Task / Sprint**

Deliverables (Teslim Edilecek Çıktılar)

- **SDLC Privacy by Design Checklist (v1.0):** Discovery, Design, Dev, Test ve Release aşamaları için teknik kontrol listesi.
- **Data Whitelist & Minimization Şablonu:** Yeni eklenecek özelliklerde veri toplama sınırlarını çizen standart form dokümanı.
- **Logging Şeması & PII Redaction Standardı:** Yazılımcılar için kişisel veri içermeyen loglama geliştirme kılavuzu.
- **Release Privacy Smoke Test Seti:** Canlıya çıkış onayında QA ve PO ekiplerince uygulanacak hızlı doğrulama testi.
- **30–90 Gün Review Takvimi & 365 Gün Refresh Planı:** Canlı sonrası gizlilik denetimi ve yıllık checklist güncelleme prosedürü.



[Diagram / Flow]

Yazılım geliştirme yaşam döngüsünün (Discovery ➔ Design ➔ Dev ➔ Test ➔ Release) 5 temel aşamasını yatay bir zaman çizelgesinde (timeline) gösteren 16:9 formatında yüksek çözünürlüklü bir SDLC Privacy Mimari Diyagramı. Koyu teknolojik arka plan üzerinde; Discovery aşamasında "Data Whitelist", Design aşamasında "Privacy by Default UI", Dev aşamasında "Log Redaction & KMS", Test aşamasında "Consent QA Firing Test", Release aşamasında ise "Privacy Smoke Test & Gate" sembolize ediliyor. Aşama geçişlerinde yeşil kilitli güvenlik

kapıları (Privacy Gates) ve veri akış yönleri kurumsal bir yazılım mimarisi şeması olarak sergileniyor.

[Checklist / Framework Card]

Product Owner'lar, yazılım mimarları ve QA mühendisleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir SDLC Privacy by Design Checklist Kartı. Koyu karbon gri zemin üzerinde; kaynak kod matrisi, gizlilik kalkanı ikonu, PII log maskeleme sembolü ve 14 günlük sprint zamanlayıcısı. Kartın üzerinde; "Discovery & Design Privacy Gates", "Automated PII Log Redaction & KMS Secrets", "Consent-Driven Firing & QA Smoke Tests", ve "Release Privacy Gate & 365-Day Refresh" teslimat kalemi başlıkları, yanlarında parlak yeşil onay rozetleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.