

Chatbot/Voicebot Diyalog & Log KVKK Checklist Şablonu — Yazılım / Bot KVKK (v1.0)

Asset Amaç: Bu asset, chatbot ve voicebot projelerinde KVKK riskini azaltmak için veri minimizasyonu odaklı diyalog tasarımı, hassas işlemlerin güvenli kanala yönlendirilmesi, konuşma ve ses loglarında otomatik maskeleyme/anonimleştirme stratejisi ile 3. parti NLP servislerine veri paylaşım sınırlarını tek kontrol seti altında toplar. Otel rezervasyon/asistan botları ve B2B müşteri destek botu senaryolarında hızlıca uygulanabilir teknik bir KVKK standardı sunar.

Kim Kullanır?: Ürün Yönetimi (PO), Müşteri Destek / Rezervasyon Operasyonu, IT/BT ve KVKK / Uyum Ekipleri.

Nasıl Kullanılır?

1. Bot diyalogları için "Veri Whitelist" tablosunu doldurarak sorulacak ve kesinlikle sorulmayacak alanları netleştirin.
2. Ödeme, iptal, profil güncelleme gibi hassas işlemleri dış güvenli kanala (*secure portal/form*) aktaran akışı kurgulayın.
3. Loglama şemasını minimize edip PII Redaction, TTL ve 3. parti NLP paylaşım kısıtlarını tanımlayarak 180 günlük periyodik yenileme (*refresh*) planını devreye alın.

CHECKLIST & SPRINT PLAN — Chatbot & Voicebot KVKK Control Set

A) Ölçüm & Önceliklendirme Checklist'i

- **[] Bot Kullanım Amaçları Net:** Botun hizmet vereceği alanlar sınırı çizilerek tanımlandı (*Rezervasyon sorgulama, SSS, Arıza/Destek kaydı*).
- **[] Diyalog Veri Whitelist Hazır:** Kullanıcıdan istenebilecek veri alanları listelendi (Örn: *Rezervasyon No, İsim-Soyisim, Talep Özeti*).
- **[] Yasaklı Alanlar Listesi Tanımlı:** Bot üzerinden toplanması kesinlikle yasaklanan veriler belirlendi (*TCKN, Kredi Kartı No, CVV, Sağlık/Alerji Bilgisi*).
- **[] Serbest Metin Limit & Uyarılar:** Serbest metin (*free-text*) giriş alanlarına karakter limiti konuldu ve "Lütfen kredi kartı veya TC Kimlik numaranızı yazmayınız" uyarısı eklendi.
- **[] Hassas İşlemler Güvenli Kanalda:** Ödeme, iade, iptal ve kişisel profil değişiklikleri chat içinden çıkarılıp doğruluk garantili güvenli web portalına yönlendirildi.
- **[] Bot İçi Kimlik Doğrulama Yasağı:** Şifre, OTP veya TCKN ile kimlik doğrulama bot sohbet ekranı içerisinde yapılmıyor.
- **[] Konuşma & Ses Loglarında PII Redaction:** Konuşma dökümlerindeki (*transcript*) veya ses kayıtlarındaki e-posta, telefon ve adres gibi PII veriler Regex/NER ile anlık maskeleniyor.
- **[] Log Retention & TTL Tanımlı:** Konuşma ve ses logları için otomatik silinme (*Time-To-Live / TTL*) süresi belirlendi (Örn: *30 gün*).
- **[] Log Erişimlerinde RBAC & Audit:** Log veritabanına erişimler rol bazlı kısıtlandı (RBAC) ve tüm sorgular silinemez audit sunucusuna kaydediliyor.
- **[] NLP Vendor Payload Minimizasyonu:** Google Dialogflow, OpenAI, AWS Lex vb. 3. parti NLP servislerine gönderilen metinlerden PII arındırılıyor.

- [] **Yönetim Paneli MFA:** Bot yönetim ve log inceleme panellerine erişimde Çok Faktörlü Kimlik Doğrulama (MFA) zorunlu kılındı.
- [] **180 Günlük Periyodik Refresh:** Bot diyalog akışları, maskeleye filtreleri ve NLP veri paylaşım kuralları 6 ayda bir denetleniyor.

B) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm
Kullanıcı serbest metin alanına kredi kartı veya TCKN yazıyor.	Uyarı metninin bulunmaması, input karakter limiti ve maskeleye olmaması.	Giriş Uyarısı + Karakter Limiti + Anlık PII Redaction: Mesaj kutusu üzerine uyarı yerleştirilmesi ve PII tespitinde verinin loga düşmeden maskelenmesi.
Bot üzerinden ödeme/iptal yapılırken veri sızıntısı riski oluşuyor.	Hassas işlemler için güvenli kanal (<i>secure iframe/portal</i>) tasarımı yapılmaması.	Güvenli Portal Yönlendirmesi & SMS/OTP Doğrulanmış Erişim: İşlemin bot dışı şifreli web formuna taşınması.
Konuşma dökümleri (transcript) ham kişisel veriyle saklanıyor.	Minimalist loglama şemasının ve zaman aşımı (TTL) kuralının olmaması.	Minimalist Log Şeması + PII Filtering + Otomatik TTL (30 Gün): Sadece işlem durumu ve anonimleştirilmiş metinlerin saklanması.

C) 14 Günlük Sprint Planı (Gün 1–14)

[Gün 1–4: Whitelist, Güvenli Kanal & Akış] → [Gün 5–8: Log Şeması, Redaction & RBAC] → [Gün 9–11: NLP Minimizasyonu & Test] → [Gün 12–14: Pilot, Review & Refresh]

- **Gün 1:** Bot amaçlarının ve "Diyalog Veri Whitelist (v1.0)" dokümanının netleştirilmesi.
- **Gün 2:** Hassas işlem listesinin çıkarılması ve güvenli web kanalı (*secure portal/link*) yönlendirme mimarisinin tasarlanması.
- **Gün 3:** Otel rezervasyon sorgulama ve B2B destek senaryoları için KVKK uyumlu diyalog akışlarının çizilmesi.
- **Gün 4:** Chatbot Arayüzüne serbest metin giriş sınırı ve "Hassas Veri Yazmayınız" uyarılarının entegre edilmesi.
- **Gün 5:** Minimalist konuşma loglama şemasının hazırlanması (PII alanlarının şemadan tamamen çıkarılması).

- **Gün 6:** Konuşma ve ses kayıtları için anlık Regex/NER tabanlı PII Redaction kütüphanesinin kurulması.
- **Gün 7:** Log veritabanı için otomatik silme (*TTL / Retention*) prosedürlerinin konfigüre edilmesi.
- **Gün 8:** Log ve yönetim paneli erişimleri için RBAC yetki matrisinin ve audit loglama altyapısının kurulması.
- **Gün 9:** 3. parti NLP servislerine (Dialogflow, OpenAI vb.) giden *payload* verilerinin arındırılması ve minimizasyonu.
- **Gün 10:** Bot yönetim panelleri için zorunlu MFA yapılandırmasının tamamlanması.
- **Gün 11:** Test senaryolarının (PII sızdırma, açık rıza reddi, güvenli kanal yönlendirme) simüle edilmesi.
- **Gün 12:** Botun kısıtlı bir kullanıcı grubuyla pilot olarak canlıya alınması.
- **Gün 13:** Pilot kullanım loglarının incelenmesi, PII maskeleye hatalarının ve kaçakların düzeltilmesi.
- **Gün 14:** Kapanış raporunun hazırlanması, ekiplere teslim edilmesi ve 180 günlük refresh takviminin başlatılması.

D) Öncesi / Sonrası KPI Tablosu

Ölçüm Metriği / KPI	Öncesi (Mevcut Durum)	Sonrası (Sprint Sonrası)	Hedef Değer
PII İçeren Log Olayı Sayısı	Yüksek (Ham metin saklama)	0 (Anlık PII Redaction ile temiz)	0 ihlal
Hassas İşlem Güvenli Kanal Yönlendirme Oranı	%0 (Chat içinde işlem)	%100 (Tamamı güvenli portalda)	%100
NLP Servisine Gönderilen PII Alan Sayısı	5 – 8 Alan (Ad, tel, e-posta vb.)	0 Alan (Sadece intent & anonim text)	0 PII Alanı
Yönetim Paneli MFA Kapsama Oranı	%0 – %20	%100 Zorunlu MFA	%100
Log Saklama Süresi Uyum Oranı (TTL)	Süresiz / Belirsiz	Maksimum 30 Gün (Otomatik Silme)	%100 Uyum

Deliverables (Teslim Edilecek Çıktılar)

- **Bot Diyalog Whitelist & Yap/Yapma Standardı Dokümanı:** İzin verilen ve yasaklanan veri alanları listesi.
- **Güvenli Kanal Yönlendirme & Kimlik Doğrulama Akış Şeması:** Hassas işlemlerin bot dışına taşınması mimarisi.
- **Minimalist Log Şeması, PII Redaction & TTL Kılavuzu:** Konuşma ve ses kayıtlarının anonimleştirilmesi ve saklama rehberi.
- **3rd Party NLP Payload Minimizasyonu Standart Dokümanı:** Dış servislere veri aktarım sınırları şartnamesi.
- **180 Günlük Bot KVKK Review & Refresh Takvimi:** Periyodik diyalog ve log denetim prosedürü.

[Diagram / Flow]

Kullanıcı mesajının/sesinin alınmasından başlayıp Serbest Metin Uyarısı & PII Redaction katmanına, oradan Intent Analizi için 3. Parti NLP Servisine, hassas işlemlerde ise Güvenli Kanala (Secure Portal) yönlendirilmesini gösteren 16:9 formatında yüksek çözünürlüklü bir Bot KVKK Mimarisi Diyagramı. Koyu şık teknolojik zemin üzerinde; mavi ve turuncu veri akış çizgileri, kilitli veri kalkanları, PII maskeleye filtresi, izole log veritabanı ve TTL zaman aşımı simgeleri profesyonel bir sistem şeması olarak sergileniyor.

[Checklist / Framework Card]

Product Owner'lar, yapay zeka mühendisleri ve KVKK uyum ekipleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Bot KVKK Uyum Checklist Kartı. Koyu karbon gri zemin üzerinde; chatbot diyalog balonu, kilitli güvenlik kalkanı, PII maskeleye gözü ve 180 günlük zamanlayıcı. Kartın üzerinde; "Dialogue Data Whitelist & Prohibited Field Enforcement", "Secure Channel Offloading for Sensitive Transactions", "Real-Time PII Redaction & Automated TTL Log Purge", ve "NLP Payload Minimization & 180-Day Refresh Schedule" teslimat kalemi başlıkları, yanlarında yeşil onay rozetleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.