Mesaj Kanalları İçin KVKK Kontrol Listesi (v1.0)

Asset Amacı: Bu checklist; otellerin DM, WhatsApp ve Web Chat kanallarında KVKK ve veri güvenliği standartlarını operasyonel olarak uygulamasını sağlar. Amacı; minimum veri toplama prensibini oturtmak, hassas veri paylaşımlarını engellemek, erişim yetkilerini düzenlemek ve veri sızıntısı (incident) riskini azaltmaktır.

(Not: Bu döküman hukuki danışmanlık değil, operasyonel iyi uygulama rehberidir.)

Kim Kullanır?: Call Center ve Rezervasyon Ekipleri, Mesaj Operatörleri, IT Birimi, Operasyon ve QA Sorumluları.

Nasıl Kullanılır? (3 Adım)

1. **Standartlaştırma:** "Minimum veri seti" ve "asla istenmeyecekler" listesini mevcut SOP (Standart Operasyon Prosedürü) dökümanınıza entegre edin.
2. **Sınırlama:** Yetki matrisi ve saklama politikası ile personelin verilere erişimini görev tanımına göre kısıtlayın ve sistem loglarını periyodik olarak kontrol edin.
3. **Denetim:** Ayda bir kez 50 konuşma üzerinden mini audit (denetim) gerçekleştirin ve hatalı örnekleri eğitimlerde anonimleştirerek tekrar edin.

Yapılması / Yapılmaması Gerekenler (Audit Checklist)

- [ ] **Hassas Veri Yasağı:** Kredi kartı bilgisi, CVV, kart görseli, kimlik/pasaport kopyası veya OTP/şifre gibi bilgileri kesinlikle talep etmeyin (YASAK).
- [ ] **Minimum Veri Prensibi:** Sadece rezervasyon için gerekli olan minimum veri seti (Ad, Soyad, İletişim vb.) dışında veri istemeyin.
- [ ] **Güvenli Yönlendirme:** Ödeme ve kimlik doğrulama gibi işlemleri WhatsApp/DM üzerinden yapmak yerine güvenli ödeme linklerine veya PMS kanallarına yönlendirin.
- [ ] **Görsel Paylaşımı:** Ekran görüntüsü paylaşımından kaçının; gerekliyse sadece maskelenmiş özet bilgiler paylaşın.
- [ ] **Kontrollü Gönderim:** Forward (yönlendirme) işlemlerinde yanlış kişiye veri gitme riskine karşı "ikinci kontrol" adımı ekleyin.
- [ ] **Veri Yaşam Döngüsü:** Saklama sürelerini belirleyin; anonimleştirme ve silme prosedürlerini yazılı hale getirin.
- [ ] **İzleme:** Erişim loglarını düzenli takip edin ve aylık 50 konuşma üzerinden kalite denetimi (Mini Audit) yapın.

Yetki ve Erişim Matrisi

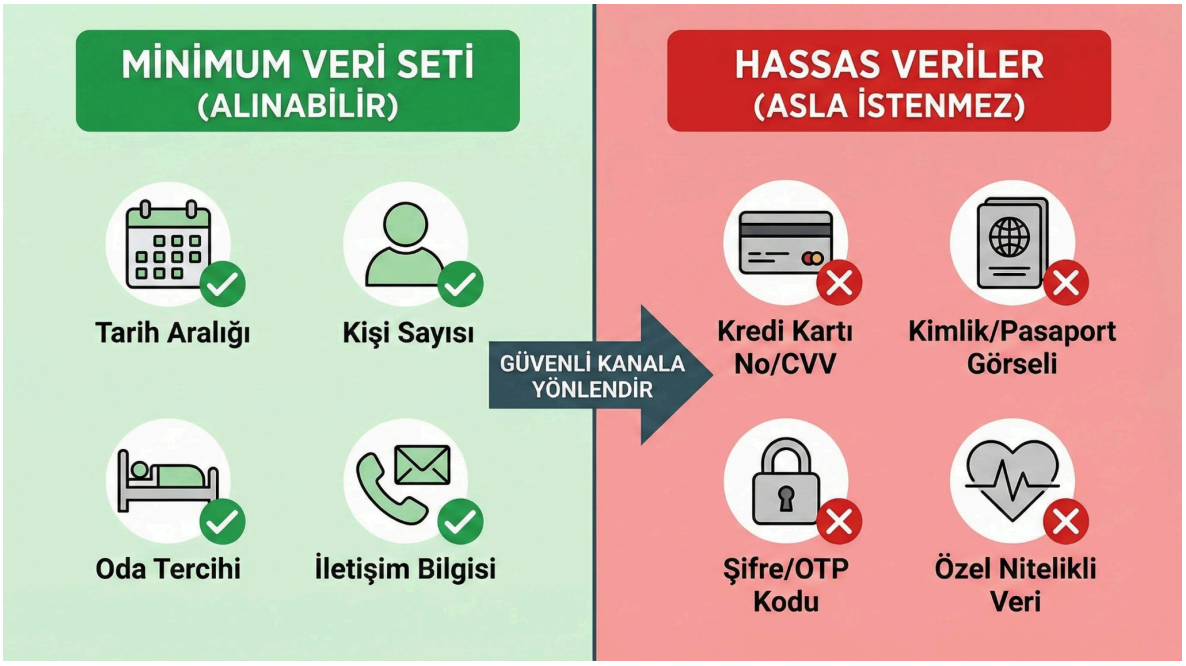
Rol	Yetki Seviyesi	Sorumluluk Alanı
Message Team	Görüntüle / Yanıtla	Günlük misafir iletişimi
Supervisor	QA + Onay	Kalite kontrol ve eskalasyon yönetimi
IT / Admin	Log + Kayıtlı Silme	Sistem güvenliği ve veri temizliği

14 Günlük Uygulama Sprint Planı

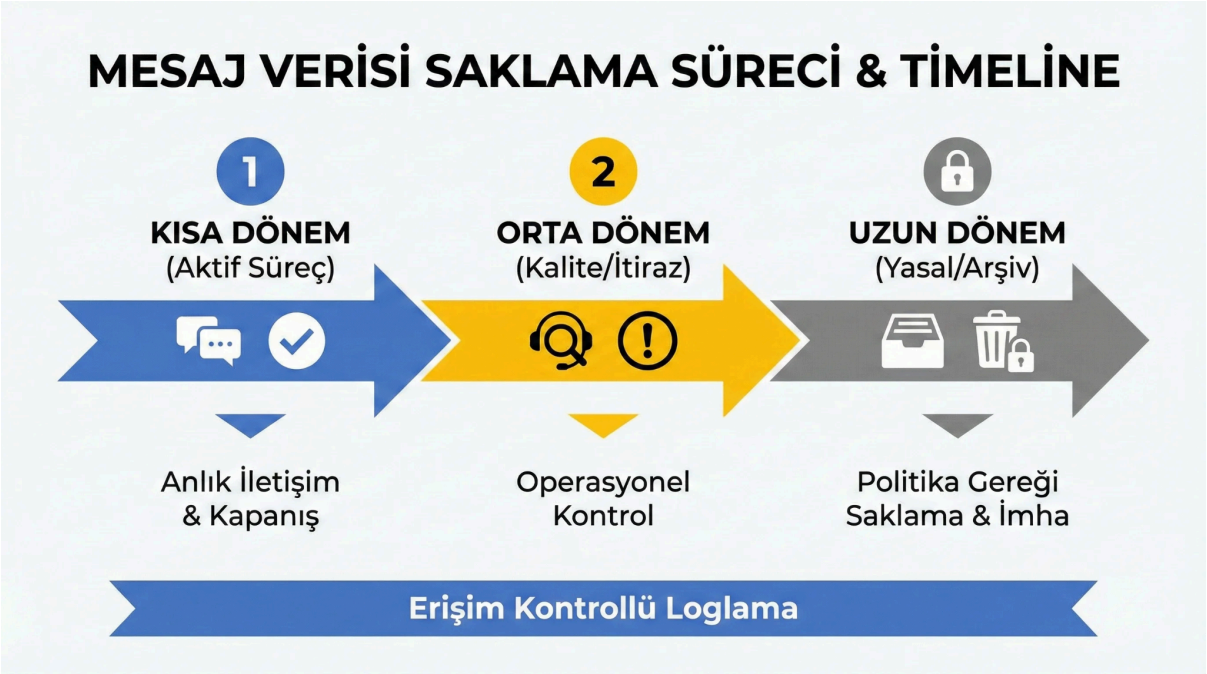
- **Gün 1–2:** Minimum veri seti ve "asla istenmeyecekler" (yasaklı liste) dökümanının oluşturulması.
- **Gün 3–5:** Mevcut mesaj şablonlarına veri güvenliği uyarı metinlerinin eklenmesi.
- **Gün 6–7:** Sistem üzerinde rol bazlı yetki matrisinin tanımlanması ve erişim ayarlarının yapılması.
- **Gün 8–10:** Veri saklama, loglama ve silme prosedürlerinin teknik olarak devreye alınması.
- **Gün 11–14:** Tüm ekipler için KVKK farkındalık eğitimi ve ilk mini audit uygulamasının yapılması.

Deliverables

KVKK Mesajlaşma Kontrol Listesi, Yetki/Erişim Matrisi Tablosu, Veri Saklama ve Loglama Prosedürü.



“Hangi personelin hangi veriye ne düzeyde erişebileceğini gösteren yetki tablosu.”



“Misafir verisinin sisteme girişinden silinmesine veya anonimleştirilmesine kadar geçen yasal saklama sürelerini gösteren diyagram.”