FLOWMATIX

Veri Koruma Etki Değerlendirmesi (DPIA)

GDPR Madde 35 uyarınca

Versiyon 1.0 · Nisan 2026 · Sorumlu: Bastian Barkowski

1. Yönetici Özeti

Bu Veri Koruma Etki Değerlendirmesi, Flowmatix tarafından sağlanan saç ekimi kliniklerinin hastalarının ve potansiyel hastalarının kişisel verilerinin işlenmesinin risklerini ve koruyucu önlemlerini belgelemektedir. İşleme, GDPR Madde 9 kapsamındaki **özel kategorideki kişisel verileri** (sağlık verileri) ve **yapay zeka ile otomatik karar vermeyi** (Anthropic Claude) içerir, böylece GDPR Madde 35(3)'te belirtilen iki kriteri karşılar. Bu nedenle bir DPIA yasal olarak zorunludur.

> **Sonuç:** Tüm risklerin ve önlemlerin değerlendirilmesinden sonra, kalan artık risk **DÜŞÜK ila ORTA** olarak sınıflandırılır. Belgelenen teknik ve organizasyonel önlemlere uyularak işleme yasal olarak gerçekleştirilebilir.

2. İşlemenin Tanımı

2.1 Veri Sorumlusu

GDPR Madde 4(7) kapsamındaki veri sorumluları, Flowmatix'in klinik müşterileridir. Flowmatix kendisi, GDPR Madde 4(8) kapsamında veri işleyen olarak hareket eder. Bu DPIA, klinik müşterilerini kendi uyum yükümlülüklerinde desteklemek için veri işleyen tarafından hazırlanır.

2.2 Amaç ve Hukuki Dayanak

Amaç	Hukuki dayanak
WhatsApp üzerinden hasta iletişimi	Madde 6(1)(b) (sözleşme başlatma), Madde 9(2)(h) (sağlık hizmeti)
Anamnez / ön değerlendirme	Madde 9(2)(a) (açık rıza), Madde 9(2)(h)
Yapay zeka destekli işleme (Claude)	Madde 9(2)(a) (Anthropic açıklamasıyla açık rıza)
Randevu yönetimi	Madde 6(1)(b)
İstatistikler / raporlama	Madde 6(1)(f) (meşru menfaat)

2.3 Veri Kategorileri ve İlgili Kişiler

İlgili kliniğin hastalarının ve potansiyel hastalarının temel, iletişim, sağlık, görsel, randevu, iletişim ve seyahat verileri işlenir (tam liste için DPA § 3'e bakın).

2.4 Teknik Mimari (özet)

- **Barındırma:** Hetzner Online GmbH, Falkenstein/Nürnberg, Almanya (ISO 27001)
- **Veritabanı:** PostgreSQL 16, Satır Düzeyi Güvenlik (RLS) ile, klinik başına çok kiracılı ayrım
- **Frontend:** React (Vite), TLS 1.3, Cloudflare CDN/WAF
- **Backend:** Fastify/TypeScript, BullMQ Queue, Redis
- **WhatsApp sağlayıcısı:** 360dialog GmbH (Berlin) → Meta Cloud API
- **AI bileşeni:** Anthropic Claude API (Sonnet 4.5), Sıfır Veri Saklama API modu
- **Kimlik doğrulama:** Yenileme jetonu rotasyonlu JWT, isteğe bağlı MFA (TOTP), bcrypt maliyet faktörü 12

3. Gereklilik ve Orantılılık

3.1 Gereklilik

Otomatik ön değerlendirme olmadan, klinikler her hasta sorgusunu manuel olarak işlemek zorunda kalır — günde 50–500 sorgu gibi tipik bir hacimde, bu ekonomik olarak uygulanabilir olmaz. Yapay zeka destekli ön değerlendirme yalnızca tıbbi değerlendirmeleri hazırlamaya hizmet eder ve onların yerine geçmez. Tıbbi kararların nihai sorumluluğu kliniğin tıbbi personelinde kalır.

3.2 Veri Minimizasyonu

- Yalnızca ön değerlendirme ve randevu rezervasyonu için gerekli veriler toplanır.
- Hasta fotoğrafları yalnızca tedavi eden hekim tarafından istenen sayıda toplanır.
- Hassas alanlar (örn. anamnez JSON) veritabanında takma adlandırılır/şifrelenir.
- Mesaj içeriği Anthropic'e açık tanımlayıcılar olmadan gönderilir.

3.3 Saklama Sınırlaması (Madde 5(1)(e))

Platform, yapılandırılabilir saklama süresi (varsayılan: § 630f BGB uyarınca 10 yıl) sona erdikten sonra hasta verilerini anonimleştiren otomatik bir saklama tarayıcısı uygular. Hastalar istedikleri zaman CRM aracılığıyla derhal silme talep edebilirler (GDPR Madde 17 uyarınca Hard Delete).

4. Risk Değerlendirmesi

4.1 Tanımlanan Riskler

Risk	Olasılık	Şiddet	Derecelendirme
Hasta verilerine yetkisiz erişim	Düşük	Yüksek	Orta
Sistem arızası nedeniyle veri kaybı	Çok düşük	Orta	Düşük
Kiracılar arası veri sızıntısı	Çok düşük	Çok yüksek	Orta
ABD alt işleyicilerine aktarım (Anthropic, Cloudflare)	Yüksek (sürekli)	Orta	Orta
Hatalı yapay zeka işlemi yanlış bilgiye yol açar	Orta	Orta	Orta
Hasta onayı geri çeker — veriler silinmez	Düşük	Yüksek	Orta
Klinik personeli erişimi kötüye kullanır	Düşük	Yüksek	Orta
Klinik personelinin kimlik avı / hesap ele geçirme	Orta	Yüksek	Yüksek
Fidye yazılımı / şantaj	Düşük	Çok yüksek	Orta
Klinik bilgisi olmadan Google Drive'a fotoğraf yükleme	Düşük (artık opt-in)	Yüksek	Düşük

4.2 Risk Azaltma Önlemleri

Erişim Koruması

- Tüm klinik hesapları için çok faktörlü kimlik doğrulama (TOTP) mevcut — öneri: yönetici rolleri için zorunlu
- Kısa ömürlü JWT + yenileme jetonu rotasyonu
- Şifre hashleme için bcrypt maliyet faktörü 12
- Giriş uç noktalarında hız sınırlama (5 deneme / 15 dakika)
- Şüpheli etkinlikte oturum iptali

Kiracı Ayrımı

- PostgreSQL Satır Düzeyi Güvenlik, veritabanı düzeyinde organization_id kontrolünü zorlar
- Uygulama kodu kiracı bağlamı (AsyncLocalStorage) kullanır
- Uygulama kullanıcısı için BYPASSRLS yok

- RLS etkisi olan tüm değişiklikler için kod incelemeleri

Üçüncü Ülke Aktarımları (Schrems II)

- Tüm ABD alt işleyicileriyle AB Standart Sözleşme Hükümleri (SCC 2021/914)
- Anthropic: Sıfır Veri Saklama API modu aktif — veriler eğitim için kullanılmaz
- Anthropic API çağrısı öncesi takma adlandırma (doğrudan tanımlayıcı yok)
- Cloudflare: yalnızca yönlendirme/CDN, içerik verisi saklanmaz

Yapay Zeka Riskleri

- Bot 512 token ile sınırlıdır → tıbbi tanıların halüsinasyonu yok
- Tıbbi kararları yasaklayan katı sistem komutları
- `<patient_message>` etiketleriyle sarmalanarak komut enjeksiyonu koruması
- Fotoğraf tamamlandığında: insan doktor incelemecisine otomatik devir
- Saldırganlık / karmaşık sorularda: otomatik devir
- Açık GDPR onayı olmadan bot yanıtı yok

Kullanılabilirlik ve Kurtarma

- Saha dışı çoğaltma ile günlük, haftalık, aylık yedeklemeler
- RTO: 4 saat, RPO: 24 saat
- 7/24 izleme (Grafana, Prometheus, Loki, Uptime Kuma)
- Felaket kurtarma planı belgelenmiş ve yıllık olarak test edilmiştir

Denetim İzi

- Tüm veri erişimlerinin tam denetim günlüğü (GDPR Madde 30 işleme kayıtları)
- Hasta kayıtlarına okuma erişimi kullanıcı, IP, zaman damgası ile kaydedilir
- Standart kullanıcılar denetim günlüğünü silemez

İlgili Kişi Hakları

- Veri dışa aktarma uç noktası (Madde 15 + 20) — tüm hasta verilerinin JSON indirme
- Hard delete uç noktası (Madde 17) — onay ile tam silme
- Onay günlüğü her onayı zaman damgasıyla belgeler
- Saklama süresinden sonra otomatik anonimleştirme

5. Artık Risk Değerlendirmesi

Kategori	Önlemler öncesi	Önlemler sonrası
Gizlilik	Yüksek	Düşük
Bütünlük	Orta	Düşük
Kullanılabilirlik	Orta	Düşük
Üçüncü ülke aktarımı	Yüksek	Orta
Yapay zeka halüsinasyonu	Orta	Düşük
Genel	**Yüksek**	**Düşük–Orta**

6. Denetim Otoritesi ile İstişare

Kalan artık risk düşük ila orta olarak sınıflandırıldığından, GDPR Madde 36 uyarınca denetim otoritesi ile önceden istişare **gerekli değildir**. DPIA dahili olarak belgelenir ve denetim otoritesinden veya klinik müşterilerinden gelen talep üzerine sağlanır.

7. Düzenli İnceleme

Bu DPIA en az yılda bir veya işlemede önemli değişiklikler olduğunda gözden geçirilir ve güncellenir. Önemli değişiklikler şunları içerir:

- Yeni alt işleyicilerin devreye alınması
- Amaçların veya veri kategorilerinin değişmesi
- Yapay zeka sağlayıcısı veya modelinin değişmesi
- Yeni risklerin keşfi (örn. güvenlik açıkları)
- İçtihat değişiklikleri (örn. Schrems III)

8. Sorumluluklar

Rol	Sorumluluk
Flowmatix Yönetimi	Bastian Barkowski — genel sorumluluk, DPIA onayı
Veri Koruma Görevlisi	privacy@flowmatix.io
Teknik uygulama	Mühendislik Ekibi (Bastian Barkowski)
Alt işleyici yönetimi	privacy@flowmatix.io

HAZIRLAYAN

Bastian Barkowski · Flowmatix

Hude, Nisan 2026

SONRAKİ İNCELEME

Nisan 2027

veya önemli değişiklikte