FLOWMATIX

Veri İşleme Sözleşmesi (DPA)

KVKK ve GDPR Madde 28 uyarınca

Versiyon 2.0 · Nisan 2026

VERİ SORUMLUSU

[Klinik Adı]

[Cadde, Numara]
[Posta kodu, Şehir, Ülke]
Temsilci: [Yönetim / Sahip]
— bundan sonra "Veri Sorumlusu" —

VERİ İŞLEYEN

Flowmatix – Automation
Sahip: Bastian Barkowski
An der Moorbäke 6, 27798 Hude, Almanya
E-posta: legal@flowmatix.io
— bundan sonra "Veri İşleyen" —

Giriş

Veri Sorumlusu, hasta iletişimi otomasyonu, ön değerlendirme, randevu organizasyonu ve tıbbi değerlendirme için yapay zeka destekli hazırlık amacıyla Veri İşleyen'in hizmetlerinden yararlanır. Bu süreçte Veri Sorumlusu'nun hastalarına ve potansiyel hastalarına ait kişisel veriler işlenir. Bu sözleşme, GDPR Madde 28 ve KVKK uyarınca tarafların veri koruma yükümlülüklerini düzenler ve önceki tüm veri işleme anlaşmalarının yerine geçer.

§ 1 Konu ve Süre

(1) Konu

Bu sözleşmenin konusu, Flowmatix CRM ve otomasyon platformunun Veri Sorumlusu'na sunulması kapsamında Veri İşleyen tarafından kişisel verilerin işlenmesidir.

(2) Süre

Sözleşme imzalandığı tarihte yürürlüğe girer ve süresiz olarak devam eder. Ana sözleşmenin sona ermesiyle otomatik olarak sona erer veya her iki taraf da dört hafta önceden yazılı bildirimle feshedebilir. Haklı sebeple olağanüstü fesih hakkı saklıdır.

§ 2 İşlemenin Niteliği ve Amacı

Kişisel veriler yalnızca aşağıdaki amaçlarla işlenir:

- WhatsApp ve benzeri kanallar üzerinden dijital hasta iletişimi
- Anamnez verilerine dayalı hasta ön değerlendirmesi
- Tıbbi değerlendirme için hasta dosyalarının yapay zeka destekli hazırlığı (Anthropic Claude API kullanılarak)
- Danışmanlık, ameliyat tarihleri ve takip iletişiminin organizasyonu
- Hatırlatmaların, bakım sonrası mesajların ve tedavi planlarının gönderilmesi
- Hasta belgelerinin, fotoğraflarının ve tıbbi bilgilerinin yönetimi
- Veri Sorumlusu için istatistikler ve raporlar sunma
- Platformun teknik desteği ve bakımı

Veri İşleyen tarafından tıbbi teşhis veya tedavi önerisi yapılmaz. Tıbbi kararların nihai sorumluluğu Veri Sorumlusu'na ve tıbbi personeline aittir.

§ 3 Kişisel Veri Kategorileri

- **Temel veriler:** Ad ve soyad, cinsiyet, yaş / doğum tarihi, dil, ülke
- **İletişim verileri:** Telefon numarası (WhatsApp), e-posta adresi
- **Sağlık verileri (GDPR Madde 9 / KVKK Madde 6):** Anamnez, saç durumu, mevcut hastalıklar, ilaçlar, alerjiler, önceki tedaviler, sigara durumu, kan sulandırıcılar, diğer tıbbi bilgiler
- **Görsel veriler:** Hasta fotoğrafları (ön, yan, donör bölge, yakın çekimler)
- **Randevu verileri:** Danışmanlık ve ameliyat tarihleri, takvim rezervasyonları
- **İletişim içeriği:** WhatsApp mesajları, sesli mesajlar (yazıya dökülmüş), belgeler
- **Seyahat verileri:** Uçuş bilgileri (hasta tarafından gönüllü olarak iletilen), sürücü/otel bilgileri
- **Onay kayıtları:** Zaman damgalı GDPR onay günlükleri

§ 4 İlgili Kişi Kategorileri

- Veri Sorumlusu'nun hastaları ve potansiyel hastaları

- Veri Sorumlusu'nun çalışanları ve tıbbi personeli (platformun kullanımı için gerekli olduğu ölçüde sınırlı)

§ 5 Veri İşleyen'in Yükümlülükleri

(1) Belgelenmiş Talimatlara Bağlılık

Veri İşleyen, kişisel verileri yalnızca Veri Sorumlusu'nun belgelenmiş talimatları doğrultusunda işler; üçüncü ülkelere aktarımlar dahil. Yasal yükümlülükler hariçtir.

(2) Gizlilik

Veri İşleyen, işlemeye yetkili tüm kişilerin gizlilikle yükümlü olmasını veya uygun bir yasal gizlilik yükümlülüğüne tabi olmasını sağlar. Çalışanlar düzenli olarak veri koruma konusunda eğitim alır.

(3) İşleme Güvenliği

Veri İşleyen, GDPR Madde 32 uyarınca gerekli tüm önlemleri uygular. Teknik ve organizasyonel önlemlerin ayrıntılı açıklaması **Ek 1**'de yer almaktadır.

(4) Destek

Veri İşleyen, işlemenin niteliğini dikkate alarak, ilgili kişilerin taleplerine yanıt verme ve GDPR Madde 32–36 kapsamındaki yükümlülüklere (özellikle güvenlik, ihlal bildirimleri ve veri koruma etki değerlendirmeleri) uyma konusunda Veri Sorumlusu'na uygun teknik ve organizasyonel önlemlerle destek sağlar.

§ 6 Alt Veri İşleyenler

(1) Genel Yetki

Veri Sorumlusu, Veri İşleyen'e hizmetin sağlanması için diğer veri işleyenleri ("Alt Veri İşleyenler") devreye alma konusunda genel yazılı yetki verir. Sözleşme imzalandığı tarihte devreye alınmış Alt Veri İşleyenler **Ek 2**'de listelenmiştir.

(2) Değişiklikler

Veri İşleyen, Alt Veri İşleyenlerin eklenmesi veya değiştirilmesine ilişkin amaçlanan değişiklikler hakkında Veri Sorumlusu'nu en az 30 gün önceden kayıtlı iletişim adresine e-posta ile bilgilendirir. Veri Sorumlusu, zorlayıcı veri koruma nedenleriyle 14 gün içinde yazılı olarak değişikliğe itiraz edebilir. İtiraz halinde her iki taraf da olağanüstü fesih hakkına sahiptir.

(3) Alt Veri İşleyenlerin Yükümlülükleri

Veri İşleyen, her Alt Veri İşleyeni en azından bu DPA'da belirtilen veri koruma yükümlülüklerine sözleşmeye dayalı olarak bağlar. Bir Alt Veri İşleyen, veri koruma yükümlülüklerini yerine getirmezse,

Veri İşleyen, bu Alt Veri İşleyen'in yükümlülüklerinin yerine getirilmesinden Veri Sorumlusu'na karşı sorumlu kalır.

§ 7 Uluslararası Veri Aktarımları

Kişisel veriler AEA dışındaki üçüncü ülkelere aktarıldığında, Veri İşleyen GDPR Madde 44 vd. uyarınca aşağıdaki güvencelerden birinin mevcut olmasını sağlar:

- AB Komisyonu'nun yeterlilik kararı, veya
- Mevcut sürümünde (Uygulama Kararı (AB) 2021/914) AB Standart Sözleşme Hükümleri (SCC), gerektiğinde Schrems II içtihadı uyarınca ek önlemlerle desteklenmiş olarak, veya
- Bağlayıcı Kurumsal Kurallar (BCR), veya
- İlgili kişinin GDPR Madde 49(1)(a) uyarınca belirli bir aktarıma açık rızası.

KVKK uyumluluğu (Türk hastalar): Türk kanunları kapsamındaki kişisel verilerin yurtdışına aktarılması için, Veri Sorumlusu KVKK Madde 9 uyarınca her hastadan açık rıza alır veya KVKK Kurulu tarafından önceden onaylanmış bir taahhütname kullanır. Veri İşleyen, KVKK Aydınlatma Metni şablonunu sağlayarak bu süreçte Veri Sorumlusu'nu destekler.

Tüm üçüncü ülke aktarımlarının ve hukuki dayanaklarının tam listesi **Ek 2**'de yer almaktadır.

§ 8 Veri İhlali Bildirimi

Veri İşleyen, herhangi bir kişisel veri ihlalinden haberdar olduktan sonra gecikmeksizin ve her durumda **24 saat içinde** Veri Sorumlusu'nu bilgilendirir (GDPR Madde 33). Bildirim en az şunları içerir:

- İhlalin niteliğinin açıklaması (etkilenen ilgili kişi ve kayıtların kategorileri ve yaklaşık sayısı)
- Veri Koruma Görevlisi'nin veya diğer iletişim noktasının adı ve iletişim bilgileri
- Olası sonuçların açıklaması
- Alınan veya önerilen önlemlerin açıklaması

Veri İşleyen, denetim makamına ve gerektiğinde etkilenen ilgili kişilere bildirim yükümlülüklerini yerine getirme konusunda Veri Sorumlusu'nu destekler.

§ 9 İlgili Kişilerin Hakları

Veri İşleyen, GDPR Madde 12–22 kapsamında ilgili kişilerin haklarının yönetiminde Veri Sorumlusu'na destek olur, özellikle:

- **Erişim hakkı (Madde 15):** Platform, saklanan tüm hasta verilerini indirmek için bir dışa aktarma fonksiyonu (JSON formatı) sunar.
- **Düzeltme hakkı (Madde 16):** Temel veriler ve hasta kayıtları Veri Sorumlusu tarafından istediği zaman güncellenebilir.

- **Silme hakkı (Madde 17):** Platform, tüm kişisel verileri geri alınamaz şekilde kaldıran tam silme fonksiyonu ("hard delete") sunar.
- **Kısıtlama hakkı (Madde 18):** Veri Sorumlusu hasta kayıtlarını salt okunur duruma getirebilir.
- **Veri taşınabilirliği hakkı (Madde 20):** Dışa aktarma fonksiyonu, verileri yapılandırılmış, yaygın olarak kullanılan, makine tarafından okunabilir bir formatta (JSON) sağlar.
- **İtiraz hakkı (Madde 21):** Veri Sorumlusu, otomatik işlemeyi istediği zaman devre dışı bırakabilir.

§ 10 Denetim Hakları

Veri Sorumlusu, Veri İşleyen tarafından bu sözleşmeye uyumun denetlenmesi hakkına sahiptir. Talep üzerine, Veri İşleyen uyumu kanıtlamak için gerekli tüm bilgileri sağlar.

Denetimler, dört hafta önceden bildirimde bulunarak yerinde veya uzaktan, takvim yılı başına en fazla bir kez ve en fazla bir iş günü olarak gerçekleştirilebilir; veri koruma ihlali için somut belirtiler olmadıkça. Yerinde denetim yerine, Veri İşleyen bağımsız bir denetçinin (örn. ISO 27001, SOC 2, BSI C5) güncel raporunu sunabilir.

§ 11 Saklama ve Silme

Veri İşleyen, kişisel verileri yalnızca anlaşılan hizmetleri sağlamak için gerekli olduğu sürece veya yasal saklama yükümlülükleri olduğu sürece saklar. Platform, yapılandırılabilir saklama süresi (varsayılan: § 630f BGB uyarınca 10 yıl) sona erdikten sonra hasta verilerini anonimleştiren otomatik bir saklama tarayıcısı uygular.

Sözleşmenin sona ermesi üzerine, Veri İşleyen, Veri Sorumlusu yapılandırılmış bir formatta iadeyi açıkça talep etmediği sürece tüm kişisel verileri **30 gün içinde** siler veya anonimleştirir. Talep üzerine silme yazılı olarak onaylanır.

§ 12 Sorumluluk

Tarafların sorumluluğu GDPR Madde 82'ye tabidir. Veri İşleyen, yalnızca GDPR kapsamında özellikle veri işleyenlere yüklenen yükümlülüklerine uymadığı veya Veri Sorumlusu'nun yasal talimatlarına aykırı veya bunların dışında hareket ettiği takdirde sorumludur.

Veri İşleyen'in tıbbi kararlar, tedavi tedbirleri veya terapi önerileri konusundaki sorumluluğu hariç tutulmuştur. Bunlar yalnızca Veri Sorumlusu'nun sorumluluğundadır.

§ 13 Veri Koruma Görevlisi

Veri İşleyen'in Veri Koruma Görevlisi şu adresten ulaşılabilir: **privacy@flowmatix.io**. Veri Sorumlusu, (varsa) Veri Koruma Görevlisi'nin adını ve iletişim bilgilerini gecikmeksizin Veri İşleyen'e bildirir.

§ 14 Geçerli Hukuk ve Yetkili Mahkeme

Bu sözleşme, Uluslararası Mal Satışına İlişkin Sözleşmeler Hakkında BM Sözleşmesi hariç, münhasıran Alman hukukuna tabidir. Bu sözleşmeden veya bu sözleşmeyle bağlantılı olarak doğan uyuşmazlıklar için yetkili mahkeme, Veri Sorumlusu'nun tüccar, kamu hukuku tüzel kişisi veya kamu hukuku özel varlığı olması koşuluyla, Hude (veya Almanya'daki en yakın yetkili mahkeme) olarak belirlenmiştir.

§ 15 Son Hükümler

(1) Bu sözleşmenin münferit hükümleri geçersiz olur veya geçersiz hale gelirse, sözleşmenin geri kalanının geçerliliği etkilenmez. Taraflar geçersiz hükmü, geçersiz hükmün ekonomik ve hukuki amacına en yakın geçerli bir hükümle değiştirir.

(2) Bu sözleşmedeki değişiklikler ve eklemeler yazılı olarak yapılmalıdır. Bu, bu yazılı şekil şartının kaldırılması için de geçerlidir.

(3) Bu DPA ile ana sözleşme arasında çelişki olması durumunda, bu DPA'nın hükümleri geçerlidir.

VERİ SORUMLUSU

[Ad]

Yer, Tarih, İmza

VERİ İŞLEYEN

Bastian Barkowski · Flowmatix

Hude, _____, _____

Ek 1 — Teknik ve Organizasyonel Önlemler (TOM)

Bu ek, riske uygun bir koruma seviyesi sağlamak için GDPR Madde 32 uyarınca uygulanan teknik ve organizasyonel önlemleri açıklamaktadır.

1. Gizlilik

Önlem	Uygulama
Fiziksel erişim kontrolü	Sertifikalı veri merkezlerinde sunucular (Hetzner Online GmbH, Falkenstein/Nürnberg, Almanya) — ISO 27001 sertifikalı. Fiziksel erişim yalnızca iki faktörlü kimlik doğrulamalı yetkili personel için.
Sistem erişim kontrolü	Tüm platform hesapları için çok faktörlü kimlik doğrulama (TOTP). Yenileme jetonu rotasyonlu oturum çerezleri. Bcrypt şifre hashleme (maliyet faktörü 12).
Veri erişim kontrolü	6 rollü rol tabanlı erişim kontrolü (RBAC). Veritabanı düzeyinde satır düzeyi güvenlik (RLS) kiracı ayrımını zorlar. Her çalışan yalnızca kendi kliniğinin verilerini görür.
Kiracı ayrımı	Klinik başına katı ayrımlı çok kiracılı mimari (organization_id) tüm katmanlarda. PostgreSQL satır düzeyi güvenlik, uygulama hatalarında bile kiracılar arası erişimi engeller.
Takma adlandırma	Hassas alanlar (örn. anamnez verileri) şifrelenmiş olarak saklanır. Denetim günlükleri isimler yerine kullanıcı kimlikleri içerir.

2. Bütünlük

Önlem	Uygulama
Aktarım kontrolü	Tüm dış bağlantılar için aktarım şifrelemesi (TLS 1.3). WhatsApp iletişimi WhatsApp protokolü aracılığıyla uçtan uca şifrelenmiştir.
Giriş kontrolü	Zaman damgası, kullanıcı kimliği, IP adresi ve kullanıcı aracısı ile tüm veri erişimlerinin ve değişikliklerinin tam denetim kaydı. Hasta kayıtlarına okuma erişimi GDPR Madde 30 uyarınca kaydedilir.
Beklemede şifreleme	Veritabanı yedeklemeleri AES-256 ile şifrelenmiştir. Hassas alanlar ayrıca uygulama katmanında şifrelenir.

3. Kullanılabilirlik ve Dayanıklılık

Önlem	Uygulama
Kullanılabilirlik kontrolü	Saha dışı çoğaltma ile günlük, haftalık ve aylık otomatik yedeklemeler. Uyarı ile 7/24 izleme (Grafana, Prometheus, Loki, Uptime Kuma). Coğrafi olarak yedekli DNS.
Kurtarılabilirlik	Kurtarma Süresi Hedefi (RTO): 4 saat. Kurtarma Noktası Hedefi (RPO): 24 saat. Felaket kurtarma planı belgelenmiş ve yıllık olarak test edilmiştir.
Dayanıklılık	Harici API'ler için devre kesici, veritabanı bağlantıları için otomatik yük devretme, AOF + RDB ile Redis kalıcılığı.

4. Düzenli İnceleme Prosedürleri

Önlem	Uygulama
Veri koruma yönetimi	Veri Koruma Görevlisi atandı (privacy@flowmatix.io). GDPR Madde 30 uyarınca işleme faaliyetleri kayıtları tutulmaktadır. Sağlık verilerinin işlenmesi için Veri Koruma Etki Değerlendirmesi (DPIA) belgelenmiştir.
Olay yanıt yönetimi	Veri koruma olaylarını tespit etme, raporlama ve ele alma için belgelenmiş süreç. 24 saat içinde Veri Sorumlusu'na bildirim yükümlülüğü (bkz. § 8).
Tasarımdan gizlilik	Tasarımdan gizlilik ilkesi. Veri minimizasyonu. Amaç sınırlaması. Varsayılan ayarlar gizlilik dostudur (örn. Google Drive otomatik yükleme varsayılan olarak devre dışı).
Alt işleyici yönetimi	Alt işleyiciler devreye alınmadan önce GDPR uyumluluğu için incelenir. Tüm alt işleyicilerle yazılı sözleşmeler (bkz. Ek 2).

Ek 2 — Alt Veri İşleyenler

Aşağıdaki alt veri işleyenler sözleşme imzalandığı tarihte devreye alınmıştır. Değişiklikler bu DPA'nın § 6(2)'sine göre bildirilecektir.

Ad ve Adres	Amaç	İşlenen veriler	Üçüncü ülke aktarımı	Güvenceler
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Almanya	Barındırma, sunucu altyapısı, yedekleme	Tümü	Hayır (AB/DE)	GDPR Madde 28 uyarınca DPA
Anthropic, PBC 548 Market St, PMB 90375, San Francisco, CA 94104, ABD	Hasta mesajlarını işlemek için yapay zeka dil modeli (Claude)	Mesaj içeriği, anamnez (doğrudan tanımlayıcı yok)	Evet (ABD)	AB Standart Sözleşme Hükümleri (SCC) 2021/914 + Sıfır Veri Saklama API modu
360dialog GmbH Torstraße 61, 10119 Berlin, Almanya	WhatsApp Business Solution Provider (BSP)	Telefon numaraları, mesaj içeriği	Meta üzerinden dolaylı olarak (İrlanda/ABD)	GDPR Madde 28 uyarınca DPA + Meta bileşenleri için SCC
Meta Platforms Ireland Ltd. 4 Grand Canal Square, Dublin 2, İrlanda	WhatsApp altyapısı (Cloud API)	Mesaj içeriği, telefon numaraları	Evet (ABD)	AB Standart Sözleşme Hükümleri (SCC) 2021/914
Stripe Payments Europe Ltd. 1 Grand Canal Street Lower, Dublin 2, İrlanda	Ödeme işleme	Ad, e-posta, ödeme verileri	Dolaylı (İrlanda/ABD)	AB Standart Sözleşme Hükümleri (SCC) 2021/914
Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107, ABD	CDN, DDoS koruması, web uygulama güvenlik duvarı	IP adresleri, HTTP başlıkları	Evet (ABD)	AB Standart Sözleşme Hükümleri (SCC) 2021/914
Brevo (eski adıyla Sendinblue) 106 boulevard Haussmann, 75008 Paris, Fransa	İşlemsel e-postalar (doğrulama, bildirimler)	E-posta adresleri, içerik	Hayır (AB/FR)	GDPR Madde 28 uyarınca DPA
Google Ireland Ltd. Gordon House, Barrow Street, Dublin 4, İrlanda	*İsteğe bağlı*: Google Calendar senkronizasyonu, Google Drive fotoğraf yedeklemesi (yalnızca Veri Sorumlusu tarafından açıkça etkinleştirildiğinde)	Randevular, hasta fotoğrafları (yalnızca opt-in ise)	Evet (ABD)	AB Standart Sözleşme Hükümleri (SCC) 2021/914 — Veri Sorumlusu'nun kendi Google Workspace DPA'sı gerekli

AviationStack apilayer Data Products GmbH, Viyana, Avusturya	Uçuş durumu sorgusu (yalnızca uçuş takibi etkinleştirildiğinde)	Uçuş numaraları (hastayla ilgili değil)	Hayır (AB/AT)	GDPR Madde 28 uyarınca DPA

Üçüncü ülke aktarımları hakkında not: ABD'ye yapılan tüm aktarımlar, mevcut sürümünde Uygulama Kararı (AB) 2021/914 uyarınca AB Standart Sözleşme Hükümleri (SCC) temelinde gerçekleştirilir. AAD'nin "Schrems II" kararının gerekliliklerini karşılamak için ek teknik ve organizasyonel önlemler (örn. şifreleme, takma adlandırma) gözden geçirilir ve uygun şekilde uygulanır.

Ek 3 — Veri Sorumlusu Talimatları

Veri Sorumlusu, kişisel verilerin işlenmesi için Veri İşleyen'e aşağıdaki sürekli talimatları verir:

1. Yalnızca bu sözleşmenin § 2'sinde belirtilen amaçlarla işleme.
2. Verilerin yalnızca AEA içindeki sunucularda saklanması (Hetzner Almanya), Ek 2'de listelenen alt işleyiciler hariç.
3. Sağlık verilerinin (GDPR Madde 9) işlenmesi yalnızca platform onay günlüğünde belgelenmiş ilgili kişinin açık rızası ile.
4. Yapılandırılmış saklama süresinin (varsayılan: 10 yıl) dolmasından sonra hasta verilerinin otomatik olarak anonimleştirilmesi.
5. Veri Sorumlusu'nun talebi üzerine 24 saat içinde bir hasta kaydının tamamen silinmesi ("hard delete").
6. İlgili kişilerin talebi üzerine JSON formatında veri dışa aktarımı sağlanması.
7. Verilerin kendi amaçları için kullanılmaması, özellikle hasta verileri ile yapay zeka modellerinin eğitilmemesi.
8. İşlenen verilerle ilgili olarak yetkililer veya denetim makamlarından gelen taleplerin derhal bildirilmesi.

Veri Sorumlusu, **privacy@flowmatix.io** adresine e-posta ile istediği zaman başka bireysel talimatlar verebilir. Veri İşleyen, talimatı gecikmeksizin uygulayacak veya bir talimatın görüşüne göre veri koruma yasasını ihlal ettiğini düşünüyorsa Veri Sorumlusu'nu gecikmeksizin bilgilendirecektir.