ProcessMind Güvenlik Önlemleri

Yürürlük tarihi: 14 Eylül 2026

Bu belge, ProcessMind B.V.'nin Müşteri Verilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için sürdürdüğü teknik ve organizasyonel önlemleri ("TOM'lar") açıklar. ProcessMind, Müşteri Verilerini her düzeyde — ağ ve altyapıdan kimlik, yetkilendirme, veri izolasyonu, şifreleme, izleme ve yazılım geliştirmeye kadar — birden fazla bağımsız güvenlik katmanının koruduğu derinlemesine savunma yaklaşımını izler. Bu önlemler Veri İşleme Ekini, Gizlilik Politikasını ve SaaS Barındırma Politikasını tamamlar. ProcessMind bu önlemleri en az yılda bir kez gözden geçirir ve günceller.

Müşteri Verileri hiçbir zaman üçüncü taraflara satılmaz, üçüncü taraflarla paylaşılmaz veya üçüncü taraflarca kendi amaçları için kullanılmaz.

---

1. Altyapı Güvenliği

1.1 Bulut Platformu. ProcessMind yalnızca AB'de (Frankfurt, Almanya, `eu-central-1`) Amazon Web Services (AWS) üzerinde barındırılır. AWS, ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 ve PCI DSS sertifikalarını sürdürür. Tam liste için AWS Uyumluluk Programlarına bakın.

1.2 Sunucusuz Mimari. ProcessMind uygulama mantığı AWS Lambda ve AWS tarafından yönetilen hizmetler üzerinde çalışır. ProcessMind, müşteriler tarafından yönetilen uzun ömürlü uygulama sunucularını işletmez; bu da işletim sistemi yama uygulama ve sunucu güçlendirme çalışmalarının büyük bir bölümünü ortadan kaldırır.

1.3 Ağ Sınırları. ProcessMind, veritabanı ve ağ kontrolleri için bir AWS VPC sürdürür. Aurora PostgreSQL, internet çıkışı olmayan özel alt ağlarda çalışır, herkese açık değildir ve VPC akış günlükleri etkinleştirilmiştir. ProcessMind, uygulama Lambda işlevlerini varsayılan olarak VPC içine yerleştirmez. Lambda'lar, IAM ve Secrets Manager kimlik doğrulamasını kullanarak TLS üzerinden AWS RDS Data API aracılığıyla Aurora'ya erişir.

1.4 İçerik Dağıtımı ve Uç Kontrolleri. Müşterilere yönelik web sitesi, frontend SPA ve herkese açık kaynak trafiği Amazon CloudFront üzerinden sunulur. Tüm CloudFront dağıtımları, en düşük TLS politikası olarak TLS 1.2'yi (2021) zorunlu kılar. Web sitesi ve frontend SPA dağıtımları ayrıca HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, referrer policy ve permissions policy dahil olmak üzere güvenlik yanıt başlıkları ekler. Herkese açık kaynaklar dağıtımı, kaynak bucket'ını gizli tutmak için CloudFront Origin Access Control kullanır. Müşterilere yönelik API trafiği Amazon API Gateway üzerinden ayrı olarak işlenir: HTTPS istek/yanıt trafiği özel bir API alt alan adındaki HTTP API üzerinden sunulur ve gerçek zamanlı istemci bağlantıları özel bir WebSocket alt alan adındaki ayrı bir API Gateway WebSocket API üzerinden sunulur.

1.5 Ortamların Ayrıştırılması. Üretim ve geliştirme ortamları ayrı AWS hesapları, ayrı veritabanları ve ayrı altyapı yığınları kullanır. Geliştirici kimlik bilgileri üretim Müşteri Verilerine erişim sağlamaz.

---

2. Veri Şifreleme

2.1 Aktarım Sırasında Şifreleme. İstemciler ile ProcessMind hizmetleri arasında aktarılan tüm veriler TLS 1.2 veya daha yüksek sürüm kullanılarak şifrelenir. Müşterilere yönelik uç noktalar HTTPS üzerinden sunulur. Doğrudan ProcessMind tarafından oluşturulan S3 bucket'ları, SNS konuları ve SQS kuyrukları yalnızca SSL erişimini zorunlu kılar. RDS Data API üzerinden veritabanı erişimi ve diğer AWS hizmet çağrıları HTTPS/TLS kullanır.

2.2 Beklemede Şifreleme. Aurora PostgreSQL, otomatik anahtar döndürme özelliğine sahip müşteri tarafından yönetilen AWS KMS anahtarları kullanılarak beklemede şifrelenir. Doğrudan ProcessMind tarafından oluşturulan müşteri verisi ve operasyonel S3 bucket'ları, yüklemeler, kaynaklar ve erişim günlüğü bucket'ları dahil olmak üzere, müşteri tarafından yönetilen KMS anahtarlarını kullanır. Doğrudan ProcessMind tarafından oluşturulan CloudWatch günlük grupları, SNS konuları ve SQS

kuyrukları da müşteri tarafından yönetilen KMS anahtarlarını kullanır. SST tarafından yönetilen web sitesi ve frontend kaynak bucket'ları, müşteri tarafından yönetilen KMS anahtarları yerine AWS tarafından yönetilen S3 sunucu tarafı şifrelemesini (SSE-S3 / AES-256) kullanır.

2.3 Anahtar Yönetimi ve Gizli Bilgiler. Veritabanı şifreleme anahtarları AWS KMS aracılığıyla merkezi olarak yönetilir ve anahtar erişimi, en az ayrıcalık ilkelerini izleyen IAM politikalarıyla düzenlenir. Veritabanı kimlik bilgileri AWS Secrets Manager'da saklanır. Aurora ana gizli bilgisi ve kısıtlı uygulama kullanıcısı gizli bilgisi her otuz (30) günde bir otomatik olarak döndürülür. Üretim anahtarları ve gizli bilgileri hiçbir zaman kaynak kodunda saklanmaz; yalnızca geliştirmeye özgü kimlik bilgileri üretimden ayrıdır. Bazı AWS/CDK/SST tarafından yönetilen destekleyici kaynaklar, hizmet veya çerçeve müşteri tarafından yönetilen anahtar yapılandırmasını sunmadığında AWS tarafından yönetilen şifrelemeyi kullanmaya devam eder.

---

3. Veri İzolasyonu ve Yerleşimi

3.1 Kiracı İzolasyonu. Her müşteri kiracısına özel, izole bir veritabanı örneği tahsis edilir. Müşteri Verileri veritabanı düzeyinde hiçbir zaman diğer müşterilerin verileriyle karıştırılmaz. Paylaşılan meta veriler (ör. hesap kayıtları, faturalandırma, kullanıcı-kiracı eşleştirmeleri), sıkı erişim kontrollerine sahip ayrı bir çok kiracılı veritabanında saklanır. Kiracı ve kuruluş kapsamındaki paylaşılan tablolar, istek kapsamındaki veritabanı bağlamı aracılığıyla uygulanan PostgreSQL satır düzeyi güvenlik (RLS) politikalarıyla ayrıca korunur.

3.2 Veri Yerleşimi. Veritabanları, dosya yüklemeleri, yedeklemeler ve sorgu sonuçları dahil tüm Müşteri Verileri yalnızca AB'de (Frankfurt, Almanya) saklanır. AEA dışında bulunan bir alt işleyici belirli bir işleme faaliyeti için (örneğin yapay zekâ modeli işleme veya ödeme işleme) görevlendirildiğinde, aktarım Veri İşleme Ekinde açıklanan uygun bir

aktarım mekanizmasıyla güvence altına alınır ve alt işleyici ile işleme konumu Alt İşleyici Listesinde listelenir.

3.3 Veri Saklama ve Silme. Saklama ve silme süreleri Veri İşleme Ekinde Madde 6'da belirtilmiştir. Müşteriler verilerini istedikleri zaman uygulama üzerinden veya ProcessMind ile iletişime geçerek silebilir. Yedek kopyalar, geçerli yedekleme saklama süreleri sona erdikçe kaldırılır (Madde 7.1).

---

4. Kimlik ve Erişim Yönetimi

4.1 Kimlik Doğrulama. ProcessMind, Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC ve LinkedIn OAuth 2.0/OIDC aracılığıyla Single Sign-On (SSO) desteği sunar. ProcessMind, güvenen taraf olarak hareket eder ve kullanıcı parolalarını saklamaz. Çok faktörlü kimlik doğrulama, kimlik sağlayıcısı tarafından zorunlu kılınır — örneğin bir kuruluş Microsoft Entra ID'yi (Azure AD) bağladığında, o kuruluşun kendi MFA ve erişim politikaları uygulanır.

4.2 Oturum Yönetimi. Tarayıcı oturumları, SameSite ve Secure bayraklarına sahip güvenli, HttpOnly çerezler üzerinden iletilen imzalı JSON Web Token'ları (JWT) kullanır. Belirteç imzaları, kimlik doğrulaması yapılmış her istekte doğrulanır.

4.3 Yetkilendirme Modeli. ProcessMind, temel uygulama API'leri için API Gatewayin yerel yetkilendiricilerine dayanmaz. Yetkilendirme, iş mantığı çalıştırılmadan önce oturum durumunu ve kiracı kapsamını doğrulayan paylaşılan Lambda işleyici sarmalayıcılarında uygulanır. Genel rotalar, kimlik doğrulaması gerektirmeyen akışlar, webhooks, olay alımı ve CORS preflight için açıkça izin listesine alınır. Harici API uç noktaları özel kimlik doğrulama işleyicileri kullanır. Customer Data'ya erişim, kimliği doğrulanmış kiracı veya kuruluş bağlamıyla sınırlandırılır.

4.4 En Az Ayrıcalık. Dahili sistemler en az ayrıcalık ilkesini izler. Çerçeve kesin kapsamlandırmaya izin verdiğinde IAM rolleri gereken asgari kaynaklarla sınırlandırılır. Bazı SST/CDK tarafından oluşturulan roller,

bağlamalar ve çalışma zamanı işlemleri için daha geniş yönetilen veya satır içi politikalar kullanır; bu durumlar gözden geçirilir, mümkün olduğunda kaynak kapsamına alınır ve açık istisnalar olarak izlenir.

4.5 Çalışan Erişim Kontrolleri. Çalışanların dahili sistemlere erişimi, SSO ve zorunlu MFA ile Active Directory üzerinden yönetilir. Rol tabanlı erişim kontrolü (RBAC), Müşteri Verilerine erişimin bilmesi gereken esasına göre yetkili personelle sınırlı olmasını sağlar. Erişim hakları periyodik olarak gözden geçirilir.

---

5. Günlük Kaydı, İzleme ve Denetim

5.1 Merkezi Günlük Kaydı. HTTP API erişim günlük kaydı ve WebSocket erişim günlük kaydı, yapılandırılmış JSON alanlarıyla etkinleştirilir ve bir (1) hafta saklama süresiyle Amazon CloudWatch Logs'a yazılır. Bu erişim günlük grupları müşteri tarafından yönetilen bir AWS KMS anahtarıyla şifrelenir. Uygulama günlükleri, müşteri tarafından yönetilen bir AWS KMS anahtarıyla şifrelenen Amazon CloudWatch günlük gruplarında merkezileştirilir ve on (10) yıl saklanır. Ayrı denetim ve telemetri günlük grupları da müşteri tarafından yönetilen bir AWS KMS anahtarıyla şifrelenir ve on (10) yıl saklanır. Aurora PostgreSQL motor günlük dışa aktarma grubu bir (1) hafta saklanır.

5.2 Neler Günlüğe Kaydedilir ve Neler Kaydedilmez. ProcessMind, istek zamanı, istek tanımlayıcıları, rota veya yol, yanıt durumu, gecikme, kaynak IP'si ve kullanıcı aracısı dahil olmak üzere HTTP API ve WebSocket erişim olaylarını günlüğe kaydeder. ProcessMind ayrıca kimlik doğrulama olaylarını, eşzamansız hata yollarını ve destekleyici Lambda uygulama faaliyetlerini merkezi CloudWatch günlük gruplarına kaydeder. VPC akış günlükleri etkinleştirilmiştir. ProcessMind şu anda web sitesi, frontend SPA veya herkese açık kaynaklar dağıtımları üzerinde CloudFront standart erişim günlük kaydını etkinleştirmemektedir.

5.3 İzleme ve Uyarı. CloudWatch alarmları ve panoları sistem durumunu, ölü mektup kuyruklarını ve güvenlikle ilgili hataları izler. Eşzamansız işleme

hataları şifrelenmiş ölü mektup kuyruklarına yönlendirilir (on dört (14) gün saklama; küçük resim ve arama dizini kuyrukları için iki (2) gün) ve DLQ alarmları inceleme amacıyla SNS bildirimlerini tetikler. Ayrıca ProcessMind, gerçek zamanlı frontend hata izleme, performans izleme ve oturum yeniden oynatma için Sentry kullanır. Oturum yeniden oynatmaları yalnızca hata oluşan oturumlar için kaydedilir ve metin, form girdileri ve medya yeniden oynatmalarda maskelenir veya engellenir. Sentry verileri AB'de (Frankfurt) alınır ve ProcessMind Kullanım Verileriyle (tarayıcı hataları, performans izleri, cihaz meta verileri ve maskelenmiş yeniden oynatma kayıtları) sınırlıdır. Sentry, alt işleyici listesinde listelenir.

5.4 Günlük Koruması. Günlükler, özel ve erişim kontrollü CloudWatch günlük gruplarında saklanır ve beklemede şifrelenir. Üretim ve geliştirme günlükleri ortam ve hesap sınırlarıyla ayrılır.

---

6. Otomatik Kontrol Doğrulaması ve Güvenlik Açığı Yönetimi

6.1 ProcessMind'ın Yaptıkları. ProcessMind, birden fazla sektör kural paketi (AWS Solutions, NIST 800-53 ve PCI DSS dahil) kullanarak altyapı sentezi ve dağıtım iş akışının bir parçası olarak `cdk-nag` çalıştırır. Yığın bazında raporlar oluşturulur ve altyapı değişiklik yönetiminin bir parçası olarak incelenir. Bulgular düzeltilmiş, kabul edilmiş risk veya planlanan iyileştirme olarak sınıflandırılır.

6.2 İstisnalar Nasıl Yönetilir. Bastırmalar, çerçevenin izin verdiği durumlarda merkezi bir kayıt defterine kaydedilir, etkilenen yığınlarla sınırlandırılır ve yazılı gerekçe gerektirir; bir yığın satır içi bastırma içerdiğinde, bu bastırma ilgili yığının yanında belgelenir. Bir bulgu giderildiğinde, ilgili bastırma güncellenir veya kaldırılır. ProcessMind, bastırmayı incelemeden genel bir muafiyet olarak değerlendirmez.

6.3 ProcessMind'ın Şu Anda Yapmadıkları. ProcessMind, esaslı altyapı kontrolü istisnalarını izler ve inceler. Başlıca istisnalar şunlardır:

- application Lambdas varsayılan olarak VPC içine yerleştirilmez; Aurora'ya TLS üzerinden RDS Data API aracılığıyla IAM ve Secrets Manager kimlik doğrulaması kullanılarak erişir
- WebSocket API ve statik dağıtımlar AWS WAF'ın arkasında değildir (WebSocket bağlantıları kısa ömürlü HMAC token'ları kullanır; ödemeyle ilgili coğrafi kısıtlamalar ödeme sisteminde uygulanır) ve statik dağıtımlarda CloudFront standart erişim günlüğü kaydı bulunmaz
- veritabanı kurtarma, ayrı bir AWS Backup planı veya Aurora Enhanced Monitoring yerine Aurora otomatik yedeklemelerine ve belirli bir zamana geri yüklemeye dayanır
- değiştirilebilir bucket'lar için bölgeler arası S3 replikasyonu veya S3 Object Lock bulunmaz
- bazı AWS/CDK/SST tarafından yönetilen destekleyici kaynaklar, hizmetin müşteri tarafından kontrol edilen bir alternatif sunmadığı durumlarda AWS tarafından yönetilen şifrelemeyi veya daha geniş kapsamlı oluşturulmuş IAM politikalarını kullanır

Eksiksiz bastırma kaydı altyapı koduyla birlikte tutulur ve talep üzerine sunulur. `cdk-nag` kural paketlerinin kullanılması, harici bir sertifikasyon, denetim görüşü veya HIPAA, NIST ya da PCI DSS uyumluluğuna ilişkin hukuki bir tasdik değil, mühendislik kontrol doğrulamasıdır.

6.4 Bağımlılık Yönetimi. Yazılım bağımlılıkları bilinen güvenlik açıkları bakımından sürekli olarak izlenir. Kritik ve yüksek önem dereceli güvenlik açıkları, yedi (7) gün hedefiyle yamalanır. Bağımlılıklar düzenli bir döngü kapsamında güncellenir.

6.5 Güvenli Yazılım Geliştirme Yaşam Döngüsü (SDLC). ProcessMind, yazılım geliştirmede savunma derinliği yaklaşımını izler. Üretime yönelik her değişiklik, dağıtımdan önce birden çok bağımsız otomatik doğrulama katmanından geçmelidir:

- **Statik analiz ve tür güvenliği:** TypeScript strict mode ve ESLint, derleme zamanında tür doğruluğunu, null güvenliğini ve güvenlikle

ilgili kodlama kalıplarını zorunlu kılar.

- **Yapay zekâ destekli kod incelemesi:** Yapay zekâ destekli analiz, otomatik testleri tamamlayarak güvenlik risklerini, mantık hatalarını ve kurallardan sapmaları belirlemek üzere pull request'ler hakkında ek bir inceleme perspektifi sağlar.
- **Birim ve entegrasyon testleri:** kapsamlı bir Vitest test paketi, geliştirme ortamındaki canlı AWS kaynaklarına karşı iş mantığını, veri erişim kalıplarını, API davranışını ve hata işlemeyi doğrular.
- **Uçtan uca testler:** Playwright tabanlı tarayıcı testleri; kimlik doğrulama, veri yükleme, süreç modelleme, simülasyon ve çok kiracılı izolasyon dâhil olmak üzere kritik kullanıcı iş akışlarını doğrular.
- **Altyapı uyumluluğu taraması:** `cdk-nag` her değişiklikte altyapı kodunu birden çok uyumluluk çerçevesine göre doğrular.
- **Bağımlılık güvenlik açığı taraması:** otomatik bağımlılık denetimleri, bilinen kritik ve yüksek önem dereceli güvenlik açıklarının üretime ulaşmasını engeller.

İnsan incelemesi, satır düzeyinde kod denetiminden ziyade mimariye, güvenlik sınırlarına ve tasarım düzeyindeki kararlara odaklanır. Yapısal, güvenlikle hassas veya altyapıyla ilgili değişikliklerin söz konusu olduğu durumlarda, otomatik doğrulamaya ek olarak açık insan onayı gerekir.

Tüm doğrulama katmanları, ana dala yönelik değişiklikler için gerekli birleştirme kapıları olarak CI üzerinden uygulanır. Acil üretim düzeltmeleri CI kapısını atlayabilir; ancak bunların ardından yirmi dört (24) saat içinde eksiksiz bir işlem hattı çalıştırılmalı ve olay sonrası inceleme yapılmalıdır.

---

7. Yedekleme ve Felaket Kurtarma

7.1 Otomatik Yedeklemeler. Amazon Aurora, yedi (7) günlük saklama süresiyle sürekli ve otomatik yedeklemeler gerçekleştirir. Yedeklemeler, kaynak veritabanlarıyla aynı müşteri tarafından yönetilen KMS anahtarları kullanılarak şifrelenir.

7.2 Belirli Bir Zamana Geri Yükleme. Aurora, yedekleme saklama süresi içindeki herhangi bir saniyeye belirli bir zamana geri yüklemeyi destekler ve veri bozulması veya yanlışlıkla silinme durumunda hızlı geri yüklemeyi mümkün kılar.

7.3 S3 Dayanıklılığı ve Sürüm Oluşturma. Dosya yüklemeleri ve operasyonel yapıtlar, %99,999999999 (11 dokuz) dayanıklılık sağlayan Amazon S3'te saklanır. Kurtarma ve geri alma işlemlerini desteklemek üzere yükleme bucket'ında ve kaynak bucket'larında sürüm oluşturma etkinleştirilmiştir. Web sitesi ve frontend dağıtım bucket'ları yeniden üretilebilir derleme yapıtlarıdır ve yedekleme sistemi olarak değerlendirilmez. ProcessMind şu anda bölgeler arası S3 replikasyonunu etkinleştirmemektedir.

7.4 İş Sürekliliği. Felaket kurtarma prosedürleri belgelenir ve periyodik olarak test edilir. Bir özet, Felaket Kurtarma, İş Sürekliliği ve Olay Müdahalesi belgesinde sunulmaktadır. Mimari, AWS'nin birden çok Availability Zone genelinde işlettiği `eu-central-1` bölgesindeki AWS tarafından yönetilen hizmetlere dayanır; Aurora kümesi şu anda tek bir yazıcı örneği çalıştırdığından, veritabanı kurtarma bölge içi bir yedek sunucu yerine otomatik yedeklemelere ve belirli bir zamana geri yüklemeye dayanır. Aurora yedeklemeleri, S3 dayanıklılığı, dead-letter kuyrukları ve kaynaktan yeniden oluşturulan statik varlıklar kurtarma stratejisinin parçasıdır.

---

8. Olay Müdahalesi

8.1 Olay Bildirimi. Bir Güvenlik Olayı (DPA'da tanımlandığı üzere) meydana gelmesi durumunda ProcessMind, etkilenen müşterileri gereksiz gecikme olmaksızın ve mümkün olduğu durumlarda olaydan haberdar olmasından itibaren yetmiş iki (72) saat içinde bilgilendirir.

8.2 Olayların Ele Alınması. ProcessMind; tanımlama, sınırlama, ortadan kaldırma, kurtarma ve olay sonrası incelemeyi kapsayan belgelenmiş olay müdahalesi prosedürlerini sürdürür. Bir özet, Felaket Kurtarma, İş Sürekliliği

ve Olay Müdahalesi belgesinde sunulmaktadır. Olaylardan çıkarılan dersler güvenlik kontrollerine ve süreçlerine dâhil edilir.

8.3 İletişim. Olay bildirimleri olayın niteliğini ve kapsamını, etkilenen veri kategorilerini, olayı sınırlamak için alınan önlemleri ve müşteri için önerilen eylemleri içerir.

---

9. Organizasyonel Önlemler

9.1. Bilgi Güvenliği Yönetimi. ProcessMind, ISO 27001 ilkeleriyle uyumlu bir bilgi güvenliği yönetim sistemi sürdürür. ProcessMind, ISO 27001 sertifikasyonu ve SOC 2 Type II tasdiki için sertifikasyon yolunu seçmiştir; resmî sertifikasyon süreci henüz başlamamıştır.

9.2 Güvenlik Farkındalığı. Müşteri Verilerine erişimi olan tüm personel güvenlik farkındalığı eğitimi alır. Güvenlik en iyi uygulamaları işe alıştırma sürecine, geliştirme iş akışlarına ve operasyonel prosedürlere dâhil edilmiştir.

9.3 Tedarikçi ve Alt İşleyen Yönetimi. Alt işleyenler, bu belgede açıklananlara eşdeğer veri koruma standartlarına sözleşmeyle bağlıdır. ProcessMind, herkese açık bir alt işleyen listesi tutar ve yeni bir alt işleyenle çalışmaya başlamadan en az otuz (30) gün önce bildirimde bulunur. Alt işleyenler uyumluluk bakımından yıllık olarak incelenir.

9.4 Gizlilik. Müşteri Verilerini işlemeye yetkili tüm personel yazılı gizlilik yükümlülüklerine tabidir.

---

10. Uyumluluk ve Sertifikasyonlar

Çerçeve / Standart	Durum
GDPR (AB Genel Veri Koruma Tüzüğü)	Uyumlu
AB Veri Yerleşikliği (Frankfurt, Almanya)	Uygulanıyor

Çerçeve / Standart	Durum
AWS Altyapı Sertifikasyonları (ISO 27001, SOC 2, PCI DSS)	AWS aracılığıyla devralınmıştır
ISO 27001 (ProcessMind)	Planlanıyor — sertifikasyon yolu seçildi; resmî süreç henüz başlamadı
SOC 2 Type II (ProcessMind)	Planlanıyor — sertifikasyon yolu seçildi; resmî süreç henüz başlamadı
Otomatik altyapı kontrol doğrulaması (`cdk-nag` AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless genelinde)	Sertifikasyon olarak değil, mühendislik kontrol doğrulaması olarak uygulanmaktadır
Uluslararası transferler için Standart Sözleşme Hükümleri (SCC'ler)	Uygulanmaktadır (bkz. DPA)
Veri İşleme Eki (DPA)	Herkese açık

`cdk-nag` Kural paketlerinin kullanılması, ProcessMind'in HIPAA, NIST veya PCI DSS kapsamında resmen sertifikalandırıldığı veya bağımsız olarak denetlendiği anlamına gelmez. Bu kural paketleri, altyapı tasarımını doğrulamak ve açıkları açıkça takip etmek için mühendislik korumaları olarak kullanılır.

Güvenlik, uyumluluk veya denetim raporları ya da doldurulmuş güvenlik anketleri gibi belgeleri talep etmekle ilgili sorularınız için **support@processmind.com** adresiyle iletişime geçin.