

ProcessMind 보안 조치

발효일: 2026년 9월 14일

본 문서는 ProcessMind B.V.가 고객 데이터의 기밀성, 무결성 및 가용성을 보호하기 위해 유지하는 기술적 및 조직적 조치("TOM")를 설명합니다. ProcessMind는 여러 개의 독립적인 보안 계층이 네트워크 및 인프라부터 신원, 권한 부여, 데이터 격리, 암호화, 모니터링 및 소프트웨어 개발에 이르기까지 모든 수준에서 고객 데이터를 보호하는 심층 방어 접근 방식을 따릅니다. 이러한 조치는 [데이터 처리 부속서](#), [개인정보 처리방침](#) 및 [SaaS 호스팅 정책](#)을 보완합니다. ProcessMind는 이러한 조치를 최소 매년 검토하고 업데이트합니다.

고객 데이터는 제3자에게 판매되거나 공유되지 않으며, 제3자가 자체 목적으로 사용하지 않습니다.

1. 인프라 보안

1.1 클라우드 플랫폼. ProcessMind는 EU(독일 프랑크푸르트, eu-central-1)의 Amazon Web Services(AWS)에서만 호스팅됩니다. AWS는 ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 및 PCI DSS 인증을 보유하고 있습니다. 전체 목록은 [AWS 규정 준수 프로그램](#)을 참조하시기 바랍니다.

1.2 서버리스 아키텍처. ProcessMind 애플리케이션 로직은 AWS Lambda 및 AWS 관리형 서비스에서 실행됩니다. ProcessMind는 고객이 관리하는 장기 실행 애플리케이션 서버를 운영하지 않으므로, 운영 체제 패치 및 서버 강화 작업의 상당 부분이 필요하지 않습니다.

1.3 네트워크 경계. ProcessMind는 데이터베이스 및 네트워크 통제를 위해 AWS VPC를 유지합니다. Aurora PostgreSQL은 인터넷 송신이 차단된 프라이빗 서브넷에서 실행되고 공개적으로 접근할 수 없으며, VPC 흐름 로그가 활성화되어 있습니다. ProcessMind는 기본적으로 애플리케이션 Lambda 함수를 VPC 내부에 배치하지 않습니다. Lambda는 IAM 및 Secrets Manager 인증을 사용하여 TLS를 통해 AWS RDS Data API로 Aurora에 접근합니다.

1.4 콘텐츠 전송 및 엣지 제어. 고객 대상 웹사이트, 프런트엔드 SPA 및 공개 리소스 트래픽은 Amazon CloudFront를 통해 제공됩니다. 모든 CloudFront 배포에는 TLS 1.2(2021)의 최소 TLS 정책이 적용됩니다. 웹사이트 및 프런트엔드 SPA 배포에는 HTTP Strict Transport Security(HSTS), Content Security Policy(CSP), frame-ancestors

'none', X-Frame-Options: DENY, X-Content-Type-Options, 리퍼러 정책 및 권한 정책을 포함한 보안 응답 헤더도 추가됩니다. 공개 리소스 배포에서는 CloudFront Origin Access Control을 사용하여 오리진 버킷을 비공개로 유지합니다. 고객 대상 API 트래픽은 Amazon API Gateway를 통해 별도로 처리됩니다. HTTPS 요청/응답 트래픽은 전용 API 하위 도메인의 HTTP API를 통해 제공되며, 실시간 클라이언트 연결은 전용 WebSocket 하위 도메인의 별도 API Gateway WebSocket API를 통해 제공됩니다.

1.5 환경 분리. 프로덕션 및 개발 환경은 별도의 AWS 계정, 별도의 데이터베이스 및 별도의 인프라 스택을 사용합니다. 개발자 자격 증명으로는 프로덕션 고객 데이터에 접근할 수 없습니다.

2. 데이터 암호화

2.1 전송 중 암호화. 클라이언트와 ProcessMind 서비스 간에 전송되는 모든 데이터는 TLS 1.2 이상을 사용하여 암호화됩니다. 고객 대상 엔드포인트는 HTTPS를 통해 제공됩니다.

ProcessMind가 직접 생성한 S3 버킷, SNS 주제 및 SQS 대기열에는 SSL 전용 접근이 적용됩니다. RDS Data API를 통한 데이터베이스 접근 및 기타 AWS 서비스 호출에는 HTTPS/TLS가 사용됩니다.

2.2 저장 데이터 암호화. Aurora PostgreSQL은 자동 키 교체가 적용되는 고객 관리형 AWS KMS 키를 사용하여 저장 시 암호화됩니다. 업로드, 리소스 및 접근 로그 버킷을 포함하여 ProcessMind가 직접 생성한 고객 데이터 및 운영용 S3 버킷은 고객 관리형 KMS 키를 사용합니다. ProcessMind가 직접 생성한 CloudWatch 로그 그룹, SNS 주제 및 SQS 대기열도 고객 관리형 KMS 키를 사용합니다. SST 관리형 웹사이트 및 프론트엔드 오리진 버킷은 고객 관리형 KMS 키 대신 AWS 관리형 S3 서버 측 암호화(SSE-S3 / AES-256)를 사용합니다.

2.3 키 관리 및 비밀 정보. 데이터베이스 암호화 키는 AWS KMS를 통해 중앙에서 관리되며, 키 접근은 최소 권한 원칙에 따른 IAM 정책으로 통제됩니다. 데이터베이스 자격 증명은 AWS Secrets Manager에 저장됩니다. Aurora 마스터 비밀 정보와 제한된 애플리케이션 사용자 비밀 정보는 30일마다 자동으로 교체됩니다. 프로덕션 키와 비밀 정보는 소스 코드에 저장되지 않으며, 개발 전용 자격 증명은 프로덕션 환경과 분리됩니다. 일부 AWS/CDK/SST 관리형 지원 리소스는 서비스 또는 프레임워크에서 고객 관리형 키 구성을 제공하지 않는 경우 AWS 관리형 암호화를 계속 사용합니다.

3. 데이터 격리 및 데이터 상주

3.1 테넌트 격리. 각 고객 테넌트에는 전용 격리 데이터베이스 인스턴스가 제공됩니다. 데이터베이스 수준에서 고객 데이터는 다른 고객의 데이터와 절대 혼합되지 않습니다. 공유 메타 데이터(예: 계정 기록, 청구 정보, 사용자와 테넌트 간 매핑)는 엄격한 접근 통제가 적용되는 별도의 멀티테넌트 데이터베이스에 저장됩니다. 테넌트 및 조직 범위의 공유 테이블은 요청 범위 데이터베이스 컨텍스트를 통해 적용되는 PostgreSQL 행 수준 보안(RLS) 정책으로 추가 보호됩니다.

3.2 데이터 상주. 데이터베이스, 파일 업로드, 백업 및 쿼리 결과를 포함한 모든 고객 데이터는 EU(독일 프랑크푸르트)에만 저장됩니다. 특정 처리 활동(예: AI 모델 처리 또는 결제 처리)을 위해 EEA 외부에 소재한 하위 처리자를 이용하는 경우, 데이터 이전은 데이터 처리 부속서에 설명된 적절한 이전 메커니즘에 따라 이루어지며, 해당 하위 처리자 및 처리 위치는 하위 처리자 목록에 기재됩니다.

3.3 데이터 보존 및 삭제. 보존 및 삭제 일정은 [데이터 처리 부속서](#) 제6조에 명시되어 있습니다. 고객은 애플리케이션을 통해 언제든지 데이터를 삭제하거나 ProcessMind에 연락하여 삭제를 요청할 수 있습니다. 백업 사본은 해당 백업 보존 기간이 만료되면 제거됩니다(제7.1조).

4. 신원 및 접근 관리

4.1 인증. ProcessMind는 Microsoft Entra ID(Azure AD), Google OAuth 2.0/OIDC 및 LinkedIn OAuth 2.0/OIDC를 통한 Single Sign-On(SSO)을 지원합니다.

ProcessMind는 신뢰 당사자로 기능하며 사용자 비밀번호를 저장하지 않습니다. 다중 인증은 신원 제공자가 적용합니다. 예를 들어 조직이 Microsoft Entra ID(Azure AD)를 연결하는 경우 해당 조직 자체의 MFA 및 접근 정책이 적용됩니다.

4.2 세션 관리. 브라우저 세션은 SameSite 및 Secure 플래그가 설정된 보안 HttpOnly 쿠키를 통해 전송되는 서명된 JSON Web Token(JWT)을 사용합니다. 인증된 각 요청에서 토큰 서명을 검증합니다.

4.3 권한 부여 모델. ProcessMind는 핵심 애플리케이션 API에 API Gateway 기본 권한 부여자를 사용하지 않습니다. 비즈니스 로직이 실행되기 전에 세션 상태와 테넌트 범위를 검증하는 공유 Lambda 핸들러 래퍼를 통해 권한 부여를 적용합니다. 공개 경로는 인증되지 않은 흐름, 웹훅, 이벤트 수집 및 CORS 사전 요청을 위해 명시적으로 허용 목록에 등록됩니다.

다. 외부 API 엔드포인트는 전용 인증 핸들러를 사용합니다. 고객 데이터에 대한 액세스는 인증된 테넌트 또는 조직 컨텍스트로 범위가 제한됩니다.

4.4 최소 권한. 내부 시스템에는 최소 권한 원칙이 적용됩니다. 프레임워크에서 정확한 범위 지정이 가능한 경우 IAM 역할은 필요한 최소 리소스로 범위가 제한됩니다. 일부 SST/CDK 생성 역할은 바인딩 및 런타임 운영을 위해 더 광범위한 관리형 또는 인라인 정책을 사용합니다. 이러한 사례는 검토하고, 가능한 경우 리소스 범위를 제한하며, 명시적인 예외로 추적합니다.

4.5 직원 접근 통제. 내부 시스템에 대한 직원 접근은 SSO 및 의무적 MFA가 적용되는 Active Directory를 통해 관리됩니다. 역할 기반 접근 통제(RBAC)를 통해 고객 데이터에 대한 접근을 알 필요가 있는 승인된 인원으로 제한합니다. 접근 권한은 정기적으로 검토됩니다.

5. 로깅, 모니터링 및 감사

5.1 중앙 집중식 로깅. HTTP API 접근 로깅 및 WebSocket 접근 로깅은 구조화된 JSON 필드를 사용하여 활성화되며 Amazon CloudWatch Logs에 기록되고 1년간 보존됩니다. 해당 접근 로그 그룹은 고객 관리형 AWS KMS 키로 암호화됩니다. 애플리케이션 로그는 고객 관리형 AWS KMS 키로 암호화된 Amazon CloudWatch 로그 그룹에 중앙 집중식으로 저장되며 10년간 보존됩니다. 별도의 감사 및 원격 측정 로그 그룹도 고객 관리형 AWS KMS 키로 암호화되며 10년간 보존됩니다. Aurora PostgreSQL 엔진 로그 내보내기 그룹은 1주일간 보존됩니다.

5.2 기록되는 항목과 기록되지 않는 항목. ProcessMind는 요청 시간, 요청 식별자, 경로 또는 패스, 응답 상태 및 지연 시간 등 HTTP API 및 WebSocket 접근 이벤트를 기록합니다. 접근 로그에는 호출자의 소스 IP 주소나 사용자 에이전트가 포함되지 않습니다.

ProcessMind는 인증 이벤트, 비동기 실패 경로 및 지원 Lambda 애플리케이션 활동도 중앙 집중식 CloudWatch 로그 그룹에 기록합니다. VPC 흐름 로그가 활성화되어 있습니다. ProcessMind는 현재 웹사이트, 프런트엔드 SPA 또는 공개 리소스 배포에 CloudFront 표준 접근 로깅을 활성화하지 않습니다.

5.3 모니터링 및 경고. CloudWatch 경고 및 대시보드는 시스템 상태, 배달 못한 메시지 대기열 및 보안 관련 실패를 모니터링합니다. 비동기 처리 실패는 암호화된 배달 못한 메시지 대기열로 전달되며(보존 기간 14일, 썸네일 및 검색 인덱스 대기열은 2일), DLQ 경보는 조사

를 위한 SNS 알림을 발생시킵니다. 또한 ProcessMind는 실시간 프론트엔드 오류 추적, 성능 모니터링 및 세션 재생을 위해 Sentry를 사용합니다. 세션 재생은 오류가 발생한 세션에 대해서만 기록되며, 재생 시 텍스트, 양식 입력 및 미디어는 마스킹되거나 차단됩니다.

Sentry 데이터는 EU(프랑크푸르트)에서 수집되며 ProcessMind 사용 데이터(브라우저 오류, 성능 추적, 기기 메타데이터 및 마스킹된 재생 기록)로 제한됩니다. Sentry는 [하위 처리자 목록](#)에 기재되어 있습니다.

5.4 로그 보호. 로그는 전용 접근 통제 CloudWatch 로그 그룹에 저장되고 저장 시 암호화됩니다. 프로덕션 로그와 개발 로그는 환경 및 계정 경계를 기준으로 분리됩니다.

6. 자동화된 통제 검증 및 취약성 관리

6.1 ProcessMind가 수행하는 사항. ProcessMind는 여러 업계 규칙 팩(AWS Solutions, NIST 800-53 및 PCI DSS 포함)을 사용하여 인프라 합성 및 배포 워크플로의 일부로 cdk-nag를 실행합니다. 스택별 보고서는 인프라 변경 관리의 일부로 생성 및 검토됩니다. 발견 사항은 수정, 위험 수용 또는 개선 계획으로 분류됩니다.

6.2 예외 관리 방법. 프레임워크에서 허용하는 경우 억제 항목은 중앙 등록부에 기록되고 영향을 받는 스택으로 범위가 제한되며 서면 근거가 필요합니다. 스택에 인라인 억제 항목이 포함된 경우 해당 스택과 함께 문서화됩니다. 발견 사항이 해결되면 해당 억제 항목을 업데이트하거나 제거합니다. ProcessMind는 억제를 검토에서 일괄적으로 제외하는 수단으로 취급하지 않습니다.

6.3 ProcessMind가 현재 수행하지 않는 사항. ProcessMind는 중요한 인프라 통제 예외를 추적하고 검토합니다. 주요 예외는 다음과 같습니다:

- 애플리케이션 Lambda는 기본적으로 VPC 내부에 배치되지 않습니다. IAM 및 Secrets Manager 인증을 사용하여 TLS를 통해 RDS Data API로 Aurora에 연결합니다
- 서비스의 어떤 부분도 AWS WAF로 보호되지 않습니다. AWS WAF는 API Gateway HTTP API를 지원하지 않으며, 나머지 진입점도 WAF로 보호되지 않습니다(WebSocket 연결은 단기간 유효한 HMAC 토큰을 사용하고, 결제 관련 지역 제한은 결제 시스템에서 적용됩니다). 정적 배포에는 CloudFront 표준 액세스 로깅도 설정되어 있지 않습니다

- 데이터베이스 복구는 별도의 AWS Backup 계획이나 Aurora Enhanced Monitoring이 아니라 Aurora 자동 백업 및 특정 시점 복구에 의존합니다
- 변경 가능한 버킷에는 리전 간 S3 복제 또는 S3 Object Lock이 없습니다
- 일부 AWS/CDK/SST 관리 지원 리소스는 서비스에서 고객이 제어할 수 있는 대안을 제공하지 않는 경우 AWS 관리형 암호화 또는 더 광범위하게 생성된 IAM 정책을 사용합니다

전체 억제 등록부는 인프라 코드와 함께 유지되며 요청 시 제공됩니다. cdk-nag 규칙 팩의 사용은 엔지니어링 통제 검증이며, HIPAA, NIST 또는 PCI DSS 준수에 대한 외부 인증, 감사 의견 또는 법적 확인이 아닙니다.

6.4 종속성 관리. 소프트웨어 종속성은 알려진 취약성이 있는지 지속적으로 모니터링됩니다. 심각 및 높은 심각도의 취약성은 7일 이내 패치를 목표로 합니다. 종속성은 정기적인 주기에 따라 업데이트됩니다.

6.5 보안 소프트웨어 개발 수명 주기(SDLC). ProcessMind는 소프트웨어 개발에 심층 방어 접근 방식을 적용합니다. 프로덕션에 적용되는 모든 변경 사항은 배포 전에 여러 개의 독립적인 자동 검증 계층을 통과해야 합니다:

- **정적 분석 및 타입 안전성:** TypeScript 엄격 모드와 ESLint는 컴파일 시 타입 정확성, null 안전성 및 보안 관련 코딩 패턴을 적용합니다.
- **AI 지원 코드 검토:** AI 지원 분석은 풀 리퀘스트에 대한 추가 검토 관점을 제공하여 자동화된 테스트를 보완하고 보안 위험, 로직 오류 및 규칙 위반을 식별합니다.
- **단위 및 통합 테스트:** 포괄적인 Vitest 테스트 모음은 개발 환경의 실제 AWS 리소스를 대상으로 비즈니스 로직, 데이터 접근 패턴, API 동작 및 오류 처리를 검증합니다.
- **엔드투엔드 테스트:** Playwright 기반 브라우저 테스트는 인증, 데이터 업로드, 프로세스 모델링, 시뮬레이션 및 멀티테넌트 격리를 포함한 핵심 사용자 워크플로를 검증합니다.
- **인프라 규정 준수 검사:** cdk-nag는 모든 변경 사항에 대해 여러 규정 준수 프레임워크를 기준으로 인프라 코드(IaC)를 검증합니다.
- **종속성 취약성 검사:** 자동화된 종속성 감사는 알려진 심각 및 높은 심각도의 취약성이 프로덕션에 반영되지 않도록 차단합니다.

사람의 검토는 코드의 각 줄을 검사하기보다 아키텍처, 보안 경계 및 설계 수준의 결정에 중점을 둡니다. 구조적 변경, 보안에 민감한 변경 또는 인프라 변경이 포함되는 경우 자동 검증 외에 명시적인 사람의 승인이 필요합니다.

모든 검증 계층은 메인 브랜치에 대한 애플리케이션 및 인프라 변경의 필수 병합 게이트로 CI를 통해 적용됩니다. 웹사이트 콘텐츠 및 정적 자산 릴리스는 애플리케이션 CI 게이트가 아니라 배포 시 법률 문서의 최신 여부를 자동으로 확인하는 검사를 포함한 별도의 문서화된 릴리스 절차를 따릅니다. 긴급 프로덕션 수정은 CI 게이트를 우회할 수 있지만, 24시간 이내에 전체 파이프라인 실행 및 사고 후 검토를 수행해야 합니다.

7. 백업 및 재해 복구

7.1 자동 백업. Amazon Aurora는 7일의 보존 기간으로 지속적인 자동 백업을 수행합니다. 백업은 원본 데이터베이스와 동일한 고객 관리형 KMS 키를 사용하여 암호화됩니다.

7.2 특정 시점 복구. Aurora는 백업 보존 기간 내의 임의의 시점으로 복구할 수 있으므로 데이터 손상 또는 실수로 인한 삭제가 발생한 경우 신속하게 복원할 수 있습니다.

7.3 S3 내구성 및 버전 관리. 파일 업로드 및 운영 아티팩트는 99.999999999%(11개의 9)의 내구성을 제공하는 Amazon S3에 저장됩니다. 복구 및 롤백을 지원하기 위해 업로드 버킷과 리소스 버킷에서 버전 관리가 활성화되어 있습니다. 웹사이트 및 프런트엔드 배포 버킷은 재현 가능한 빌드 아티팩트이며 백업 시스템으로 취급되지 않습니다. ProcessMind는 현재 리전 간 S3 복제를 활성화하지 않습니다.

7.4 업무 연속성. 재해 복구 절차는 문서화되어 있으며 정기적으로 테스트됩니다. 요약은 [재해 복구, 업무 연속성 및 사고 대응](#) 문서에서 확인할 수 있습니다. 아키텍처는 eu-central-1 리전 내 AWS 관리형 서비스에 의존하며, AWS는 해당 서비스를 여러 가용 영역에 걸쳐 운영합니다. Aurora 클러스터는 현재 단일 쓰기 인스턴스로 실행되므로 데이터베이스 복구는 리전 내 대기 인스턴스가 아니라 자동 백업 및 특정 시점 복구에 의존합니다. Aurora 백업, S3 내구성, 배달 못한 메시지 대기열 및 소스에서 다시 빌드하는 정적 자산은 복구 전략의 일부입니다.

8. 사고 대응

8.1 사고 통지. DPA에 정의된 보안 사고가 발생한 경우 ProcessMind는 부당한 지체 없이, 가능한 경우 사고를 인지한 시점부터 72시간 이내에 영향을 받는 고객에게 통지합니다.

8.2 사고 처리. ProcessMind는 식별, 억제, 제거, 복구 및 사고 후 검토를 다루는 문서화된 사고 대응 절차를 유지합니다. 요약은 [재해 복구, 업무 연속성 및 사고 대응](#) 문서에서 확인할

수 있습니다. 사고에서 얻은 교훈은 보안 통제 및 절차에 반영됩니다.

8.3 의사소통. 사고 통지에는 사고의 성격과 범위, 영향을 받은 데이터 범주, 사고 억제를 위해 취한 조치 및 고객에게 권고되는 조치가 포함됩니다.

9. 조직적 조치

9.1. 정보 보안 관리. ProcessMind는 ISO 27001 원칙에 부합하는 정보 보안 관리 시스템을 유지합니다. ProcessMind는 ISO 27001 인증 및 SOC 2 Type II 인증 보고서 취득을 위한 인증 경로를 선정했으나, 공식 인증 절차는 아직 시작되지 않았습니다.

9.2 보안 인식. 고객 데이터에 접근할 수 있는 모든 인원은 보안 인식 교육을 받습니다. 보안 모범 사례는 온보딩, 개발 워크플로 및 운영 절차에 반영됩니다.

9.3 공급업체 및 하위 처리자 관리. 하위 처리자는 본 문서에 설명된 것과 동등한 데이터 보호 기준을 계약상 준수해야 합니다. ProcessMind는 공개 [하위 처리자 목록](#)을 유지하며 새로운 하위 처리자를 이용하기 최소 30일 전에 통지합니다. 하위 처리자는 규정 준수 여부를 매년 검토받습니다.

9.4 기밀 유지. 고객 데이터를 처리하도록 승인된 모든 인원은 서면 기밀 유지 의무를 부담합니다.

10. 규정 준수 및 인증

프레임워크 / 표준	상태
GDPR(EU 일반 데이터 보호 규정)	준수
EU 데이터 상주(독일 프랑크푸르트)	시행 중
AWS 인프라 인증(ISO 27001, SOC 2, PCI DSS)	AWS를 통해 승계
ISO 27001(ProcessMind)	계획됨 — 인증 경로 선정, 공식 절차는 아직 시작되지 않음

프레임워크 / 표준	상태
SOC 2 Type II(ProcessMind)	계획됨 — 인증 경로 선정, 공식 절차는 아직 시작되지 않음
자동화된 인프라 통제 검증(cdk-nag AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	인증이 아닌 엔지니어링 통제 검증으로 시행
국제 이전을 위한 표준 계약 조항(SCC)	시행 중(DPA 참조)
데이터 처리 부속서(DPA)	공개적으로 이용 가능

cdk-nag 규칙 팩을 사용한다고 해서 ProcessMind가 HIPAA, NIST 또는 PCI DSS에 따라 공식 인증을 받았거나 독립적인 감사를 받았다는 의미는 아닙니다. 해당 규칙 팩은 인프라 설계를 검증하고 격차를 명시적으로 추적하기 위한 엔지니어링 보호 장치로 사용됩니다.

보안, 규정 준수에 관한 질문이 있거나 감사 보고서 또는 작성 완료된 보안 설문지와 같은 문서를 요청하려면 support@processmind.com으로 문의하시기 바랍니다.