

Các biện pháp bảo mật của ProcessMind

Ngày có hiệu lực: 14 tháng 9 năm 2026

Tài liệu này mô tả các biện pháp kỹ thuật và tổ chức ("TOM") mà ProcessMind B.V. duy trì để bảo vệ tính bảo mật, toàn vẹn và khả dụng của Dữ liệu Khách hàng. ProcessMind áp dụng phương pháp bảo vệ nhiều lớp, theo đó nhiều lớp bảo mật độc lập bảo vệ Dữ liệu Khách hàng ở mọi cấp độ – từ mạng và hạ tầng đến danh tính, cấp quyền, cô lập dữ liệu, mã hóa, giám sát và phát triển phần mềm. Các biện pháp này bổ sung cho [Phụ lục Xử lý Dữ liệu](#), [Chính sách quyền riêng tư](#) và [Chính sách Lưu trữ SaaS](#).

ProcessMind rà soát và cập nhật các biện pháp này ít nhất hằng năm.

Dữ liệu Khách hàng không bao giờ được bán cho, chia sẻ với hoặc được bên thứ ba sử dụng cho mục đích riêng của họ.

1. An ninh hạ tầng

1.1 Nền tảng đám mây. ProcessMind được lưu trữ độc quyền trên Amazon Web Services (AWS) tại EU (Frankfurt, Đức, eu-central-1). AWS duy trì các chứng nhận ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 và PCI DSS. Xem [Các chương trình tuân thủ của AWS](#) để biết danh sách đầy đủ.

1.2 Kiến trúc phi máy chủ. Logic ứng dụng ProcessMind chạy trên AWS Lambda và các dịch vụ do AWS quản lý. ProcessMind không vận hành các máy chủ ứng dụng có thời hạn hoạt động dài do khách hàng quản lý, qua đó loại bỏ phần lớn công việc vá hệ điều hành và tăng cường bảo mật máy chủ.

1.3 Ranh giới mạng. ProcessMind duy trì một AWS VPC để kiểm soát cơ sở dữ liệu và mạng. Aurora PostgreSQL chạy trong các mạng con riêng tư, không có lưu lượng đi ra internet, không thể truy cập công khai và đã bật nhật ký luồng VPC. Theo mặc định, ProcessMind không đặt các hàm Lambda của ứng dụng bên trong VPC. Lambda truy cập Aurora thông qua AWS RDS Data API qua TLS, sử dụng xác thực IAM và Secrets Manager.

1.4 Phân phối nội dung và kiểm soát tại biên. Lưu lượng truy cập vào trang web hướng đến khách hàng, SPA giao diện người dùng và tài nguyên công khai được phân phối thông qua Amazon CloudFront. Tất cả các bản phân phối CloudFront đều áp dụng chính sách TLS tối thiểu là TLS 1.2 (2021). Các bản phân phối trang web và SPA giao diện người dùng cũng bổ sung các tiêu đề phản hồi bảo mật, bao gồm HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, chính sách referrer và chính sách quyền. Bản phân phối tài nguyên công khai sử dụng CloudFront Origin Access Control để giữ riêng tư bucket nguồn. Lưu lượng API hướng đến khách hàng được xử lý riêng thông qua Amazon API Gateway: lưu lượng yêu cầu/phản hồi HTTPS được phân phối qua HTTP API trên một tên miền phụ API chuyên dụng, còn các kết nối máy khách theo thời gian thực được phân phối qua một WebSocket API riêng của API Gateway trên một tên miền phụ WebSocket chuyên dụng.

1.5 Tách biệt môi trường. Môi trường sản xuất và phát triển sử dụng các tài khoản AWS, cơ sở dữ liệu và ngăn xếp hạ tầng riêng biệt. Thông tin xác thực của nhà phát triển không cấp quyền truy cập Dữ liệu Khách hàng trong môi trường sản xuất.

2. Mã hóa dữ liệu

2.1 Mã hóa khi truyền. Tất cả dữ liệu được truyền giữa máy khách và các dịch vụ ProcessMind đều được mã hóa bằng TLS 1.2 trở lên. Các điểm cuối hướng tới khách hàng được cung cấp qua HTTPS. Các vùng lưu trữ S3, chủ đề SNS và hàng đợi SQS do ProcessMind trực tiếp tạo ra chỉ cho phép truy cập qua SSL. Việc truy cập cơ sở dữ liệu thông qua RDS Data API và các lệnh gọi dịch vụ AWS khác sử dụng HTTPS/TLS.

2.2 Mã hóa khi lưu trữ. Aurora PostgreSQL được mã hóa khi lưu trữ bằng các khóa AWS KMS do khách hàng quản lý, với tính năng tự động luân chuyển khóa. Các vùng lưu trữ S3 chứa dữ liệu khách hàng và dữ liệu vận hành do ProcessMind trực tiếp tạo ra, bao gồm các vùng lưu trữ tải lên, tài

nguyên và nhật ký truy cập, sử dụng khóa KMS do khách hàng quản lý. Các nhóm nhật ký CloudWatch, chủ đề SNS và hàng đợi SQS do ProcessMind trực tiếp tạo ra cũng sử dụng khóa KMS do khách hàng quản lý. Các vùng lưu trữ gốc của trang web và giao diện người dùng do SST quản lý sử dụng mã hóa phía máy chủ S3 do AWS quản lý (SSE-S3 / AES-256) thay vì khóa KMS do khách hàng quản lý.

2.3 Quản lý khóa và bí mật. Các khóa mã hóa cơ sở dữ liệu được quản lý tập trung thông qua AWS KMS và quyền truy cập khóa được điều chỉnh bằng các chính sách IAM theo nguyên tắc đặc quyền tối thiểu. Thông tin xác thực cơ sở dữ liệu được lưu trong AWS Secrets Manager. Bí mật chính của Aurora và bí mật của người dùng ứng dụng bị giới hạn quyền được tự động luân chuyển mỗi ba mươi (30) ngày. Khóa và bí mật trong môi trường sản xuất không bao giờ được lưu trong mã nguồn; thông tin xác thực chỉ dùng cho môi trường phát triển được tách biệt khỏi môi trường sản xuất. Một số tài nguyên hỗ trợ do AWS/CDK/SST quản lý tiếp tục sử dụng mã hóa do AWS quản lý khi dịch vụ hoặc khuôn khổ không cung cấp cấu hình khóa do khách hàng quản lý.

3. Cô lập và lưu trữ dữ liệu

3.1 Cô lập khách thuê. Mỗi khách hàng được cấp một phiên bản cơ sở dữ liệu riêng biệt, được cô lập. Dữ liệu Khách hàng không bao giờ bị trộn lẫn với dữ liệu của khách hàng khác ở cấp cơ sở dữ liệu. Siêu dữ liệu dùng chung (ví dụ: bản ghi tài khoản, thanh toán, ánh xạ người dùng với khách thuê) được lưu trong một cơ sở dữ liệu đa khách thuê riêng biệt với các biện pháp kiểm soát truy cập nghiêm ngặt. Các bảng dùng chung được giới hạn theo khách thuê và tổ chức còn được bảo vệ bằng chính sách bảo mật cấp hàng (RLS) của PostgreSQL, được thực thi thông qua ngữ cảnh cơ sở dữ liệu theo từng yêu cầu.

3.2 Lưu trữ dữ liệu. Tất cả Dữ liệu Khách hàng, bao gồm cơ sở dữ liệu, tệp tải lên, bản sao lưu và kết quả truy vấn, chỉ được lưu trữ tại EU (Frankfurt, Đức). Khi sử dụng một bên xử lý phụ đặt ngoài EEA cho một hoạt động xử lý cụ thể

(ví dụ: xử lý bằng mô hình AI hoặc xử lý thanh toán), việc chuyển dữ liệu được bảo đảm bằng cơ chế chuyển dữ liệu phù hợp như mô tả trong Phụ lục Xử lý Dữ liệu; bên xử lý phụ và địa điểm xử lý được liệt kê trong Danh sách Bên xử lý phụ.

3.3 Lưu giữ và xóa dữ liệu. Thời hạn lưu giữ và xóa được quy định tại Mục 6 của [Phụ lục Xử lý Dữ liệu](#). Khách hàng có thể xóa dữ liệu của mình bất cứ lúc nào thông qua ứng dụng hoặc bằng cách liên hệ với ProcessMind. Các bản sao lưu được xóa khi hết thời hạn lưu giữ bản sao lưu áp dụng (Mục 7.1).

4. Quản lý danh tính và quyền truy cập

4.1 Xác thực. ProcessMind hỗ trợ Đăng nhập một lần (SSO) thông qua Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC và LinkedIn OAuth 2.0/OIDC. ProcessMind đóng vai trò là bên dựa vào dịch vụ xác thực và không lưu trữ mật khẩu người dùng. Nhà cung cấp danh tính thực thi xác thực đa yếu tố — ví dụ, khi một tổ chức kết nối Microsoft Entra ID (Azure AD), các chính sách MFA và truy cập riêng của tổ chức đó sẽ được áp dụng.

4.2 Quản lý phiên. Các phiên trình duyệt sử dụng JSON Web Token (JWT) có chữ ký, được truyền qua cookie bảo mật, HttpOnly với các cờ SameSite và Secure. Chữ ký mã thông báo được xác thực trong mỗi yêu cầu đã xác thực.

4.3 Mô hình ủy quyền. ProcessMind không phụ thuộc vào các authorizer gốc của API Gateway đối với các API ứng dụng cốt lõi. Việc ủy quyền được thực thi trong các trình bao bọc trình xử lý Lambda dùng chung, xác thực trạng thái phiên và phạm vi tenant trước khi logic nghiệp vụ chạy. Các tuyến công khai được đưa rõ ràng vào danh sách cho phép đối với các luồng không xác thực, webhook, tiếp nhận sự kiện và yêu cầu CORS preflight. Các điểm cuối API bên ngoài sử dụng trình xử lý xác thực chuyên dụng. Quyền truy cập vào Dữ liệu Khách hàng được giới hạn theo tenant hoặc tổ chức đã xác thực.

4.4 Đặc quyền tối thiểu. Các hệ thống nội bộ tuân theo nguyên tắc đặc quyền tối thiểu. Vai trò IAM được giới hạn ở mức tài nguyên tối thiểu cần thiết khi khuôn khổ cho phép xác định phạm vi chính xác. Một số vai trò do SST/CDK tạo ra sử dụng các chính sách được quản lý hoặc chính sách nội tuyến có phạm vi rộng hơn để hỗ trợ liên kết và hoạt động thời gian chạy; các trường hợp này được rà soát, giới hạn theo tài nguyên khi có thể và theo dõi như các ngoại lệ được xác định rõ.

4.5 Kiểm soát quyền truy cập của nhân viên. Quyền truy cập của nhân viên vào các hệ thống nội bộ được quản lý thông qua Active Directory với SSO và MFA bắt buộc. Kiểm soát truy cập dựa trên vai trò (RBAC) bảo đảm quyền truy cập Dữ liệu Khách hàng chỉ giới hạn cho nhân sự được ủy quyền trên cơ sở cần biết. Quyền truy cập được rà soát định kỳ.

5. Ghi nhật ký, giám sát và kiểm toán

5.1 Ghi nhật ký tập trung. Tính năng ghi nhật ký truy cập HTTP API và WebSocket được bật với các trường JSON có cấu trúc và nhật ký được ghi vào Amazon CloudWatch Logs với thời hạn lưu giữ một (1) năm. Các nhóm nhật ký truy cập đó được mã hóa bằng khóa AWS KMS do khách hàng quản lý. Nhật ký ứng dụng được tập trung trong các nhóm nhật ký Amazon CloudWatch được mã hóa bằng khóa AWS KMS do khách hàng quản lý và lưu giữ trong mười (10) năm. Các nhóm nhật ký kiểm toán và đo từ xa riêng biệt cũng được mã hóa bằng khóa AWS KMS do khách hàng quản lý và lưu giữ trong mười (10) năm. Nhóm nhật ký xuất nhật ký của công cụ Aurora PostgreSQL được lưu giữ trong một (1) tuần.

5.2 Nội dung được ghi nhật ký và không được ghi nhật ký. ProcessMind ghi nhật ký các sự kiện truy cập HTTP API và WebSocket — thời gian yêu cầu, mã định danh yêu cầu, tuyến hoặc đường dẫn, trạng thái phản hồi và độ trễ. Nhật ký truy cập không bao gồm địa chỉ IP nguồn hoặc tác nhân người dùng của bên gọi. ProcessMind cũng ghi nhật ký các sự kiện xác thực, đường dẫn lỗi bất đồng bộ và hoạt động ứng dụng Lambda hỗ trợ vào các nhóm nhật ký CloudWatch tập trung. Nhật ký luồng VPC được bật. Hiện tại,

ProcessMind không bật tính năng ghi nhật ký truy cập tiêu chuẩn CloudFront trên các bản phân phối trang web, SPA giao diện người dùng hoặc tài nguyên công khai.

5.3 Giám sát và cảnh báo. Các cảnh báo và bảng điều khiển CloudWatch giám sát tình trạng hệ thống, hàng đợi thư chết và các lỗi liên quan đến bảo mật. Các lỗi xử lý bất đồng bộ được chuyển đến hàng đợi thư chết được mã hóa (thời hạn lưu giữ mười bốn (14) ngày; hai (2) ngày đối với hàng đợi hình thu nhỏ và chỉ mục tìm kiếm), và cảnh báo DLQ kích hoạt thông báo SNS để điều tra. Ngoài ra, ProcessMind sử dụng Sentry để theo dõi lỗi giao diện người dùng theo thời gian thực, giám sát hiệu suất và phát lại phiên. Chỉ ghi lại phiên phát lại đối với các phiên xảy ra lỗi; văn bản, dữ liệu nhập vào biểu mẫu và nội dung đa phương tiện được che hoặc chặn trong bản phát lại. Dữ liệu Sentry được tiếp nhận tại EU (Frankfurt) và chỉ giới hạn ở Dữ liệu Sử dụng ProcessMind (lỗi trình duyệt, dấu vết hiệu suất, siêu dữ liệu thiết bị và bản ghi phát lại đã được che). Sentry được liệt kê trong [danh sách bên xử lý phụ](#).

5.4 Bảo vệ nhật ký. Nhật ký được lưu trong các nhóm nhật ký CloudWatch chuyên dụng, có kiểm soát truy cập và được mã hóa khi lưu trữ. Nhật ký môi trường sản xuất và phát triển được tách biệt theo ranh giới môi trường và tài khoản.

6. Xác thực biện pháp kiểm soát tự động và quản lý lỗ hổng

6.1 Những gì ProcessMind thực hiện. ProcessMind chạy cdk-nag như một phần của quy trình tổng hợp hạ tầng và triển khai, sử dụng nhiều bộ quy tắc trong ngành (bao gồm AWS Solutions, NIST 800-53 và PCI DSS). Báo cáo theo từng ngăn xếp được tạo và rà soát như một phần của hoạt động quản lý thay đổi hạ tầng. Các phát hiện được phân loại để khắc phục, chấp nhận rủi ro hoặc lên kế hoạch cải thiện.

6.2 Cách quản lý ngoại lệ. Các trường hợp loại trừ được ghi nhận trong sổ đăng ký tập trung khi khuôn khổ cho phép, giới hạn trong các ngăn xếp bị ảnh hưởng và phải có lý do bằng văn bản; nếu một ngăn xếp có trường hợp loại trừ nội tuyến, trường hợp đó được ghi lại cùng với ngăn xếp đó. Khi một

phát hiện được khắc phục, trường hợp loại trừ tương ứng được cập nhật hoặc xóa bỏ. ProcessMind không xem việc loại trừ là sự miễn trừ toàn diện khỏi hoạt động rà soát.

6.3 Những việc ProcessMind hiện chưa thực hiện. ProcessMind theo dõi và rà soát các ngoại lệ trọng yếu đối với biện pháp kiểm soát hạ tầng. Các ngoại lệ chính gồm:

- Các Lambda ứng dụng theo mặc định không được đặt bên trong VPC; chúng truy cập Aurora thông qua RDS Data API qua TLS với xác thực IAM và Secrets Manager
- Không phần nào của dịch vụ được AWS WAF bảo vệ: AWS WAF không hỗ trợ API Gateway HTTP APIs và các điểm truy cập còn lại cũng không được WAF bảo vệ (các kết nối WebSocket sử dụng token HMAC có thời hạn ngắn; các hạn chế địa lý liên quan đến thanh toán được thực thi trong hệ thống thanh toán); các bản phân phối tĩnh cũng không bật ghi nhật ký truy cập tiêu chuẩn của CloudFront
- Việc khôi phục cơ sở dữ liệu dựa vào các bản sao lưu tự động và khả năng khôi phục tại một thời điểm cụ thể của Aurora, thay vì một kế hoạch AWS Backup riêng hoặc Aurora Enhanced Monitoring
- Không có sao chép S3 liên vùng hoặc S3 Object Lock đối với các bucket có thể thay đổi
- Một số tài nguyên hỗ trợ do AWS/CDK/SST quản lý sử dụng mã hóa do AWS quản lý hoặc các chính sách IAM được tạo rộng hơn khi dịch vụ không cung cấp phương án thay thế do khách hàng kiểm soát

Sổ đăng ký đầy đủ các trường hợp loại trừ được duy trì cùng với mã hạ tầng và được cung cấp theo yêu cầu. Việc sử dụng các bộ quy tắc `cdk-nag` là hoạt động xác thực biện pháp kiểm soát kỹ thuật, không phải chứng nhận bên ngoài, ý kiến kiểm toán hoặc xác nhận pháp lý về việc tuân thủ HIPAA, NIST hoặc PCI DSS.

6.4 Quản lý phần phụ thuộc. Các phần phụ thuộc phần mềm được giám sát liên tục để phát hiện lỗ hổng đã biết. Các lỗ hổng nghiêm trọng và mức độ

cao được vá với mục tiêu trong vòng bảy (7) ngày. Các phần phụ thuộc được cập nhật theo chu kỳ thường xuyên.

6.5 Vòng đời phát triển phần mềm an toàn (SDLC). ProcessMind áp dụng phương pháp bảo vệ nhiều lớp trong phát triển phần mềm. Mọi thay đổi đối với môi trường sản xuất phải vượt qua nhiều lớp xác thực tự động độc lập trước khi triển khai:

- **Phân tích tĩnh và an toàn kiểu dữ liệu:** Chế độ nghiêm ngặt của TypeScript và ESLint thực thi tính chính xác của kiểu dữ liệu, an toàn với giá trị null và các mẫu lập trình liên quan đến bảo mật tại thời điểm biên dịch.
- **Rà soát mã có hỗ trợ AI:** Phân tích có hỗ trợ AI cung cấp thêm một góc nhìn rà soát đối với các yêu cầu kéo nhằm xác định rủi ro bảo mật, lỗi logic và sai lệch quy ước, bổ sung cho kiểm thử tự động.
- **Kiểm thử đơn vị và tích hợp:** Bộ kiểm thử Vitest toàn diện xác thực logic nghiệp vụ, mẫu truy cập dữ liệu, hành vi API và xử lý lỗi dựa trên các tài nguyên AWS đang hoạt động trong môi trường phát triển.
- **Kiểm thử đầu cuối:** Các bài kiểm thử trình duyệt dựa trên Playwright xác minh các quy trình làm việc quan trọng của người dùng, bao gồm xác thực, tải dữ liệu lên, mô hình hóa quy trình, mô phỏng và cô lập đa khách thuê.
- **Quét tuân thủ hạ tầng:** cdk-nag xác thực mã hạ tầng theo nhiều khuôn khổ tuân thủ trong mỗi lần thay đổi.
- **Quét lỗ hổng phần phụ thuộc:** Các cuộc kiểm tra phần phụ thuộc tự động ngăn lỗ hổng đã biết ở mức nghiêm trọng và mức độ cao được đưa vào môi trường sản xuất.

Hoạt động rà soát của con người tập trung vào kiến trúc, ranh giới bảo mật và các quyết định ở cấp độ thiết kế thay vì kiểm tra mã từng dòng. Khi có thay đổi về cấu trúc, nhạy cảm về bảo mật hoặc liên quan đến hạ tầng, ngoài xác thực tự động còn phải có phê duyệt rõ ràng của con người.

Tất cả các lớp xác thực được thực thi thông qua CI dưới dạng các điều kiện bắt buộc để hợp nhất những thay đổi ứng dụng và hạ tầng vào nhánh

chính. Nội dung trang web và các bản phát hành tài sản tĩnh tuân theo quy trình phát hành riêng đã được lập thành văn bản, với các bước kiểm tra tại thời điểm triển khai — bao gồm kiểm tra tự động để bảo đảm các tài liệu pháp lý được cập nhật — thay vì điều kiện CI của ứng dụng. Các bản sửa lỗi khẩn cấp trong môi trường sản xuất có thể bỏ qua điều kiện CI nhưng phải được tiếp nối bằng một lần chạy đầy đủ quy trình và rà soát sau sự cố trong vòng hai mươi bốn (24) giờ.

7. Sao lưu và khôi phục sau thảm họa

7.1 Sao lưu tự động. Amazon Aurora thực hiện sao lưu liên tục, tự động với thời hạn lưu giữ bảy (7) ngày. Bản sao lưu được mã hóa bằng cùng các khóa KMS do khách hàng quản lý như cơ sở dữ liệu nguồn.

7.2 Khôi phục theo thời điểm. Aurora hỗ trợ khôi phục theo thời điểm đến bất kỳ giây nào trong thời hạn lưu giữ bản sao lưu, cho phép khôi phục nhanh trong trường hợp dữ liệu bị hỏng hoặc vô tình bị xóa.

7.3 Độ bền và lập phiên bản S3. Tập tải lên và cấu phần vận hành được lưu trong Amazon S3, dịch vụ cung cấp độ bền 99.999999999% (11 số 9). Tính năng lập phiên bản được bật trên vùng lưu trữ tải lên và các vùng lưu trữ tài nguyên để hỗ trợ khôi phục và hoàn tác. Các vùng lưu trữ triển khai trang web và giao diện người dùng là cấu phần bản dựng có thể tái tạo và không được xem là hệ thống sao lưu. Hiện tại, ProcessMind không bật tính năng sao chép S3 liên khu vực.

7.4 Duy trì hoạt động kinh doanh. Các quy trình khôi phục sau thảm họa được lập thành văn bản và kiểm thử định kỳ. Bản tóm tắt có trong tài liệu [Khôi phục sau thảm họa, Duy trì hoạt động kinh doanh và Ứng phó sự cố](#). Kiến trúc dựa vào các dịch vụ do AWS quản lý trong khu vực eu-central-1, được AWS vận hành trên nhiều Vùng sẵn sàng; cụm Aurora hiện chạy một phiên bản ghi duy nhất, vì vậy việc khôi phục cơ sở dữ liệu dựa vào bản sao lưu tự động và khôi phục theo thời điểm thay vì một phiên bản dự phòng trong cùng khu vực. Bản sao lưu Aurora, độ bền S3, hàng đợi thư chết và tài

sản tinh có thể dựng lại từ mã nguồn là một phần trong chiến lược khôi phục.

8. Ứng phó sự cố

8.1 Thông báo sự cố. Trong trường hợp xảy ra Sự cố An ninh (theo định nghĩa trong DPA), ProcessMind sẽ thông báo cho khách hàng bị ảnh hưởng mà không chậm trễ bất hợp lý và, nếu khả thi, trong vòng bảy mươi hai (72) giờ kể từ khi biết về sự cố.

8.2 Xử lý sự cố. ProcessMind duy trì các quy trình ứng phó sự cố đã được lập thành văn bản, bao gồm nhận diện, ngăn chặn, loại bỏ, khôi phục và rà soát sau sự cố. Bản tóm tắt có trong tài liệu [Khôi phục sau thảm họa, Duy trì hoạt động kinh doanh và Ứng phó sự cố](#). Các bài học rút ra từ sự cố được tích hợp vào các biện pháp kiểm soát và quy trình bảo mật.

8.3 Trao đổi thông tin. Thông báo sự cố bao gồm tính chất và phạm vi sự cố, các loại dữ liệu bị ảnh hưởng, biện pháp đã thực hiện để ngăn chặn sự cố và hành động được khuyến nghị cho khách hàng.

9. Biện pháp tổ chức

9.1. Quản lý an toàn thông tin. ProcessMind duy trì hệ thống quản lý an toàn thông tin phù hợp với các nguyên tắc ISO 27001. ProcessMind đã lựa chọn lộ trình chứng nhận ISO 27001 và xác nhận SOC 2 Type II; quy trình chứng nhận chính thức vẫn chưa bắt đầu.

9.2 Nhận thức về bảo mật. Tất cả nhân sự có quyền truy cập Dữ liệu Khách hàng đều được đào tạo nâng cao nhận thức về bảo mật. Các thực tiễn tốt nhất về bảo mật được lồng ghép vào quy trình tiếp nhận nhân sự mới, quy trình làm việc phát triển và quy trình vận hành.

9.3 Quản lý nhà cung cấp và bên xử lý phụ. Các bên xử lý phụ bị ràng buộc theo hợp đồng phải tuân thủ các tiêu chuẩn bảo vệ dữ liệu tương đương với những tiêu chuẩn được mô tả trong tài liệu này. ProcessMind duy trì [danh](#)

[sách bên xử lý phụ](#) công khai và thông báo trước ít nhất ba mươi (30) ngày trước khi sử dụng một bên xử lý phụ mới. Các bên xử lý phụ được rà soát hằng năm về việc tuân thủ.

9.4 Bảo mật thông tin. Tất cả nhân sự được ủy quyền xử lý Dữ liệu Khách hàng đều chịu sự ràng buộc của nghĩa vụ bảo mật bằng văn bản.

10. Tuân thủ và chứng nhận

Khuôn khổ / Tiêu chuẩn	Trạng thái
GDPR (Quy định chung về bảo vệ dữ liệu của EU)	Tuân thủ
Lưu trữ dữ liệu tại EU (Frankfurt, Đức)	Được thực thi
Chứng nhận hạ tầng AWS (ISO 27001, SOC 2, PCI DSS)	Kế thừa thông qua AWS
ISO 27001 (ProcessMind)	Dự kiến — đã chọn lộ trình chứng nhận; quy trình chính thức chưa bắt đầu
SOC 2 Type II (ProcessMind)	Dự kiến — đã chọn lộ trình chứng nhận; quy trình chính thức chưa bắt đầu
Xác thực biện pháp kiểm soát hạ tầng tự động (cdk-nag trên AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Được triển khai để xác thực biện pháp kiểm soát kỹ thuật, không phải chứng nhận
Điều khoản Hợp đồng Tiêu chuẩn (SCC) cho việc chuyển dữ liệu quốc tế	Đã triển khai (xem DPA)
Phụ lục Xử lý Dữ liệu (DPA)	Được cung cấp công khai

Việc sử dụng các bộ quy tắc cdk-nag không có nghĩa là ProcessMind được chứng nhận chính thức hoặc được kiểm toán độc lập theo HIPAA, NIST hoặc PCI DSS. Các bộ quy tắc đó được sử dụng làm biện pháp bảo vệ trong hoạt động kỹ thuật để xác thực thiết kế hạ tầng và theo dõi rõ ràng các thiếu sót.

Nếu bạn có câu hỏi về bảo mật, tuân thủ hoặc muốn yêu cầu tài liệu như báo cáo kiểm toán hay bảng câu hỏi bảo mật đã hoàn thành, hãy liên hệ support@processmind.com.