Tuyên bố về Nhật ký kiểm toán và SIEM của ProcessMind

Ngày có hiệu lực: ngày 12 tháng 11 năm 2026

Tuyên bố này mô tả cách ProcessMind B.V. ghi nhận các hành động liên quan đến bảo mật và hành chính được thực hiện đối với Dữ liệu Khách hàng ("nhật ký kiểm toán"). Tuyên bố này bổ sung cho Các Biện pháp Bảo mật, Phụ lục Xử lý Dữ liệu, Thỏa thuận Khách hàng và Danh sách Nhà thầu phụ.

---

1. Phạm vi

1.1 Một nhật ký kiểm toán. ProcessMind duy trì một nhật ký kiểm toán duy nhất cho các hành động liên quan đến bảo mật và hành chính được thực hiện đối với Dữ liệu Khách hàng và Dịch vụ ProcessMind. Nhật ký kiểm toán tách biệt với nhật ký vận hành (ứng dụng), nhật ký truy cập HTTP và bảng tin hoạt động của sản phẩm; các luồng này phục vụ những mục đích khác nhau và không được xem là dấu vết kiểm toán.

1.2 Những nội dung không thuộc nhật ký. Nhật ký kiểm toán không ghi lại mọi lần đọc Dữ liệu Khách hàng và không phải là lịch sử thay đổi của sản phẩm đối với các mô hình quy trình, sơ đồ, tài liệu hoặc mô phỏng. Những nội dung đó được ghi lại trong lịch sử thay đổi quy trình có sẵn bên trong sản phẩm.

---

2. Nội dung của từng hồ sơ kiểm toán

2.1 Các trường. Mỗi hồ sơ có các trường dưới đây. Tập hợp trường được cố định theo lược đồ hồ sơ: hồ sơ không thể có thêm trường không nằm trong danh sách này và hành động không thể thêm trường chưa được khai báo trong danh mục.

- *schemaVersion* (number): phiên bản lược đồ hồ sơ, hiện là 1.

- *eventId* (string): mã định danh duy nhất của hồ sơ. Hồ sơ mới sử dụng ULID; các hàng được chuyển từ kho dữ liệu trước đây giữ nguyên UUID.
- *occurredAt*, *ingestedAt* (dấu thời gian): thời điểm hành động xảy ra và thời điểm bộ ghi kiểm toán lưu hồ sơ. Cả hai đều theo UTC.
- *eventClass* (enum): security, auth, admin, data, api, ai hoặc platform.
- *action* (enum): một mã trong danh mục hành động khép kín đã được rà soát, ví dụ auth.login.blocked hoặc api.key.revoked.
- *outcome* (enum): success, failure, denied hoặc error.
- *severity* (enum): info, notice, warning hoặc critical, được xác định dựa trên kết quả. Hành động thành công sử dụng giá trị mặc định trong danh mục (info, trừ khi hành động quy định khác); thất bại được ghi nhận là notice, còn bị từ chối hoặc lỗi là warning.
- *actor* (object): chủ thể thực hiện hành động. type (user, apiKey, service, system hoặc anonymous), id, email, displayName và onBehalfOf cùng onBehalfOfEmail nếu hành động được thực hiện thay cho một tài khoản khác.
- *actorContext* (object): phiên thực hiện hành động. sessionId, authMethod (oidc, password, loginToken, apiKey hoặc none) và cờ phiên hỗ trợ.
- *organizationId*, *tenantId* (mã định danh, có thể null): tổ chức và môi trường mà hành động thuộc về. Giá trị null đối với hồ sơ không liên quan đến khách hàng nào hoặc nằm ở cấp cao hơn môi trường.
- *resource* (object, có thể null): đối tượng bị ảnh hưởng. type, id và name, trong đó type là một trong các giá trị apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant hoặc user.
- *source* (object): nơi tạo ra hồ sơ. service (api, externalApi, superadminApi, worker, cron hoặc webSocket), function và version.
- *stage*, *region* (string): giai đoạn triển khai tạo ra hồ sơ (ví dụ prod) và AWS region (eu-central-1 đối với hồ sơ khách hàng).

- *correlation* (object): requestId, traceId và parentEventId, liên kết hồ sơ với yêu cầu gây ra hồ sơ đó và với các hồ sơ trước đó trong cùng luồng.
- *network* (object, có thể null): sourceIp và userAgent. Chỉ được thu thập đối với các hành động có mục tương ứng trong danh mục cho phép: đăng nhập, quyết định truy cập, thay đổi hành chính và cài đặt, tải dữ liệu lên, tải xuống và xuất dữ liệu, thay đổi khóa API và thay đổi chính sách AI.
- *detail* (object): dữ liệu riêng của hành động, được xác thực theo lược đồ của hành động đó. Giá trị chỉ là kiểu nguyên thủy (string, number, boolean, null), để hồ sơ vẫn có thể truy vấn và biên tập thông tin.

2.2 Từ vựng khép kín. Các hành động được lấy từ danh sách mã hành động cố định đã được rà soát; hồ sơ kiểm toán không có thông điệp dạng văn bản tự do. Mỗi hành động cũng khai báo những trường bổ sung mà hành động đó có thể chứa, do đó hồ sơ không thể âm thầm phát sinh một loại nội dung mới.

---

3. Những hành động được ghi nhận

3.1 Các hành động hiện được ghi nhận. ProcessMind ghi nhận, trong số những hành động khác:

- **Xác thực:** đăng nhập thành công và thất bại, đăng nhập bị chặn (tài khoản bị khóa, miền không được phép, email của nhà cung cấp chưa được xác minh), đăng xuất, cấp và chuyển giao mã thông báo đăng nhập.
- **Cấp quyền:** từ chối truy cập, bao gồm mọi thông tin xác thực API bên ngoài bị từ chối, phạm vi và trạng thái tenant, cũng như từ chối nguồn gốc (CORS).
- **Truy cập hỗ trợ:** thời điểm bắt đầu phiên hỗ trợ của ProcessMind trên tài khoản khách hàng, nêu rõ cả nhân viên vận hành và tài khoản bị ảnh hưởng.

- **Thông tin xác thực API:** tạo, thay đổi phạm vi và thu hồi khóa API, bao gồm các phạm vi được cấp.
- **Quản trị tài khoản và vai trò:** tạo người dùng, gửi lời mời, chỉnh sửa hồ sơ quản trị viên, xóa, cấp và thu hồi vai trò, cũng như thay đổi tư cách thành viên tenant hoặc tổ chức.
- **Vòng đời tổ chức:** tạo, xóa, khôi phục, lên lịch xóa và hủy lịch xóa, cũng như xóa hoàn tất.
- **Tải dữ liệu lên, tải xuống và xuất dữ liệu:** tải lên, tải xuống và xóa hiện vật; tải lên và cập nhật dữ liệu dạng bảng; tải xuống dữ liệu xuất; xóa bảng dữ liệu; và tạo, thay đổi, xóa webhook (kết nối).
- **Trạng thái thanh toán:** thay đổi gói, tạm ngưng và khôi phục do thanh toán, và hủy đăng ký.
- **Bảng điều khiển nhà cung cấp của ProcessMind:** thực thi truy vấn có đặc quyền, quản trị người dùng và tổ chức, thay đổi cài đặt và tính năng, yêu cầu đồng bộ hóa thanh toán và di chuyển dữ liệu.
- **Các hành động hành chính và phá hủy do tác vụ đã lên lịch của ProcessMind thực hiện:** xóa tenant, tổ chức, người dùng và khách hàng tiềm năng, quét dữ liệu theo thời hạn lưu giữ và lỗi quy trình xử lý dữ liệu.
- **Tính toàn vẹn của nhật ký kiểm toán:** lỗi trong quy trình ghi của chính nhật ký kiểm toán.

3.2 Chỉnh sửa không gian làm việc. Các chỉnh sửa bên trong không gian làm việc (mô hình quy trình, tài liệu, mô phỏng, bảng điều khiển, bình luận và dấu trang) được ghi nhận trong lịch sử thay đổi quy trình riêng của sản phẩm, không phải trong nhật ký kiểm toán. Nhật ký kiểm toán ghi nhận ai đã tải dữ liệu lên, tải xuống, xuất hoặc xóa; lịch sử thay đổi ghi nhận nội dung nào đã thay đổi bên trong mô hình. Danh sách mã hành động được ghi nhận hiện tại có thể được cung cấp từ ProcessMind theo yêu cầu.

---

4. Những nội dung không bao giờ được ghi nhận

Mật khẩu, mã thông báo xác thực, giá trị khóa API, cookie, tiêu đề ủy quyền, nội dung yêu cầu hoặc phản hồi, nội dung tệp, URL ký trước và lời nhắc hoặc

nội dung hoàn tất của AI không bao giờ được ghi vào nhật ký kiểm toán. Hồ sơ kiểm toán có thể chứa dữ liệu cá nhân cần thiết để xác định chủ thể: địa chỉ email của chủ thể thực hiện hành động, cùng địa chỉ IP nguồn và user agent đối với các hành động có mục tương ứng trong danh mục cho phép (đăng nhập, quyết định truy cập, thay đổi hành chính và cài đặt, di chuyển dữ liệu, thay đổi khóa API và chính sách AI). Các trường được phép được xác định cho từng hành động và được rà soát khi thêm hành động.

---

5. Tính toàn vẹn

5.1 Chỉ ghi nối tiếp. Nhật ký kiểm toán chỉ cho phép ghi nối tiếp. Không vai trò ứng dụng nào có quyền cập nhật hoặc xóa nhật ký, và ràng buộc cơ sở dữ liệu từ chối cả hai thao tác.

5.2 Một bộ ghi duy nhất. Hồ sơ được ghi bởi một thành phần duy nhất, thành phần này xác thực mã hành động và dữ liệu tải trọng trước khi ghi. Hồ sơ không vượt qua xác thực sẽ bị từ chối và báo cáo, thay vì chỉ được ghi một phần.

5.3 Xử lý lỗi. Lỗi ghi kiểm toán không bao giờ làm thất bại hành động nghiệp vụ mà hồ sơ mô tả. Lỗi được ghi nhận trên một luồng vận hành có cảnh báo, và bản thân hồ sơ được lưu giữ trong một bản sao thứ cấp để có thể khôi phục.

---

6. Thời hạn lưu giữ và địa điểm

6.1 Thời hạn lưu giữ. Hồ sơ kiểm toán được lưu giữ ít nhất mười (10) năm kể từ ngày sự kiện.

6.2 Địa điểm và mã hóa. Hồ sơ kiểm toán được lưu trữ tại Liên minh Châu Âu (Frankfurt, Đức, `eu-central-1`) và được mã hóa khi lưu trữ bằng khóa AWS KMS do khách hàng quản lý. Một bản sao trực tiếp cũng được ghi vào nhóm nhật ký Amazon CloudWatch có kiểm soát truy cập để có thể điều tra sự cố trong khi sự cố đang diễn ra.

6.3 Không sao chép giữa các khu vực. Hồ sơ kiểm toán không được sao chép ra ngoài Liên minh Châu Âu.

---

7. Truy cập hồ sơ kiểm toán

7.1 Quyền truy cập. Nhật ký kiểm toán trong ứng dụng được bao gồm trong gói Process Architecture trở lên. Quản trị viên tổ chức có thể đọc toàn bộ hồ sơ của tổ chức; quản trị viên giới hạn theo tenant có thể đọc hồ sơ của tenant mình. Phạm vi được xác định từ phiên đã xác thực và được kiểm tra trước khi truy vấn, do đó yêu cầu không thể mở rộng phạm vi sang tenant hoặc tổ chức khác.

7.2 Nhân sự ProcessMind. Nhân sự ProcessMind chỉ truy cập hồ sơ kiểm toán để hỗ trợ, ứng phó sự cố hoặc thực hiện nghĩa vụ pháp lý, trên cơ sở cần biết. Quyền truy cập giữa các khách hàng bị giới hạn ở một vai trò hỗ trợ chuyên biệt và chính việc truy cập đó cũng là một hành động hành chính.

7.3 Cách nhận hồ sơ. Quản trị viên tổ chức và tenant có thể đọc hồ sơ kiểm toán của mình trong nhật ký kiểm toán trong ứng dụng, đồng thời lấy hoặc xuất hồ sơ thông qua API bên ngoài. Đối với yêu cầu lớn hơn hoặc cần hỗ trợ, bộ phận hỗ trợ ProcessMind cung cấp hồ sơ ở định dạng CSV hoặc JSON cho tổ chức, tenant và khoảng thời gian được chỉ định, với mục tiêu xử lý yêu cầu thông thường trong vòng năm (5) ngày làm việc.

---

8. Xóa hồ sơ kiểm toán

8.1 Theo yêu cầu. Khi nhận được yêu cầu bằng văn bản đã được xác minh, ProcessMind xóa hồ sơ kiểm toán thuộc về tổ chức khách hàng khỏi kho kiểm toán và xác nhận việc xóa bằng văn bản. Không thể chỉnh sửa từng hồ sơ trong bản sao CloudWatch vận hành; hồ sơ sẽ hết hạn theo thời hạn lưu giữ riêng của bản sao đó.

8.2 Nội dung được lưu giữ. Hồ sơ ghi nhận việc xóa đã diễn ra (mã định danh tổ chức, ngày, người yêu cầu, lý do và số lượng hồ sơ đã xóa) được

lưu giữ dưới dạng hồ sơ kiểm toán cấp nền tảng và không chứa Dữ liệu Khách hàng. Hồ sơ không thuộc về khách hàng nào (sự kiện nền tảng ProcessMind) không bị ảnh hưởng bởi yêu cầu xóa của khách hàng.

8.3 Yêu cầu xóa dữ liệu cá nhân. Khi yêu cầu liên quan đến một cá nhân thuộc khách hàng vẫn đang hoạt động, hồ sơ bảo mật được lưu giữ nhằm xác lập, thực hiện hoặc bảo vệ các khiếu nại pháp lý theo quy định tại Điều 17(3)(b) và (e) GDPR; cơ sở này được ghi nhận trong hồ sơ hoạt động xử lý và trong Chính sách Quyền riêng tư.

---

9. Tích hợp và xuất SIEM

9.1 Tính khả dụng. Kho lưu trữ kiểm toán bất biến là tùy chọn Enterprise, được kích hoạt cho tổ chức khách hàng theo yêu cầu. Kho này ghi các đối tượng NDJSON được nén hằng ngày vào một tiền tố riêng cho từng tổ chức trong một vùng lưu trữ S3 Object-Locked (WORM), kèm theo tệp kê khai và đối soát hằng đêm.

9.2 Phương thức cung cấp hiện tại. Hiện ProcessMind không cung cấp trình kết nối SIEM gốc hoặc luồng đẩy dữ liệu. Dữ liệu được cung cấp theo phương thức kéo từ ba giao diện: API đọc (`GET /v1/tenant/{tenantId}/audit`), tác vụ xuất có giới hạn (tạo tác vụ bằng `POST /v1/tenant/{tenantId}/audit/exports` và lấy kết quả từ lệnh gọi trạng thái, lệnh này trả về URL tải xuống có thời hạn ngắn), và, với kho lưu trữ Enterprise, các đối tượng hằng ngày nằm dưới tiền tố riêng của tổ chức trong vùng lưu trữ Object-Locked, mà SIEM của khách hàng đọc thông qua thỏa thuận truy cập. ProcessMind không tự cung cấp hồ sơ đến địa điểm do khách hàng lựa chọn theo lịch trình riêng.

9.3 Hoạt động giám sát của ProcessMind. Hoạt động giám sát bảo mật của ProcessMind sử dụng cùng các hồ sơ này: lỗi ghi kiểm toán, đợt tăng đột biến lỗi xác thực, thay đổi đặc quyền và các hành động hành chính có tính phá hủy sẽ kích hoạt cảnh báo nội bộ.

---

10. Bằng chứng cung cấp cho khách hàng

Theo yêu cầu và trong phạm vi áp dụng nghĩa vụ bảo mật, ProcessMind cung cấp tuyên bố này, Các Biện pháp Bảo mật, Phụ lục Xử lý Dữ liệu, Danh sách Nhà thầu phụ, mẫu hồ sơ kiểm toán đã biên tập thông tin và quy trình áp dụng cho các yêu cầu truy cập và xóa.

---

11. Giới hạn

Để tránh hiểu nhầm, ProcessMind xác nhận có kho kiểm toán chỉ cho phép ghi nối tiếp đối với mọi tổ chức và, khi quyền sử dụng kho lưu trữ kiểm toán được bật, có bản sao Object-Locked (WORM) với đối soát tệp kê khai hằng đêm. ProcessMind hiện không xác nhận có chuỗi băm, trình kết nối SIEM gốc đẩy dữ liệu theo thời gian thực, khả năng biên tập hồ sơ kiểm toán theo từng người dùng, chứng nhận ISO 27001 hoặc SOC 2 bao quát biện pháp kiểm soát này, hoặc phạm vi bao quát mọi lần đọc Dữ liệu Khách hàng. Khách hàng có thể tự đọc và xuất dữ liệu thông qua nhật ký kiểm toán trong ứng dụng và API bên ngoài.