Declaração da ProcessMind sobre o registro de auditoria e SIEM

Data de vigência: 12 de novembro de 2026

Esta declaração descreve como a ProcessMind B.V. registra ações administrativas e relevantes para a segurança realizadas em relação aos Dados do Cliente (o "registro de auditoria"). Ela complementa as Medidas de Segurança, o Adendo de Tratamento de Dados, o Contrato do Cliente e a Lista de Subprocessadores.

---

1. Escopo

1.1 Um único registro de auditoria. A ProcessMind mantém um único registro de auditoria para ações administrativas e relevantes para a segurança realizadas em relação aos Dados do Cliente e ao Serviço ProcessMind. O registro de auditoria é separado dos registros operacionais (da aplicação), dos registros de acesso HTTP e do feed de atividades do produto; esses fluxos têm finalidades diferentes e não são apresentados como uma trilha de auditoria.

1.2 O que não é. O registro de auditoria não é um registro de cada leitura dos Dados do Cliente e não é o histórico de alterações do produto para modelos de processos, diagramas, documentação ou simulações. Esses itens são registrados no histórico de alterações de processos disponível dentro do produto.

---

2. Conteúdo de cada registro de auditoria

2.1 Campos. Cada registro contém os campos abaixo. O conjunto é fixado pelo esquema do registro: um registro não pode ganhar um campo que não esteja nesta lista, e uma ação não pode adicionar um campo que não tenha declarado no registro.

- *schemaVersion* (número): versão do esquema do registro, atualmente 1.
- *eventId* (string): identificador único do registro. Os novos registros usam um ULID; as linhas migradas do repositório anterior mantêm seu UUID.
- *occurredAt*, *ingestedAt* (carimbos de data e hora): quando a ação ocorreu e quando o gravador de auditoria armazenou o registro. Ambos em UTC.
- *eventClass* (enum): security, auth, admin, data, api, ai ou platform.
- *action* (enum): um código da lista fechada e revisada de ações, por exemplo, auth.login.blocked ou api.key.revoked.
- *outcome* (enum): success, failure, denied ou error.
- *severity* (enum): info, notice, warning ou critical, derivado do resultado. Uma ação bem-sucedida usa o valor padrão definido no registro (info, salvo indicação em contrário para a ação); uma falha é registrada como notice; e denied ou error como warning.
- *actor* (objeto): quem realizou a ação. type (user, apiKey, service, system ou anonymous), id, email, displayName e onBehalfOf, além de onBehalfOfEmail quando a ação foi realizada em nome de outra conta.
- *actorContext* (objeto): a sessão que realizou a ação. sessionId, authMethod (oidc, password, loginToken, apiKey ou none) e um indicador de sessão de suporte.
- *organizationId*, *tenantId* (identificadores, anuláveis): a organização e o ambiente aos quais a ação pertence. Nulo para registros que não dizem respeito a nenhum cliente ou que estão acima do ambiente.
- *resource* (objeto, anulável): o objeto afetado. type, id e name, em que type é um dos seguintes: apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant ou user.
- *source* (objeto): onde o registro foi produzido. service (api, externalApi, superadminApi, worker, cron ou webSocket), function e

version.

- *stage*, *region* (strings): o estágio de implantação que produziu o registro (por exemplo, prod) e a região da AWS (eu-central-1 para registros de clientes).
- *correlation* (objeto): requestId, traceId e parentEventId, que vinculam o registro à solicitação que o causou e aos registros anteriores no mesmo fluxo.
- *network* (objeto, anulável): sourceIp e userAgent. Capturados somente para as ações cuja entrada no registro permite essa captura: início de sessão, decisões de acesso, alterações administrativas e de configurações, uploads, downloads e exportações de dados, alterações de chaves de API e alterações de políticas de IA.
- *detail* (objeto): a carga útil própria da ação, validada de acordo com o esquema dessa ação. Os valores são apenas primitivos (string, number, boolean, null), para que o registro permaneça consultável e possa ter dados ocultados.

2.2 Vocabulário fechado. As ações são selecionadas de uma lista fixa e revisada de códigos de ação; não há mensagem em texto livre em um registro de auditoria. Cada ação também declara quais campos adicionais pode conter, de modo que um registro não possa adquirir silenciosamente um novo tipo de conteúdo.

---

3. Quais ações são registradas

3.1 Registradas atualmente. Entre outras, a ProcessMind registra:

- **Autenticação:** êxito e falha no início de sessão, início de sessão bloqueado (conta bloqueada, domínio não permitido, e-mail do provedor não verificado), encerramento de sessão, emissão e transferência de token de início de sessão.
- **Autorização:** recusas de acesso, incluindo cada credencial de API externa rejeitada, escopo e estado do tenant, e rejeições de origem

(CORS).

- **Acesso de suporte:** início de uma sessão de suporte da ProcessMind em uma conta de cliente, identificando tanto o operador quanto a conta afetada.
- **Credenciais de API:** criação, alteração de escopo e revogação de chaves de API, incluindo os escopos concedidos.
- **Administração de contas e funções:** criação de usuários, convites, edições de perfis de administrador, exclusões, concessões e revogações de funções e alterações de associação a tenants ou organizações.
- **Ciclo de vida da organização:** criação, exclusão, restauração, agendamento e cancelamento de exclusão e apagamento concluído.
- **Upload, download e exportação de dados:** upload, download e exclusão de artefatos, upload e atualização de dados tabulares, downloads de exportações, exclusão de tabelas de dados e criação, alteração e exclusão de webhooks (conexões).
- **Estado de cobrança:** alterações de plano, suspensão e recuperação decorrentes de pagamentos e cancelamento de assinatura.
- **Console do provedor da ProcessMind:** execução de consultas privilegiadas, administração de usuários e organizações, alterações de configurações e funcionalidades, solicitações de sincronização de cobrança e migrações.
- **Ações administrativas e destrutivas realizadas pelas tarefas agendadas da ProcessMind:** exclusões de tenants, organizações, usuários e leads, varreduras de retenção e falhas de pipeline.
- **Integridade do registro de auditoria:** falhas no próprio processo de gravação do registro de auditoria.

3.2 Edições no espaço de trabalho. As edições feitas dentro de um espaço de trabalho (modelos de processos, documentação, simulações, painéis, comentários e favoritos) são registradas no próprio histórico de alterações de processos do produto, não no registro de auditoria. O registro de

auditoria registra quem fez upload, download, exportou ou excluiu dados; o histórico de alterações registra o que mudou dentro de um modelo. A lista atual de códigos de ação registrados está disponível mediante solicitação à ProcessMind.

---

4. O que nunca é registrado

Senhas, tokens de autenticação, valores de chaves de API, cookies, cabeçalhos de autorização, corpos de solicitações ou respostas, conteúdo de arquivos, URLs pré-assinadas e prompts ou conclusões de IA nunca são gravados no registro de auditoria. Os registros de auditoria podem conter dados pessoais necessários para atribuição: o endereço de e-mail de um agente e o endereço IP de origem e o user agent para as ações cuja entrada no registro permite essa captura (início de sessão, decisões de acesso, alterações administrativas e de configurações, movimentação de dados, alterações de chaves de API e de políticas de IA). Os campos permitidos são definidos para cada ação e revisados quando uma ação é adicionada.

---

5. Integridade

5.1 Somente acréscimo. O registro de auditoria permite somente acréscimos. Nenhuma função da aplicação tem privilégio de atualização ou exclusão sobre ele, e uma restrição do banco de dados rejeita ambas as operações.

5.2 Um único gravador. Os registros são gravados por um único componente que valida o código da ação e sua carga útil antes da gravação. Um registro que não seja validado é rejeitado e reportado, em vez de ser gravado parcialmente.

5.3 Tratamento de falhas. Uma falha na gravação de auditoria nunca faz falhar a ação comercial que ela descreve. Ela é registrada em um

processo operacional com alarme, e o próprio registro é preservado em uma cópia secundária para que possa ser recuperado.

---

6. Retenção e localização

6.1 Retenção. Os registros de auditoria são retidos por pelo menos dez (10) anos a partir da data do evento.

6.2 Localização e criptografia. Os registros de auditoria são armazenados na União Europeia (Frankfurt, Alemanha, `eu-central-1`) e criptografados em repouso com uma chave AWS KMS gerenciada pelo cliente. Uma cópia ativa também é gravada em um grupo de logs do Amazon CloudWatch com acesso controlado, para que um incidente possa ser investigado enquanto estiver ocorrendo.

6.3 Sem replicação entre regiões. Os registros de auditoria não são replicados para fora da União Europeia.

---

7. Acesso aos registros de auditoria

7.1 Direito de acesso. O registro de auditoria no aplicativo está incluído no plano Process Architecture e nos planos superiores. Um administrador da organização pode ler toda a organização; um administrador com escopo de tenant pode ler seu próprio tenant. O escopo é derivado da sessão autenticada e verificado antes da consulta, de modo que uma solicitação não possa ampliá-lo para outro tenant ou organização.

7.2 Pessoal da ProcessMind. O pessoal da ProcessMind acessa os registros de auditoria somente para suporte, resposta a incidentes ou cumprimento de uma obrigação legal, com base na necessidade de conhecimento. O acesso entre clientes é restrito a uma função de suporte dedicada, e o próprio acesso é uma ação administrativa.

7.3 Como obter registros. Administradores de organizações e tenants podem ler seus registros de auditoria no registro de auditoria do aplicativo

e obtê-los ou exportá-los pela API externa. Para uma solicitação maior ou assistida, o suporte da ProcessMind fornece os registros em CSV ou JSON para uma organização, tenant e período especificados, com prazo-alvo de cinco (5) dias úteis para uma solicitação padrão.

---

8. Exclusão de registros de auditoria

8.1 Mediante solicitação. Mediante solicitação por escrito verificada, a ProcessMind apaga os registros de auditoria pertencentes a uma organização de cliente do repositório de auditoria e confirma o apagamento por escrito. A cópia operacional do CloudWatch não pode ser editada registro por registro; ela expira de acordo com seu próprio período de retenção.

8.2 O que é retido. O registro de que o apagamento ocorreu (identificador da organização, data, solicitante, motivo e número de registros removidos) é retido como um registro de auditoria no nível da plataforma e não contém Dados do Cliente. Os registros que não pertencem a nenhum cliente (eventos da plataforma ProcessMind) não são afetados por uma solicitação de apagamento de cliente.

8.3 Solicitações de apagamento individuais. Quando uma solicitação diz respeito a um indivíduo de um cliente que permanece ativo, o registro de segurança é retido para o estabelecimento, exercício ou defesa de reivindicações legais, conforme permitido pelo Artigo 17(3)(b) e (e) do GDPR; essa base é registrada no registro das atividades de tratamento e na Política de Privacidade.

---

9. Integração e exportação de SIEM

9.1 Disponibilidade. O arquivo imutável de auditoria é uma opção Enterprise, habilitada para uma organização de cliente mediante solicitação. Ele grava diariamente objetos NDJSON compactados sob um

prefixo por organização em um bucket S3 com Object Lock (WORM), com um manifesto e reconciliação noturna.

9.2 Entrega atual. Atualmente, a ProcessMind não oferece um conector SIEM nativo nem um feed push. A entrega é pull, por meio de três interfaces: a API de leitura (`GET /v1/tenant/{tenantId}/audit`), a tarefa de exportação limitada (crie-a com `POST /v1/tenant/{tenantId}/audit/exports` e obtenha o resultado na chamada de status, que retorna uma URL de download de curta duração) e, com o arquivo Enterprise, os objetos diários sob o próprio prefixo da organização no bucket com Object Lock, que o SIEM do cliente lê por meio de um acordo de acesso. A ProcessMind não entrega registros, segundo seu próprio cronograma, em um local escolhido pelo cliente.

9.3 Monitoramento próprio da ProcessMind. O monitoramento de segurança da ProcessMind consome os mesmos registros: falhas de gravação de auditoria, rajadas de falhas de autenticação, alterações de privilégios e ações administrativas destrutivas geram alertas internos.

---

10. Evidências disponíveis aos clientes

Mediante solicitação e, quando aplicável, sob confidencialidade, a ProcessMind fornece esta declaração, as Medidas de Segurança, o Adendo de Tratamento de Dados, a Lista de Subprocessadores, uma amostra redigida de registros de auditoria e o procedimento usado para solicitações de acesso e apagamento.

---

11. Limitações

Para evitar dúvidas, a ProcessMind declara manter um repositório de auditoria somente para acréscimos para cada organização e, quando o direito ao arquivo de auditoria estiver habilitado, uma cópia com Object Lock (WORM), com reconciliação noturna do manifesto. A ProcessMind não declara atualmente manter uma cadeia de hashes, um conector SIEM

nativo de envio em tempo real, ocultação de dados de registros de auditoria por usuário, uma atestação ISO 27001 ou SOC 2 que abranja esse controle, nem cobertura de cada leitura dos Dados do Cliente. A leitura e exportação por autosserviço do cliente estão disponíveis por meio do registro de auditoria no aplicativo e da API externa.