Declaración de ProcessMind sobre el registro de auditoría y SIEM

Fecha de entrada en vigor: 12 de noviembre de 2026

Esta declaración describe cómo ProcessMind B.V. registra las acciones administrativas y relevantes para la seguridad realizadas en relación con los Datos del Cliente (el «registro de auditoría»). Complementa las Medidas de seguridad, el Anexo de tratamiento de datos, el Acuerdo con el cliente y la Lista de subencargados.

---

1. Ámbito de aplicación

1.1 Un único registro de auditoría. ProcessMind mantiene un único registro de auditoría de las acciones administrativas y relevantes para la seguridad realizadas en relación con los Datos del Cliente y el Servicio de ProcessMind. El registro de auditoría es independiente del registro operativo (de la aplicación), del registro de acceso HTTP y del feed de actividad del producto; esos flujos tienen fines distintos y no se presentan como un registro de auditoría.

1.2 Lo que no es. El registro de auditoría no registra todas las lecturas de los Datos del Cliente ni constituye el historial de cambios del producto para los modelos de procesos, diagramas, documentación o simulaciones. Estos se registran en el historial de cambios de procesos disponible dentro del producto.

---

2. Contenido de cada registro de auditoría

2.1 Campos. Cada registro contiene los campos que se indican a continuación. El conjunto está fijado por el esquema del registro: no se puede añadir un campo que no figure en esta lista, y una acción no puede añadir un campo que no haya declarado en el registro.

- *schemaVersion* (número): versión del esquema del registro, actualmente 1.
- *eventId* (cadena): identificador único del registro. Los registros nuevos utilizan un ULID; las filas migradas del almacén anterior conservan su UUID.
- *occurredAt*, *ingestedAt* (marcas de tiempo): cuándo tuvo lugar la acción y cuándo el componente de escritura de auditoría almacenó el registro. Ambas en UTC.
- *eventClass* (enumeración): security, auth, admin, data, api, ai o platform.
- *action* (enumeración): un código de la lista cerrada y revisada de acciones, por ejemplo, auth.login.blocked o api.key.revoked.
- *outcome* (enumeración): success, failure, denied o error.
- *severity* (enumeración): info, notice, warning o critical, derivado del resultado. Una acción satisfactoria utiliza el valor predeterminado de su registro (info, salvo que la acción indique otra cosa); los fallos se registran como notice y los resultados denied o error como warning.
- *actor* (objeto): quién realizó la acción. type (user, apiKey, service, system o anonymous), id, email, displayName y onBehalfOf, además de onBehalfOfEmail cuando la acción se realizó en nombre de otra cuenta.
- *actorContext* (objeto): la sesión desde la que se realizó la acción. sessionId, authMethod (oidc, password, loginToken, apiKey o none) y un indicador de sesión de asistencia.
- *organizationId*, *tenantId* (identificadores, anulables): la organización y el entorno a los que pertenece la acción. Nulos en los registros que no se refieren a ningún cliente o que se sitúan por encima del entorno.
- *resource* (objeto, anulable): el objeto afectado. type, id y name, donde type es uno de los siguientes: apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant o user.

- *source* (objeto): dónde se generó el registro. service (api, externalApi, superadminApi, worker, cron o webSocket), function y version.
- *stage*, *region* (cadenas): la fase de despliegue que generó el registro (por ejemplo, prod) y la región de AWS (eu-central-1 para los registros de clientes).
- *correlation* (objeto): requestId, traceId y parentEventId, que vinculan el registro con la solicitud que lo causó y con los registros anteriores del mismo flujo.
- *network* (objeto, anulable): sourceIp y userAgent. Se capturan únicamente para las acciones cuyo registro correspondiente así lo permite: inicio de sesión, decisiones de acceso, cambios administrativos y de configuración, cargas de datos, descargas y exportaciones, cambios de claves de API y cambios de políticas de IA.
- *detail* (objeto): la carga propia de la acción, validada conforme al esquema de dicha acción. Los valores son únicamente primitivos (cadena, número, booleano o nulo), de modo que el registro siga siendo consultable y se puedan suprimir datos.

2.2 Vocabulario cerrado. Las acciones se seleccionan de una lista fija y revisada de códigos; los registros de auditoría no contienen mensajes de texto libre. Cada acción también declara qué campos adicionales puede contener, de modo que no se puedan añadir silenciosamente nuevos tipos de contenido a un registro.

---

3. Acciones que se registran

3.1 Registros actuales. ProcessMind registra, entre otras, las siguientes acciones:

- **Autenticación:** inicios de sesión satisfactorios y fallidos, inicios de sesión bloqueados (cuenta bloqueada, dominio no permitido,

correo electrónico del proveedor no verificado), cierre de sesión, emisión y transferencia de tokens de inicio de sesión.

- **Autorización:** denegaciones de acceso, incluidas todas las credenciales de API externa rechazadas, el ámbito y el estado del tenant, y los rechazos de origen (CORS).
- **Acceso de asistencia:** inicio de una sesión de asistencia de ProcessMind en una cuenta de cliente, con identificación tanto del operador como de la cuenta afectada.
- **Credenciales de API:** creación, cambio de ámbito y revocación de claves de API, incluidos los ámbitos concedidos.
- **Administración de cuentas y roles:** creación de usuarios, invitaciones, modificaciones de perfiles de administrador, eliminación, concesión y revocación de roles, y cambios de pertenencia a tenants u organizaciones.
- **Ciclo de vida de la organización:** creación, eliminación, restauración, programación y cancelación de la eliminación, y supresión completada.
- **Carga, descarga y exportación de datos:** carga, descarga y eliminación de artefactos; carga y actualización de datos tabulares; descargas de exportaciones; eliminación de tablas de datos; y creación, modificación y eliminación de webhooks (conexiones).
- **Estado de facturación:** cambios de plan, suspensión y restablecimiento por motivos de pago, y cancelación de suscripciones.
- **Consola del proveedor de ProcessMind:** ejecución de consultas con privilegios, administración de usuarios y organizaciones, cambios de configuración y funcionalidades, solicitudes de sincronización de facturación y migraciones.
- **Acciones administrativas y destructivas de los trabajos programados de ProcessMind:** eliminaciones de tenants, organizaciones, usuarios y clientes potenciales, procesos de depuración de datos conforme a los plazos de conservación y fallos de canalizaciones.

- **Integridad del registro de auditoría:** fallos del propio proceso de escritura del registro de auditoría.

3.2 Modificaciones del espacio de trabajo. Las modificaciones realizadas dentro de un espacio de trabajo (modelos de procesos, documentación, simulaciones, Dashboard, comentarios y marcadores) se registran en el historial de cambios de procesos propio del producto, no en el registro de auditoría. El registro de auditoría registra quién cargó, descargó, exportó o eliminó datos; el historial de cambios registra qué se modificó dentro de un modelo. ProcessMind facilita, previa solicitud, la lista actual de códigos de acciones registradas.

---

4. Lo que nunca se registra

Las contraseñas, los tokens de autenticación, los valores de las claves de API, las cookies, los encabezados de autorización, los cuerpos de solicitudes o respuestas, el contenido de archivos, las URL prefirmadas y las instrucciones o respuestas de IA nunca se escriben en el registro de auditoría. Los registros de auditoría pueden contener datos personales necesarios para atribuir las acciones: la dirección de correo electrónico del actor y la dirección IP de origen y el agente de usuario para las acciones cuyo registro correspondiente así lo permite (inicio de sesión, decisiones de acceso, cambios administrativos y de configuración, movimiento de datos, cambios de claves de API y de políticas de IA). Los campos permitidos se definen para cada acción y se revisan cuando se añade una acción.

---

5. Integridad

5.1 Solo anexión. El registro de auditoría solo permite anexar registros. Ningún rol de aplicación tiene privilegios para actualizarlo o eliminarlo, y una restricción de la base de datos rechaza ambas operaciones.

5.2 Un único componente de escritura. Los registros los escribe un único componente que valida el código de acción y su carga antes de escribirlos. Los registros que no superan la validación se rechazan y se notifican, en lugar de escribirse parcialmente.

5.3 Gestión de fallos. Un fallo al escribir en el registro de auditoría nunca provoca el fallo de la acción empresarial que describe. Se registra mediante un proceso operativo con alertas, y el propio registro se conserva en una copia secundaria para que pueda recuperarse.

---

6. Conservación y ubicación

6.1 Conservación. Los registros de auditoría se conservan durante al menos diez (10) años a partir de la fecha del evento.

6.2 Ubicación y cifrado. Los registros de auditoría se almacenan en la Unión Europea (Fráncfort, Alemania, `eu-central-1`) y se cifran en reposo con una clave de AWS KMS gestionada por el cliente. También se escribe una copia activa en un grupo de registros de Amazon CloudWatch con acceso controlado, para que se pueda investigar un incidente mientras está ocurriendo.

6.3 Sin replicación entre regiones. Los registros de auditoría no se replican fuera de la Unión Europea.

---

7. Acceso a los registros de auditoría

7.1 Derecho de acceso. El registro de auditoría integrado en la aplicación está incluido en el plan Process Architecture y los planes superiores. Un administrador de organización puede consultar toda la organización; un administrador con ámbito de tenant puede consultar su propio tenant. El ámbito se deriva de la sesión autenticada y se comprueba antes de la consulta, por lo que una solicitud no puede ampliarlo a otro tenant u organización.

7.2 Personal de ProcessMind. El personal de ProcessMind accede a los registros de auditoría únicamente para prestar asistencia, responder a incidentes o cumplir una obligación legal, y solo cuando sea necesario conocerlos. El acceso entre clientes está restringido a un rol de asistencia específico, y dicho acceso constituye en sí mismo una acción administrativa.

7.3 Cómo obtener los registros. Los administradores de organizaciones y tenants pueden consultar sus registros de auditoría en el registro integrado en la aplicación y obtenerlos o exportarlos mediante la API externa. Para solicitudes de mayor volumen o que requieran asistencia, el equipo de asistencia de ProcessMind proporciona los registros en formato CSV o JSON para una organización, un tenant y un intervalo de tiempo especificados; el plazo previsto para una solicitud estándar es de cinco (5) días hábiles.

---

8. Eliminación de registros de auditoría

8.1 A solicitud. Tras recibir una solicitud escrita verificada, ProcessMind elimina del almacén de auditoría los registros pertenecientes a la organización del cliente y confirma por escrito la eliminación. La copia operativa de CloudWatch no se puede editar registro por registro; caduca conforme a su propio plazo de conservación.

8.2 Información que se conserva. El registro de que se llevó a cabo la eliminación (identificador de la organización, fecha, solicitante, motivo y número de registros eliminados) se conserva como registro de auditoría a nivel de plataforma y no contiene Datos del Cliente. Los registros que no pertenecen a ningún cliente (eventos de la plataforma de ProcessMind) no se ven afectados por una solicitud de eliminación de un cliente.

8.3 Solicitudes de supresión individuales. Cuando una solicitud se refiere a una persona de un cliente que sigue activo, el registro de seguridad se conserva para la formulación, el ejercicio o la defensa de reclamaciones legales, según lo permitido por el artículo 17(3)(b) y (e) del RGPD; dicha

base se hace constar en el registro de actividades de tratamiento y en la Política de privacidad.

---

9. Integración y exportación de SIEM

9.1 Disponibilidad. El archivo de auditoría inmutable es una opción Enterprise que se habilita para la organización de un cliente previa solicitud. Escribe diariamente objetos NDJSON comprimidos bajo un prefijo por organización en un bucket S3 con Object Lock (WORM), con un manifiesto y una conciliación nocturna.

9.2 Entrega actual. Actualmente, ProcessMind no ofrece un conector SIEM nativo ni un feed de envío. La entrega se realiza mediante extracción desde tres interfaces: la API de lectura (`GET /v1/tenant/{tenantId}/audit`), el trabajo de exportación con límites (créelo con `POST /v1/tenant/{tenantId}/audit/exports` y obtenga el resultado mediante su llamada de estado, que devuelve una URL de descarga de corta duración) y, con el archivo Enterprise, los objetos diarios bajo el prefijo propio de la organización en el bucket con Object Lock, que el SIEM del cliente lee mediante un acuerdo de acceso. ProcessMind no entrega registros por iniciativa propia en una ubicación elegida por el cliente ni según un calendario establecido por este.

9.3 Supervisión propia de ProcessMind. La supervisión de seguridad de ProcessMind utiliza los mismos registros: los fallos de escritura en el registro de auditoría, los aumentos repentinos de fallos de autenticación, los cambios de privilegios y las acciones administrativas destructivas generan alertas internas.

---

10. Evidencias disponibles para los clientes

Previa solicitud y, cuando corresponda, bajo obligación de confidencialidad, ProcessMind proporciona esta declaración, las Medidas de seguridad, el Anexo de tratamiento de datos, la Lista de

subencargados, una muestra de registros de auditoría con datos suprimidos y el procedimiento utilizado para las solicitudes de acceso y supresión.

---

11. Limitaciones

Para evitar cualquier duda, ProcessMind declara que mantiene un almacén de auditoría que solo permite anexar registros para cada organización y, cuando está habilitado el derecho al archivo de auditoría, una copia con Object Lock (WORM) y conciliación nocturna del manifiesto. Actualmente, ProcessMind no declara disponer de una cadena de hashes, un conector nativo de envío en tiempo real a SIEM, supresión de datos de registros de auditoría por usuario, una certificación ISO 27001 o SOC 2 que cubra este control, ni cobertura de todas las lecturas de los Datos del Cliente. Los clientes pueden consultar y exportar sus registros por sí mismos mediante el registro de auditoría integrado en la aplicación y la API externa.