Medidas de Seguridad de ProcessMind

Fecha de entrada en vigor: 14 de septiembre de 2026

Este documento describe las medidas técnicas y organizativas («TOM») que ProcessMind B.V. mantiene para proteger la confidencialidad, integridad y disponibilidad de los Datos del Cliente. ProcessMind sigue un enfoque de defensa en profundidad, en el que múltiples capas de seguridad independientes protegen los Datos del Cliente en todos los niveles: desde la red y la infraestructura hasta la identidad, la autorización, el aislamiento de datos, el cifrado, la supervisión y el desarrollo de software. Estas medidas complementan el Anexo de Tratamiento de Datos, la Política de Privacidad y la Política de Alojamiento SaaS. ProcessMind revisa y actualiza estas medidas al menos una vez al año.

Los Datos del Cliente nunca se venden, comparten ni utilizan por terceros para sus propios fines.

---

1. Seguridad de la infraestructura

1.1 Plataforma en la nube. ProcessMind está alojado exclusivamente en Amazon Web Services (AWS) en la UE (Fráncfort, Alemania, `eu-central-1`). AWS mantiene las certificaciones ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 y PCI DSS. Consulte Programas de cumplimiento de AWS para obtener la lista completa.

1.2 Arquitectura sin servidor. La lógica de la aplicación de ProcessMind se ejecuta en AWS Lambda y servicios administrados por AWS. ProcessMind no opera servidores de aplicaciones de larga duración administrados por clientes, lo que elimina una gran parte de las tareas de aplicación de parches del sistema operativo y refuerzo de servidores.

1.3 Límites de red. ProcessMind mantiene una VPC de AWS para los controles de bases de datos y de red. Aurora PostgreSQL se ejecuta en subredes privadas sin salida a Internet, no es accesible públicamente y los

registros de flujo de la VPC están habilitados. ProcessMind no coloca las funciones Lambda de la aplicación dentro de la VPC de forma predeterminada. Las funciones Lambda acceden a Aurora mediante la API de datos de AWS RDS a través de TLS, utilizando autenticación de IAM y Secrets Manager.

1.4 Entrega de contenido y controles perimetrales. El sitio web orientado al cliente, la SPA frontend y el tráfico de recursos públicos se sirven mediante Amazon CloudFront. Todas las distribuciones de CloudFront aplican una política TLS mínima de TLS 1.2 (2021). Las distribuciones del sitio web y de la SPA frontend también añaden encabezados de respuesta de seguridad, incluidos HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, política de referencia y política de permisos. La distribución de recursos públicos utiliza CloudFront Origin Access Control para mantener privado el bucket de origen. El tráfico de la API orientado al cliente se gestiona por separado mediante Amazon API Gateway: el tráfico de solicitud/respuesta HTTPS se sirve mediante una API HTTP en un subdominio de API dedicado, y las conexiones de clientes en tiempo real se sirven mediante una API WebSocket de API Gateway independiente en un subdominio WebSocket dedicado.

1.5 Segregación de entornos. Los entornos de producción y desarrollo utilizan cuentas de AWS, bases de datos y pilas de infraestructura independientes. Las credenciales de los desarrolladores no proporcionan acceso a los Datos del Cliente de producción.

---

2. Cifrado de datos

2.1 Cifrado en tránsito. Todos los datos transmitidos entre los clientes y los servicios de ProcessMind se cifran mediante TLS 1.2 o superior. Los endpoints orientados al cliente se exponen mediante HTTPS. Los buckets de S3, los temas de SNS y las colas de SQS creados directamente por ProcessMind aplican acceso exclusivo mediante SSL. El acceso a la base

de datos a través de la API de datos de RDS y otras llamadas a servicios de AWS utiliza HTTPS/TLS.

2.2 Cifrado en reposo. Aurora PostgreSQL está cifrado en reposo mediante claves de AWS KMS administradas por el cliente, con rotación automática de claves. Los buckets de S3 de datos de clientes y operativos creados directamente por ProcessMind, incluidos los buckets de cargas, recursos y registros de acceso, utilizan claves de KMS administradas por el cliente. Los grupos de registros de CloudWatch, los temas de SNS y las colas de SQS creados directamente por ProcessMind también utilizan claves de KMS administradas por el cliente. Los buckets de origen del sitio web y de la SPA frontend administrados por SST utilizan cifrado del lado del servidor de S3 administrado por AWS (SSE-S3 / AES-256), en lugar de claves de KMS administradas por el cliente.

2.3 Gestión de claves y secretos. Las claves de cifrado de la base de datos se gestionan de forma centralizada mediante AWS KMS y el acceso a las claves se rige por políticas de IAM que siguen los principios de mínimo privilegio. Las credenciales de la base de datos se almacenan en AWS Secrets Manager. El secreto maestro de Aurora y el secreto restringido del usuario de la aplicación rotan automáticamente cada treinta (30) días. Las claves y los secretos de producción nunca se almacenan en el código fuente; las credenciales exclusivas de desarrollo están aisladas de la producción. Algunos recursos auxiliares gestionados por AWS/CDK/SST siguen utilizando cifrado administrado por AWS cuando el servicio o el framework no expone una configuración de claves administradas por el cliente.

---

3. Aislamiento y residencia de los datos

3.1 Aislamiento de tenants. Cada tenant del cliente recibe una instancia de base de datos dedicada y aislada. Los Datos del Cliente nunca se mezclan con los datos de otros clientes a nivel de base de datos. Los metadatos compartidos (por ejemplo, registros de cuentas, facturación y

asignaciones de usuarios a tenants) se almacenan en una base de datos multi-tenant independiente con controles de acceso estrictos. Las tablas compartidas cuyo ámbito corresponde a tenants y organizaciones están además protegidas por políticas de seguridad a nivel de fila (RLS) de PostgreSQL, aplicadas mediante un contexto de base de datos específico de cada solicitud.

3.2 Residencia de los datos. Todos los Datos del Cliente, incluidas las bases de datos, las cargas de archivos, las copias de seguridad y los resultados de consultas, se almacenan exclusivamente en la UE (Fráncfort, Alemania). Cuando se contrata a un subencargado ubicado fuera del EEE para una actividad de tratamiento específica (por ejemplo, el tratamiento de modelos de IA o el procesamiento de pagos), la transferencia está cubierta por un mecanismo de transferencia adecuado, según se describe en el Anexo de Tratamiento de Datos, y el subencargado y su ubicación de tratamiento figuran en la Lista de Subencargados.

3.3 Conservación y eliminación de datos. Los plazos de conservación y eliminación se establecen en la Sección 6 del Anexo de Tratamiento de Datos. Los clientes pueden eliminar sus datos en cualquier momento mediante la aplicación o poniéndose en contacto con ProcessMind. Las copias de seguridad se eliminan cuando vencen los períodos de conservación de copias de seguridad aplicables (Sección 7.1).

---

4. Gestión de identidades y accesos

4.1 Autenticación. ProcessMind admite el inicio de sesión único (SSO) mediante Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC y LinkedIn OAuth 2.0/OIDC. ProcessMind actúa como parte que confía y no almacena contraseñas de usuarios. La autenticación multifactor es aplicada por el proveedor de identidad; por ejemplo, cuando una organización conecta Microsoft Entra ID (Azure AD), se aplican las propias políticas de MFA y acceso de dicha organización.

4.2 Gestión de sesiones. Las sesiones del navegador utilizan JSON Web Tokens (JWT) firmados, transmitidos mediante cookies seguras con los atributos HttpOnly, SameSite y Secure. Las firmas de los tokens se validan en cada solicitud autenticada.

4.3 Modelo de autorización. ProcessMind no depende de los autorizadores nativos de API Gateway para sus API principales de la aplicación. La autorización se aplica en wrappers compartidos de los controladores Lambda que validan el estado de la sesión y el ámbito del tenant antes de que se ejecute la lógica empresarial. Las rutas públicas están expresamente incluidas en una lista de permitidos para flujos no autenticados, webhooks, ingesta de eventos y preflight de CORS. Los endpoints de API externos utilizan controladores de autenticación dedicados. El acceso a los Datos del Cliente está limitado al contexto del tenant o de la organización autenticados.

4.4 Mínimo privilegio. Los sistemas internos siguen el principio de mínimo privilegio. Las funciones de IAM se limitan a los recursos mínimos necesarios cuando el framework permite una delimitación precisa. Algunas funciones generadas por SST/CDK utilizan políticas administradas o insertadas más amplias para vinculaciones y operaciones en tiempo de ejecución; estos casos se revisan, se limitan a recursos cuando es posible y se registran como excepciones explícitas.

4.5 Controles de acceso de los empleados. El acceso de los empleados a los sistemas internos se gestiona mediante Active Directory con SSO y MFA obligatoria. El control de acceso basado en roles (RBAC) garantiza que el acceso a los Datos del Cliente se limite al personal autorizado que lo necesite para sus funciones. Los derechos de acceso se revisan periódicamente.

---

5. Registro, supervisión y auditoría

5.1 Registro centralizado. El registro de acceso a la API HTTP y el registro de acceso a WebSocket están habilitados con campos JSON estructurados y

se escriben en Amazon CloudWatch Logs, con una conservación de una (1) semana. Esos grupos de registros de acceso están cifrados con una clave de AWS KMS administrada por el cliente. Los registros de la aplicación se centralizan en grupos de registros de Amazon CloudWatch cifrados con una clave de AWS KMS administrada por el cliente y se conservan durante diez (10) años. Los grupos de registros independientes de auditoría y telemetría también están cifrados con una clave de AWS KMS administrada por el cliente y se conservan durante diez (10) años. El grupo de exportación de registros del motor Aurora PostgreSQL se conserva durante una (1) semana.

5.2 Qué se registra y qué no. ProcessMind registra los eventos de acceso a la API HTTP y a WebSocket, incluidos la hora de la solicitud, los identificadores de solicitud, la ruta o el path, el estado de respuesta, la latencia, la IP de origen y el agente de usuario. ProcessMind también registra eventos de autenticación, rutas de fallo asíncronas y la actividad auxiliar de la aplicación Lambda en grupos de registros de CloudWatch centralizados. Los registros de flujo de la VPC están habilitados. Actualmente, ProcessMind no habilita el registro de acceso estándar de CloudFront en las distribuciones del sitio web, la SPA frontend o los recursos públicos.

5.3 Supervisión y alertas. Las alarmas y los Dashboard de CloudWatch supervisan el estado del sistema, las colas de mensajes no entregados y los fallos relevantes para la seguridad. Los fallos del procesamiento asíncrono se dirigen a colas de mensajes no entregados cifradas (retención de catorce (14) días; dos (2) días para las colas de miniaturas y de índices de búsqueda), y las alarmas de las DLQ activan notificaciones de SNS para su investigación. Además, ProcessMind utiliza Sentry para el seguimiento de errores del frontend en tiempo real, la supervisión del rendimiento y la reproducción de sesiones. Las reproducciones de sesiones solo se registran para las sesiones en las que se produce un error, y el texto, las entradas de formularios y los archivos multimedia se enmascaran o bloquean en las reproducciones. Los datos de Sentry se

incorporan en la UE (Fráncfort) y se limitan a los Datos de uso de ProcessMind (errores del navegador, trazas de rendimiento, metadatos del dispositivo y grabaciones de reproducciones enmascaradas). Sentry figura en la lista de subencargados del tratamiento.

5.4 Protección de registros. Los registros se almacenan en grupos de registros de CloudWatch dedicados y con acceso controlado, y se cifran en reposo. Los registros de producción y desarrollo están separados mediante límites de entorno y de cuenta.

---

6. Validación automatizada de controles y gestión de vulnerabilidades

6.1 Qué hace ProcessMind. ProcessMind ejecuta `cdk-nag` como parte de su flujo de síntesis y despliegue de infraestructura, utilizando varios paquetes de reglas del sector (incluidos AWS Solutions, NIST 800-53 y PCI DSS). Se generan informes por pila y se revisan como parte de la gestión de cambios de infraestructura. Los hallazgos se clasifican como corregidos, riesgo aceptado o mejora planificada.

6.2 Cómo se gestionan las excepciones. Las supresiones se registran en un registro central cuando el framework lo permite, se limitan a las pilas afectadas y requieren una justificación por escrito; cuando una pila contiene una supresión insertada, esta se documenta junto con dicha pila. Cuando se corrige un hallazgo, la supresión correspondiente se actualiza o elimina. ProcessMind no considera la supresión como una exclusión general de la revisión.

6.3 Qué no hace actualmente ProcessMind. ProcessMind realiza el seguimiento y la revisión de las excepciones sustanciales a los controles de infraestructura. Las principales son:

- Las Lambdas de aplicación no se colocan dentro de la VPC de forma predeterminada; acceden a Aurora mediante la RDS Data API a través de TLS, con autenticación de IAM y Secrets Manager

- la WebSocket API y las distribuciones estáticas no están protegidas por AWS WAF (las conexiones WebSocket utilizan tokens HMAC de corta duración; las restricciones geográficas relacionadas con los pagos se aplican en el sistema de pagos), y las distribuciones estáticas no tienen habilitado el registro de acceso estándar de CloudFront
- la recuperación de la base de datos depende de las copias de seguridad automatizadas y la recuperación a un momento dado de Aurora, en lugar de un plan independiente de AWS Backup o de Aurora Enhanced Monitoring
- no existe replicación de S3 entre regiones ni S3 Object Lock para los buckets mutables
- algunos recursos auxiliares gestionados por AWS/CDK/SST utilizan cifrado gestionado por AWS o políticas de IAM generadas más amplias cuando el servicio no ofrece una alternativa controlada por el cliente

El registro completo de supresiones se mantiene junto con el código de infraestructura y está disponible previa solicitud. El uso de `cdk-nag` paquetes de reglas constituye una validación de controles de ingeniería, no una certificación externa, una opinión de auditoría ni una declaración legal de cumplimiento de HIPAA, NIST o PCI DSS.

6.4 Gestión de dependencias. Las dependencias de software se supervisan continuamente para detectar vulnerabilidades conocidas. Las vulnerabilidades críticas y de alta gravedad se corrigen con un objetivo de siete (7) días. Las dependencias se actualizan periódicamente.

6.5 Ciclo de vida de desarrollo de software seguro (SDLC). ProcessMind sigue un enfoque de defensa en profundidad para el desarrollo de software. Todo cambio en producción debe superar varias capas independientes de validación automatizada antes de su implementación:

- **Análisis estático y seguridad de tipos:** el modo estricto de TypeScript y ESLint aplican la corrección de tipos, la seguridad frente

a valores nulos y patrones de codificación relevantes para la seguridad en tiempo de compilación.

- **Revisión de código asistida por IA:** el análisis asistido por IA proporciona una perspectiva de revisión adicional sobre las solicitudes de incorporación de cambios para identificar riesgos de seguridad, errores lógicos y desviaciones de las convenciones, complementando las pruebas automatizadas.
- **Pruebas unitarias y de integración:** un conjunto completo de pruebas de Vitest valida la lógica empresarial, los patrones de acceso a datos, el comportamiento de la API y la gestión de errores frente a recursos de AWS activos en el entorno de desarrollo.
- **Pruebas de extremo a extremo:** las pruebas de navegador basadas en Playwright verifican flujos de trabajo críticos de los usuarios, incluida la autenticación, la carga de datos, el modelado de procesos, la simulación y el aislamiento multiinquilino.
- **Análisis de cumplimiento de la infraestructura:** `cdk-nag` valida la infraestructura como código frente a varios marcos de cumplimiento en cada cambio.
- **Análisis de vulnerabilidades de dependencias:** las auditorías automatizadas de dependencias impiden que vulnerabilidades críticas y de alta gravedad conocidas lleguen a producción.

La revisión humana se centra en la arquitectura, los límites de seguridad y las decisiones de diseño, en lugar de en la inspección del código línea por línea. Cuando intervienen cambios estructurales, sensibles desde el punto de vista de la seguridad o de infraestructura, se requiere la aprobación expresa de una persona además de la validación automatizada.

Todas las capas de validación se aplican mediante CI como controles obligatorios para la fusión de cambios en la rama principal. Las correcciones urgentes en producción pueden omitir el control de CI, pero deben ir seguidas de una ejecución completa de la canalización y una revisión posterior al incidente en un plazo de veinticuatro (24) horas.

---

7. Copias de seguridad y recuperación ante desastres

7.1 Copias de seguridad automatizadas. Amazon Aurora realiza copias de seguridad continuas y automatizadas con un periodo de conservación de siete (7) días. Las copias de seguridad se cifran utilizando las mismas claves de KMS gestionadas por el cliente que las bases de datos de origen.

7.2 Recuperación a un momento dado. Aurora admite la recuperación a un momento dado hasta cualquier segundo dentro del periodo de conservación de las copias de seguridad, lo que permite una restauración rápida en caso de corrupción de datos o eliminación accidental.

7.3 Durabilidad y control de versiones de S3. Las cargas de archivos y los artefactos operativos se almacenan en Amazon S3, que proporciona una durabilidad del 99.999999999 % (11 nueves). El control de versiones está habilitado en el bucket de cargas y en los buckets de recursos para permitir la recuperación y las reversiones. Los buckets de implementación del sitio web y del frontend son artefactos de compilación reproducibles y no se consideran un sistema de copias de seguridad. ProcessMind no habilita actualmente la replicación de S3 entre regiones.

7.4 Continuidad empresarial. Los procedimientos de recuperación ante desastres están documentados y se prueban periódicamente. Hay un resumen disponible en el documento Disaster Recovery, Business Continuity & Incident Response. La arquitectura depende de servicios gestionados de AWS dentro de la `eu-central-1` región, que AWS opera en varias zonas de disponibilidad; el clúster de Aurora ejecuta actualmente una única instancia escritora, por lo que la recuperación de la base de datos depende de las copias de seguridad automatizadas y la recuperación a un momento dado, en lugar de una instancia en espera dentro de la región. Las copias de seguridad de Aurora, la durabilidad de S3, las colas de mensajes no entregados y los activos estáticos reconstruibles a partir del origen forman parte de la estrategia de recuperación.

8. Respuesta a incidentes

8.1 Notificación de incidentes. En caso de un Incidente de Seguridad (según se define en el DPA), ProcessMind notificará a los clientes afectados sin demora indebida y, cuando sea posible, en un plazo de setenta y dos (72) horas desde que tenga conocimiento del incidente.

8.2 Gestión de incidentes. ProcessMind mantiene procedimientos documentados de respuesta a incidentes que abarcan la identificación, la contención, la erradicación, la recuperación y la revisión posterior al incidente. Hay un resumen disponible en el documento Disaster Recovery, Business Continuity & Incident Response. Las lecciones aprendidas de los incidentes se incorporan a los controles y procesos de seguridad.

8.3 Comunicación. Las notificaciones de incidentes incluyen la naturaleza y el alcance del incidente, las categorías de datos afectadas, las medidas adoptadas para contener el incidente y las acciones recomendadas para el cliente.

---

9. Medidas organizativas

9.1 Gestión de la seguridad de la información. ProcessMind mantiene un sistema de gestión de la seguridad de la información alineado con los principios de ISO 27001. ProcessMind ha seleccionado su vía de certificación para la certificación ISO 27001 y la atestación SOC 2 Type II; el proceso formal de certificación aún no ha comenzado.

9.2 Concienciación sobre seguridad. Todo el personal con acceso a Datos del Cliente recibe formación de concienciación sobre seguridad. Las mejores prácticas de seguridad están integradas en la incorporación, los flujos de trabajo de desarrollo y los procedimientos operativos.

9.3 Gestión de proveedores y subencargados. Los subencargados están obligados contractualmente a cumplir normas de protección de datos equivalentes a las descritas en este documento. ProcessMind mantiene una lista pública de subencargados y proporciona un preaviso de al

menos treinta (30) días antes de contratar a un nuevo subencargado. Los subencargados se revisan anualmente para verificar el cumplimiento.

9.4 Confidencialidad. Todo el personal autorizado a tratar Datos del Cliente está sujeto a obligaciones de confidencialidad por escrito.

---

10. Cumplimiento y certificaciones

Marco / Norma	Estado
RGPD (Reglamento General de Protección de Datos de la UE)	Cumple
Residencia de datos en la UE (Fráncfort, Alemania)	Aplicada
Certificaciones de infraestructura de AWS (ISO 27001, SOC 2, PCI DSS)	Heredadas a través de AWS
ISO 27001 (ProcessMind)	Prevista — vía de certificación seleccionada; el proceso formal aún no ha comenzado
SOC 2 Type II (ProcessMind)	Prevista — vía de certificación seleccionada; el proceso formal aún no ha comenzado
Validación automatizada de controles de infraestructura (`cdk-nag` en AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Implementada como validación de controles de ingeniería, no como certificación
Cláusulas contractuales tipo (SCC) para transferencias internacionales	Implementadas (véase DPA)
Anexo de tratamiento de datos (DPA)	Disponible públicamente

El uso de `cdk-nag` paquetes de reglas no significa que ProcessMind esté formalmente certificado o haya sido auditado de forma independiente con respecto a HIPAA, NIST o PCI DSS. Dichos paquetes de reglas se utilizan como salvaguardas de ingeniería para validar el diseño de la infraestructura y realizar un seguimiento explícito de las deficiencias.

Para preguntas relativas a la seguridad o el cumplimiento, o para solicitar documentación como informes de auditoría o cuestionarios de seguridad cumplimentados, póngase en contacto con **support@processmind.com**.