Mesures de sécurité de ProcessMind

Date d'entrée en vigueur : 14 septembre 2026

Le présent document décrit les mesures techniques et organisationnelles (« TOM ») que ProcessMind B.V. maintient afin de protéger la confidentialité, l'intégrité et la disponibilité des Customer Data. ProcessMind applique une approche de défense en profondeur, dans laquelle plusieurs couches de sécurité indépendantes protègent les Customer Data à chaque niveau — du réseau et de l'infrastructure à l'identité, l'autorisation, l'isolation des données, le chiffrement, la surveillance et le développement logiciel. Ces mesures complètent le Data Processing Addendum, la Politique de confidentialité et la Politique d'hébergement SaaS. ProcessMind examine et met à jour ces mesures au moins une fois par an.

Les Customer Data ne sont jamais vendues à des tiers, partagées avec eux ni utilisées par eux à leurs propres fins.

---

1. Sécurité de l'infrastructure

1.1 Plateforme cloud. ProcessMind est hébergé exclusivement sur Amazon Web Services (AWS) dans l'UE (Francfort, Allemagne, `eu-central-1`). AWS détient les certifications ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 et PCI DSS. Consultez AWS Compliance Programs pour obtenir la liste complète.

1.2 Architecture serverless. La logique applicative de ProcessMind s'exécute sur AWS Lambda et des services gérés par AWS. ProcessMind n'exploite pas de serveurs d'application persistants gérés par les clients, ce qui élimine une grande partie des opérations de correctifs du système d'exploitation et de durcissement des serveurs.

1.3 Limites du réseau. ProcessMind gère un AWS VPC pour les contrôles de base de données et de réseau. Aurora PostgreSQL s'exécute dans des sous-réseaux privés sans sortie vers Internet, n'est pas accessible publiquement et les journaux de flux VPC sont activés. ProcessMind ne

place pas par défaut les fonctions Lambda applicatives dans le VPC. Les fonctions Lambda accèdent à Aurora par l'intermédiaire de l'AWS RDS Data API via TLS, en utilisant l'authentification IAM et Secrets Manager.

1.4 Distribution de contenu et contrôles en périphérie. Le site web destiné aux clients, la SPA frontend et le trafic des ressources publiques sont servis par Amazon CloudFront. Toutes les distributions CloudFront imposent une politique TLS minimale de TLS 1.2 (2021). Les distributions du site web et de la SPA frontend ajoutent également des en-têtes de réponse de sécurité, notamment HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, une politique de référent et une politique d'autorisations. La distribution des ressources publiques utilise CloudFront Origin Access Control afin de maintenir le compartiment d'origine privé. Le trafic API destiné aux clients est traité séparément par Amazon API Gateway : le trafic de requêtes/réponses HTTPS est servi par une HTTP API sur un sous-domaine API dédié, et les connexions client en temps réel sont servies par une API WebSocket API Gateway distincte sur un sous-domaine WebSocket dédié.

1.5 Séparation des environnements. Les environnements de production et de développement utilisent des comptes AWS distincts, des bases de données distinctes et des piles d'infrastructure distinctes. Les identifiants des développeurs ne donnent pas accès aux Customer Data de production.

---

2. Chiffrement des données

2.1 Chiffrement en transit. Toutes les données transmises entre les clients et les services ProcessMind sont chiffrées au moyen de TLS 1.2 ou d'une version ultérieure. Les points de terminaison destinés aux clients sont exposés via HTTPS. Les compartiments S3, les rubriques SNS et les files SQS créés directement par ProcessMind imposent un accès SSL uniquement. L'accès aux bases de données par l'intermédiaire de la RDS Data API et les autres appels aux services AWS utilisent HTTPS/TLS.

2.2 Chiffrement au repos. Aurora PostgreSQL est chiffré au repos au moyen de clés AWS KMS gérées par le client, avec rotation automatique des clés. Les compartiments S3 de données clients et d'exploitation créés directement par ProcessMind, notamment les compartiments de téléversements, de ressources et de journaux d'accès, utilisent des clés KMS gérées par le client. Les groupes de journaux CloudWatch, les rubriques SNS et les files SQS créés directement par ProcessMind utilisent également des clés KMS gérées par le client. Les compartiments d'origine du site web et du frontend gérés par SST utilisent le chiffrement côté serveur S3 géré par AWS (SSE-S3 / AES-256), plutôt que des clés KMS gérées par le client.

2.3 Gestion des clés et des secrets. Les clés de chiffrement des bases de données sont gérées de manière centralisée par AWS KMS et l'accès aux clés est régi par des politiques IAM suivant les principes du moindre privilège. Les identifiants des bases de données sont stockés dans AWS Secrets Manager. Le secret principal Aurora et le secret de l'utilisateur applicatif restreint sont automatiquement renouvelés tous les trente (30) jours. Les clés et secrets de production ne sont jamais stockés dans le code source ; les identifiants réservés au développement sont isolés de la production. Certaines ressources auxiliaires gérées par AWS/CDK/SST continuent d'utiliser le chiffrement géré par AWS lorsque le service ou le framework n'expose pas de configuration de clé gérée par le client.

---

3. Isolation et localisation des données

3.1 Isolation des tenants. Chaque tenant client reçoit une instance de base de données dédiée et isolée. Les Customer Data ne sont jamais mélangées avec celles d'autres clients au niveau de la base de données. Les métadonnées partagées (par exemple, les enregistrements de compte, la facturation et les associations utilisateur-tenant) sont stockées dans une base de données multi-tenant distincte, avec des contrôles d'accès stricts. Les tables partagées limitées au tenant et à l'organisation sont en outre protégées par des politiques de sécurité au niveau des lignes (RLS) de

PostgreSQL, appliquées au moyen d'un contexte de base de données limité à la requête.

3.2 Localisation des données. Toutes les Customer Data, notamment les bases de données, les fichiers téléversés, les sauvegardes et les résultats de requêtes, sont stockées exclusivement dans l'UE (Francfort, Allemagne). Lorsqu'un sous-traitant ultérieur situé en dehors de l'EEE est engagé pour une activité de traitement spécifique (par exemple, le traitement de modèles d'IA ou le traitement des paiements), le transfert est couvert par un mécanisme de transfert approprié tel que décrit dans le Data Processing Addendum, et le sous-traitant ultérieur ainsi que son lieu de traitement sont indiqués dans la Liste des sous-traitants ultérieurs.

3.3 Conservation et suppression des données. Les délais de conservation et de suppression sont définis à la section 6 du Data Processing Addendum. Les clients peuvent supprimer leurs données à tout moment par l'intermédiaire de l'application ou en contactant ProcessMind. Les copies de sauvegarde sont supprimées à l'expiration des périodes de conservation des sauvegardes applicables (section 7.1).

---

4. Gestion des identités et des accès

4.1 Authentification. ProcessMind prend en charge le Single Sign-On (SSO) via Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC et LinkedIn OAuth 2.0/OIDC. ProcessMind agit en tant que partie de confiance et ne stocke pas les mots de passe des utilisateurs. L'authentification multifacteur est imposée par le fournisseur d'identité — par exemple, lorsqu'une organisation connecte Microsoft Entra ID (Azure AD), les propres politiques d'authentification multifacteur et d'accès de cette organisation s'appliquent.

4.2 Gestion des sessions. Les sessions de navigateur utilisent des JSON Web Tokens (JWT) signés, transmis au moyen de cookies sécurisés HttpOnly comportant les attributs SameSite et Secure. Les signatures des jetons sont validées lors de chaque requête authentifiée.

4.3 Modèle d'autorisation. ProcessMind ne dépend pas des authorizers natifs d'API Gateway pour ses API applicatives principales. L'autorisation est appliquée dans des wrappers partagés de gestionnaires Lambda qui valident l'état de la session et le périmètre du tenant avant l'exécution de la logique métier. Les routes publiques sont explicitement autorisées pour les flux non authentifiés, les webhooks, l'ingestion d'événements et le pré-vol CORS. Les points de terminaison d'API externes utilisent des gestionnaires d'authentification dédiés. L'accès aux Customer Data est limité au contexte du tenant ou de l'organisation authentifié.

4.4 Moindre privilège. Les systèmes internes suivent le principe du moindre privilège. Les rôles IAM sont limités aux ressources minimales nécessaires lorsque le framework permet une limitation précise. Certains rôles générés par SST/CDK utilisent des politiques gérées ou intégrées plus larges pour les liaisons et l'exécution ; ces cas sont examinés, limités aux ressources lorsque cela est possible et suivis comme exceptions explicites.

4.5 Contrôles d'accès des employés. L'accès des employés aux systèmes internes est géré par Active Directory avec SSO et MFA obligatoire. Le contrôle d'accès fondé sur les rôles (RBAC) garantit que l'accès aux Customer Data est limité au personnel autorisé selon le principe du besoin d'en connaître. Les droits d'accès sont examinés périodiquement.

---

5. Journalisation, surveillance et audit

5.1 Journalisation centralisée. La journalisation des accès à l'HTTP API et celle des accès WebSocket sont activées avec des champs JSON structurés et écrites dans Amazon CloudWatch Logs, avec une conservation d'une (1) semaine. Ces groupes de journaux d'accès sont chiffrés au moyen d'une clé AWS KMS gérée par le client. Les journaux applicatifs sont centralisés dans des groupes de journaux Amazon CloudWatch chiffrés au moyen d'une clé AWS KMS gérée par le client et conservés pendant dix (10) ans. Des groupes de journaux distincts pour l'audit et la télémétrie sont également chiffrés au moyen d'une clé AWS

KMS gérée par le client et conservés pendant dix (10) ans. Le groupe d'exportation des journaux du moteur Aurora PostgreSQL est conservé pendant une (1) semaine.

5.2 Ce qui est journalisé et ce qui ne l'est pas. ProcessMind journalise les événements d'accès à l'HTTP API et à WebSocket, notamment l'heure de la requête, les identifiants de requête, la route ou le chemin, le statut de réponse, la latence, l'adresse IP source et l'agent utilisateur. ProcessMind journalise également les événements d'authentification, les chemins d'échec asynchrones et l'activité applicative Lambda auxiliaire dans des groupes de journaux CloudWatch centralisés. Les journaux de flux VPC sont activés. ProcessMind n'active actuellement pas la journalisation standard des accès CloudFront sur les distributions du site web, de la SPA frontend ou des ressources publiques.

5.3 Surveillance et alertes. Les alarmes et tableaux de bord CloudWatch surveillent l'état du système, les files d'attente de lettres mortes et les défaillances pertinentes pour la sécurité. Les échecs de traitement asynchrone sont acheminés vers des files d'attente de lettres mortes chiffrées (conservation de quatorze (14) jours ; deux (2) jours pour les files d'attente de miniatures et d'index de recherche), et les alarmes DLQ déclenchent des notifications SNS aux fins d'examen. En outre, ProcessMind utilise Sentry pour le suivi des erreurs frontend en temps réel, la surveillance des performances et la relecture des sessions. Les relectures de sessions ne sont enregistrées que pour les sessions au cours desquelles une erreur se produit, et le texte, les saisies de formulaires et les médias sont masqués ou bloqués dans les relectures. Les données Sentry sont ingérées dans l'UE (Francfort) et se limitent aux ProcessMind Usage Data (erreurs de navigateur, traces de performance, métadonnées de l'appareil et enregistrements de relecture masqués). Sentry figure dans la liste des sous-traitants ultérieurs.

5.4 Protection des journaux. Les journaux sont stockés dans des groupes de journaux CloudWatch dédiés et soumis à des contrôles d'accès, et sont

chiffrés au repos. Les journaux de production et de développement sont séparés par les limites des environnements et des comptes.

---

6. Validation automatisée des contrôles et gestion des vulnérabilités

6.1 Ce que fait ProcessMind. ProcessMind exécute `cdk-nag` dans le cadre de son flux de synthèse et de déploiement de l'infrastructure, en utilisant plusieurs ensembles de règles du secteur (notamment AWS Solutions, NIST 800-53 et PCI DSS). Des rapports par pile sont générés et examinés dans le cadre de la gestion des modifications de l'infrastructure. Les constatations sont classées comme corrigées, risque accepté ou amélioration planifiée.

6.2 Gestion des exceptions. Les suppressions sont consignées dans un registre central lorsque le framework le permet, limitées aux piles concernées et soumises à une justification écrite ; lorsqu'une pile contient une suppression intégrée, celle-ci est documentée avec cette pile. Lorsqu'une constatation est corrigée, la suppression correspondante est mise à jour ou supprimée. ProcessMind ne considère pas une suppression comme une dispense générale d'examen.

6.3 Ce que ProcessMind ne fait pas actuellement. ProcessMind suit et examine les exceptions importantes aux contrôles de l'infrastructure. Les principales sont les suivantes :

- Les fonctions Lambda ne sont pas placées dans le VPC par défaut ; elles accèdent à Aurora via l'API RDS Data sur TLS avec une authentification IAM et Secrets Manager
- l'API WebSocket et les distributions statiques ne sont pas protégées par AWS WAF (les connexions WebSocket utilisent des jetons HMAC à courte durée de validité ; les restrictions géographiques liées aux paiements sont appliquées dans le système de paiement), et les distributions statiques n'activent pas la journalisation standard des accès CloudFront
- la récupération de la base de données repose sur les sauvegardes automatisées Aurora et la récupération à un instant donné, plutôt

que sur un plan AWS Backup distinct ou sur Aurora Enhanced Monitoring
- il n'existe pas de réplication S3 interrégionale ni de verrouillage d'objet S3 pour les compartiments modifiables
- certaines ressources auxiliaires gérées par AWS/CDK/SST utilisent le chiffrement géré par AWS ou des politiques IAM générées plus larges lorsque le service n'expose pas d'alternative contrôlable par le client

Le registre complet des suppressions est tenu parallèlement au code d'infrastructure et est disponible sur demande. L'utilisation des `cdk-nag` packs de règles constitue une validation des contrôles d'ingénierie, et non une certification externe, une opinion d'audit ou une attestation juridique de conformité à HIPAA, NIST ou PCI DSS.

6.4 Gestion des dépendances. Les dépendances logicielles font l'objet d'une surveillance continue visant à détecter les vulnérabilités connues. Les vulnérabilités critiques et de gravité élevée sont corrigées avec un objectif de sept (7) jours. Les dépendances sont mises à jour selon un cycle régulier.

6.5 Cycle de développement logiciel sécurisé (SDLC). ProcessMind applique une approche de défense en profondeur au développement logiciel. Toute modification apportée à la production doit passer par plusieurs couches indépendantes de validation automatisée avant son déploiement :

- **Analyse statique et sûreté des types :** le mode strict de TypeScript et ESLint imposent la correction des types, la sécurité vis-à-vis des valeurs nulles et des modèles de codage pertinents pour la sécurité au moment de la compilation.
- **Revue de code assistée par l'IA :** l'analyse assistée par l'IA fournit un point de vue supplémentaire lors de la revue des pull requests afin d'identifier les risques de sécurité, les erreurs logiques et les écarts par rapport aux conventions, en complément des tests automatisés.

- **Tests unitaires et d'intégration :** une suite complète de tests Vitest valide la logique métier, les modèles d'accès aux données, le comportement de l'API et la gestion des erreurs par rapport aux ressources AWS réelles dans l'environnement de développement.
- **Tests de bout en bout :** les tests de navigateur fondés sur Playwright vérifient les flux de travail utilisateur critiques, notamment l'authentification, le téléversement de données, la modélisation des processus, la simulation et l'isolation entre locataires.
- **Analyse de conformité de l'infrastructure :** `cdk-nag` valide l'infrastructure-as-code au regard de plusieurs référentiels de conformité à chaque modification.
- **Analyse des vulnérabilités des dépendances :** les audits automatisés des dépendances empêchent les vulnérabilités critiques et de gravité élevée connues d'atteindre la production.

La revue humaine porte principalement sur l'architecture, les limites de sécurité et les décisions de conception, plutôt que sur l'inspection du code ligne par ligne. Lorsque des modifications structurelles, sensibles du point de vue de la sécurité ou liées à l'infrastructure sont concernées, une validation humaine explicite est requise en plus de la validation automatisée.

Toutes les couches de validation sont imposées par l'intermédiaire de l'intégration continue en tant que contrôles de fusion obligatoires pour les modifications de la branche principale. Les correctifs urgents en production peuvent contourner le contrôle d'intégration continue, mais doivent être suivis de l'exécution complète du pipeline et d'une revue post-incident dans les vingt-quatre (24) heures.

---

7. Sauvegarde et reprise après sinistre

7.1 Sauvegardes automatisées. Amazon Aurora effectue des sauvegardes continues et automatisées avec une période de conservation de sept (7)

jours. Les sauvegardes sont chiffrées à l'aide des mêmes clés KMS gérées par le client que les bases de données sources.

7.2 Récupération à un instant donné. Aurora prend en charge la récupération à un instant donné, à n'importe quelle seconde comprise dans la période de conservation des sauvegardes, permettant une restauration rapide en cas de corruption des données ou de suppression accidentelle.

7.3 Durabilité et gestion des versions S3. Les téléversements de fichiers et les artefacts opérationnels sont stockés dans Amazon S3, qui fournit une durabilité de 99,999999999 % (11 neuf). La gestion des versions est activée sur le compartiment des téléversements et les compartiments de ressources afin de permettre la récupération et les restaurations à une version antérieure. Les compartiments de déploiement du site web et du frontend contiennent des artefacts de compilation reproductibles et ne sont pas considérés comme un système de sauvegarde. ProcessMind n'active actuellement pas la réplication S3 interrégionale.

7.4 Continuité des activités. Les procédures de reprise après sinistre sont documentées et testées périodiquement. Un résumé est disponible dans le document Disaster Recovery, Business Continuity & Incident Response. L'architecture repose sur des services gérés AWS au sein de la `eu-central-1` région, qu'AWS exploite sur plusieurs zones de disponibilité ; le cluster Aurora exécute actuellement une seule instance d'écriture, de sorte que la récupération de la base de données repose sur les sauvegardes automatisées et la récupération à un instant donné, plutôt que sur une instance de secours dans la région. Les sauvegardes Aurora, la durabilité S3, les files d'attente de lettres mortes et les ressources statiques reconstruites à partir de la source font partie de la stratégie de récupération.

---

8. Réponse aux incidents

8.1 Notification des incidents. En cas d'Incident de sécurité (tel que défini dans le DPA), ProcessMind notifiera les clients concernés sans retard indu et, lorsque cela est possible, dans les soixante-douze (72) heures suivant la prise de connaissance de l'incident.

8.2 Gestion des incidents. ProcessMind tient à jour des procédures documentées de réponse aux incidents couvrant l'identification, le confinement, l'éradication, la récupération et la revue post-incident. Un résumé est disponible dans le document Disaster Recovery, Business Continuity & Incident Response. Les enseignements tirés des incidents sont intégrés aux contrôles et processus de sécurité.

8.3 Communication. Les notifications d'incident indiquent la nature et la portée de l'incident, les catégories de données concernées, les mesures prises pour contenir l'incident et les actions recommandées au client.

---

9. Mesures organisationnelles

9.1 Gestion de la sécurité de l'information. ProcessMind maintient un système de gestion de la sécurité de l'information aligné sur les principes de la norme ISO 27001. ProcessMind a choisi sa voie de certification pour la certification ISO 27001 et l'attestation SOC 2 Type II ; le processus formel de certification n'a pas encore commencé.

9.2 Sensibilisation à la sécurité. Tout le personnel ayant accès aux Données client reçoit une formation de sensibilisation à la sécurité. Les bonnes pratiques de sécurité sont intégrées à l'intégration des nouveaux collaborateurs, aux flux de développement et aux procédures opérationnelles.

9.3 Gestion des fournisseurs et des sous-traitants ultérieurs. Les sous-traitants ultérieurs sont contractuellement tenus de respecter des normes de protection des données équivalentes à celles décrites dans le présent document. ProcessMind tient à jour une liste publique des sous-traitants

ultérieurs et fournit un préavis d'au moins trente (30) jours avant de faire appel à un nouveau sous-traitant ultérieur. La conformité des sous-traitants ultérieurs fait l'objet d'un examen annuel.

9.4 Confidentialité. Tout le personnel autorisé à traiter les Données client est tenu par des obligations écrites de confidentialité.

---

10. Conformité et certifications

Référentiel / Norme	Statut
RGPD (Règlement général sur la protection des données de l'UE)	Conforme
Résidence des données dans l'UE (Francfort, Allemagne)	Appliquée
Certifications de l'infrastructure AWS (ISO 27001, SOC 2, PCI DSS)	Héritées via AWS
ISO 27001 (ProcessMind)	Prévue — voie de certification choisie ; processus formel pas encore commencé
SOC 2 Type II (ProcessMind)	Prévue — voie de certification choisie ; processus formel pas encore commencé
Validation automatisée des contrôles de l'infrastructure (`cdk-nag` dans AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Mise en œuvre en tant que validation des contrôles d'ingénierie, et non en tant que certification
Clauses contractuelles types (CCT) pour les transferts internationaux	Mises en œuvre (voir DPA)

Référentiel / Norme	Statut
Avenant relatif au traitement des données (DPA)	Accessible au public

L'utilisation des `cdk-nag` packs de règles ne signifie pas que ProcessMind est formellement certifié ou fait l'objet d'un audit indépendant au regard de HIPAA, NIST ou PCI DSS. Ces packs de règles sont utilisés comme garde-fous d'ingénierie afin de valider la conception de l'infrastructure et de suivre explicitement les écarts.

Pour toute question concernant la sécurité ou la conformité, ou pour demander des documents tels que des rapports d'audit ou des questionnaires de sécurité remplis, contactez **support@processmind.com**.