Déclaration de ProcessMind relative au journal d'audit et au SIEM

Date d'entrée en vigueur : 12 novembre 2026

La présente déclaration décrit la manière dont ProcessMind B.V. consigne les actions administratives et pertinentes pour la sécurité effectuées sur les Données client (le « journal d'audit »). Elle complète les Mesures de sécurité, l'Addendum relatif au traitement des données, le Contrat client et la Liste des sous-traitants.

---

1. Champ d'application

1.1 Un seul journal d'audit. ProcessMind tient un journal d'audit unique pour les actions administratives et pertinentes pour la sécurité effectuées sur les Données client et le Service ProcessMind. Le journal d'audit est distinct de la journalisation opérationnelle (de l'application), de la journalisation des accès HTTP et du fil d'activité du produit ; ces flux répondent à des finalités différentes et ne sont pas présentés comme une piste d'audit.

1.2 Ce qu'il n'est pas. Le journal d'audit ne consigne pas chaque consultation des Données client et ne constitue pas l'historique des modifications du produit concernant les modèles de processus, les diagrammes, la documentation ou les simulations. Ces éléments sont consignés dans l'historique des modifications des processus disponible dans le produit.

---

2. Contenu de chaque enregistrement d'audit

2.1 Champs. Chaque enregistrement comporte les champs ci-dessous. L'ensemble est fixé par le schéma d'enregistrement : un enregistrement ne peut pas comporter un champ qui ne figure pas dans cette liste, et une action ne peut pas en ajouter un qu'elle n'a pas déclaré dans le registre.

- *schemaVersion* (nombre) : version du schéma d'enregistrement, actuellement 1.
- *eventId* (chaîne) : identifiant unique de l'enregistrement. Les nouveaux enregistrements utilisent un ULID ; les lignes migrées depuis l'ancien stockage conservent leur UUID.
- *occurredAt*, *ingestedAt* (horodatages) : date et heure auxquelles l'action a eu lieu et auxquelles le rédacteur du journal d'audit a stocké l'enregistrement. Les deux sont en UTC.
- *eventClass* (énumération) : security, auth, admin, data, api, ai ou platform.
- *action* (énumération) : un code issu du registre d'actions fermé et soumis à examen, par exemple auth.login.blocked ou api.key.revoked.
- *outcome* (énumération) : success, failure, denied ou error.
- *severity* (énumération) : info, notice, warning ou critical, déterminé à partir du résultat. Une action réussie utilise la valeur par défaut du registre (info, sauf indication contraire pour l'action), un échec est consigné comme notice, et un refus ou une erreur comme warning.
- *actor* (objet) : auteur de l'action. type (user, apiKey, service, system ou anonymous), id, email, displayName, ainsi que onBehalfOf et onBehalfOfEmail lorsque l'action a été effectuée pour un autre compte.
- *actorContext* (objet) : session de l'auteur de l'action. sessionId, authMethod (oidc, password, loginToken, apiKey ou none) et indicateur de session d'assistance.
- *organizationId*, *tenantId* (identifiants, pouvant être nuls) : l'organisation et l'environnement auxquels l'action se rapporte. Valeur nulle pour les enregistrements qui ne concernent aucun client ou qui se situent au-dessus de l'environnement.
- *resource* (objet, pouvant être nul) : objet concerné. type, id et name, où type est l'un des suivants : apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant ou user.

- *source* (objet) : origine de l'enregistrement. service (api, externalApi, superadminApi, worker, cron ou webSocket), function et version.
- *stage*, *region* (chaînes) : étape de déploiement à l'origine de l'enregistrement (par exemple prod) et région AWS (eu-central-1 pour les enregistrements client).
- *correlation* (objet) : requestId, traceId et parentEventId, qui relient l'enregistrement à la requête qui l'a provoqué et aux enregistrements qui le précèdent dans le même flux.
- *network* (objet, pouvant être nul) : sourceIp et userAgent. Collectés uniquement pour les actions dont l'entrée du registre le prévoit : connexion, décisions d'accès, modifications administratives et de paramètres, téléversements, téléchargements et exportations de données, modifications de clés API et modifications des politiques d'IA.
- *detail* (objet) : charge utile propre à l'action, validée par rapport au schéma de cette action. Les valeurs sont uniquement des primitives (chaîne, nombre, booléen, null), afin que l'enregistrement reste interrogeable et puisse faire l'objet d'une occultation.

2.2 Vocabulaire fermé. Les actions sont tirées d'une liste fixe de codes d'action soumis à examen ; un enregistrement d'audit ne contient aucun message en texte libre. Chaque action déclare également les champs supplémentaires qu'elle peut comporter, de sorte qu'un enregistrement ne puisse pas intégrer silencieusement un nouveau type de contenu.

---

3. Actions consignées

3.1 Actions actuellement consignées. ProcessMind consigne notamment :

- **Authentification :** réussite et échec de connexion, connexion bloquée (compte verrouillé, domaine non autorisé, adresse électronique du fournisseur non vérifiée), déconnexion, émission et transfert de jetons de connexion.

- **Autorisation :** refus d'accès, y compris chaque identifiant d'accès à l'API externe rejeté, chaque refus lié à la portée ou à l'état du tenant, ainsi que les refus liés à l'origine (CORS).
- **Accès d'assistance :** début d'une session d'assistance ProcessMind sur un compte client, avec indication de l'opérateur et du compte concerné.
- **Identifiants API :** création, modification de portée et révocation de clés API, y compris les portées accordées.
- **Administration des comptes et des rôles :** création d'utilisateurs, invitations, modifications des profils d'administrateur, suppressions, attributions et révocations de rôles, et modifications de l'appartenance à un tenant ou à une organisation.
- **Cycle de vie de l'organisation :** création, suppression, restauration, planification et annulation de suppression, et effacement effectué.
- **Téléversement, téléchargement et exportation de données :** téléversement, téléchargement et suppression d'artefacts, téléversement et mise à jour de données tabulaires, téléchargements d'exportations, suppression de tables de données, et création, modification et suppression de webhooks (connexions).
- **État de facturation :** modifications de forfait, suspension et rétablissement liés aux paiements, et résiliation d'abonnement.
- **Console fournisseur de ProcessMind :** exécution de requêtes privilégiées, administration des utilisateurs et des organisations, modifications des paramètres et des fonctionnalités, demandes de synchronisation de facturation et migrations.
- **Actions administratives et destructrices effectuées par les tâches planifiées de ProcessMind :** suppressions de tenants, d'organisations, d'utilisateurs et de prospects, opérations de purge liées à la conservation et échecs de pipeline.
- **Intégrité du journal d'audit :** échecs du processus d'écriture du journal d'audit lui-même.

3.2 Modifications de l'espace de travail. Les modifications effectuées dans un espace de travail (modèles de processus, documentation, simulations,

tableaux de bord, commentaires et favoris) sont consignées dans l'historique des modifications des processus propre au produit, et non dans le journal d'audit. Le journal d'audit indique qui a téléversé, téléchargé, exporté ou supprimé des données ; l'historique des modifications indique ce qui a changé dans un modèle. La liste actuelle des codes d'action consignés peut être obtenue auprès de ProcessMind sur demande.

---

4. Éléments qui ne sont jamais consignés

Les mots de passe, jetons d'authentification, valeurs de clés API, cookies, en-têtes d'autorisation, corps de requêtes ou de réponses, contenus de fichiers, URL présignées et invites ou réponses de l'IA ne sont jamais écrits dans le journal d'audit. Les enregistrements d'audit peuvent contenir des données à caractère personnel nécessaires à l'attribution : l'adresse électronique de l'auteur de l'action, ainsi que l'adresse IP source et l'agent utilisateur pour les actions dont l'entrée du registre le prévoit (connexion, décisions d'accès, modifications administratives et de paramètres, mouvements de données, modifications de clés API et de politiques d'IA). Les champs autorisés sont définis pour chaque action et examinés lors de l'ajout d'une action.

---

5. Intégrité

5.1 Ajout uniquement. Le journal d'audit est en ajout uniquement. Aucun rôle applicatif ne dispose d'un privilège de mise à jour ou de suppression sur celui-ci, et une contrainte de base de données rejette ces deux opérations.

5.2 Un seul rédacteur. Les enregistrements sont écrits par un composant unique qui valide le code d'action et sa charge utile avant l'écriture. Tout enregistrement qui n'est pas valide est rejeté et signalé, plutôt que partiellement écrit.

5.3 Gestion des échecs. L'échec d'une écriture dans le journal d'audit n'entraîne jamais l'échec de l'action métier qu'elle décrit. Il est consigné par un processus opérationnel assorti d'une alarme, et l'enregistrement lui-même est conservé dans une copie secondaire afin de pouvoir être récupéré.

---

6. Conservation et emplacement

6.1 Conservation. Les enregistrements d'audit sont conservés pendant au moins dix (10) ans à compter de la date de l'événement.

6.2 Emplacement et chiffrement. Les enregistrements d'audit sont stockés dans l'Union européenne (Francfort, Allemagne, `eu-central-1`) et sont chiffrés au repos au moyen d'une clé AWS KMS gérée par le client. Une copie en temps réel est également écrite dans un groupe de journaux Amazon CloudWatch à accès contrôlé afin qu'un incident puisse faire l'objet d'une enquête pendant qu'il se produit.

6.3 Aucune réplication interrégionale. Les enregistrements d'audit ne sont pas répliqués en dehors de l'Union européenne.

---

7. Accès aux enregistrements d'audit

7.1 Droit d'accès. Le journal d'audit intégré à l'application est inclus dans le forfait Process Architecture et les forfaits supérieurs. Un administrateur d'organisation peut consulter l'ensemble de l'organisation ; un administrateur dont les droits sont limités à un tenant peut consulter son propre tenant. Le périmètre est déterminé à partir de la session authentifiée et vérifié avant la requête, de sorte qu'une requête ne puisse pas l'étendre à un autre tenant ou à une autre organisation.

7.2 Personnel de ProcessMind. Le personnel de ProcessMind n'accède aux enregistrements d'audit qu'à des fins d'assistance, de réponse aux incidents ou pour satisfaire à une obligation légale, selon le principe du

besoin d'en connaître. L'accès entre clients est limité à un rôle d'assistance dédié, et cet accès constitue lui-même une action administrative.

7.3 Obtention des enregistrements. Les administrateurs d'organisation et de tenant peuvent consulter leurs enregistrements d'audit dans le journal d'audit intégré à l'application et les récupérer ou les exporter au moyen de l'API externe. Pour une demande plus importante ou nécessitant une assistance, le service d'assistance de ProcessMind fournit les enregistrements au format CSV ou JSON pour une organisation, un tenant et une période déterminés, avec un délai cible de cinq (5) jours ouvrables pour une demande standard.

---

8. Suppression des enregistrements d'audit

8.1 Sur demande. Sur réception d'une demande écrite vérifiée, ProcessMind efface du stockage d'audit les enregistrements d'audit appartenant à une organisation cliente et confirme cet effacement par écrit. La copie opérationnelle dans CloudWatch ne peut pas être modifiée enregistrement par enregistrement ; elle expire conformément à sa propre période de conservation.

8.2 Éléments conservés. L'enregistrement de l'effacement (identifiant de l'organisation, date, demandeur, motif et nombre d'enregistrements supprimés) est conservé en tant qu'enregistrement d'audit au niveau de la plateforme et ne contient aucune Donnée client. Les enregistrements qui n'appartiennent à aucun client (événements de la plateforme ProcessMind) ne sont pas concernés par une demande d'effacement d'un client.

8.3 Demandes d'effacement individuelles. Lorsqu'une demande concerne une personne au sein d'un client qui demeure actif, l'enregistrement de sécurité est conservé aux fins de la constatation, de l'exercice ou de la défense de droits en justice, dans la mesure autorisée par l'article 17, paragraphe 3, points b) et e), du RGPD ; ce fondement est consigné dans le registre des activités de traitement et dans la Politique de confidentialité.

9. Intégration et exportation SIEM

9.1 Disponibilité. L'archive d'audit immuable est une option Enterprise, activée pour une organisation cliente sur demande. Elle écrit quotidiennement des objets NDJSON compressés sous un préfixe propre à chaque organisation dans un compartiment S3 verrouillé (WORM), avec un manifeste et un rapprochement nocturne.

9.2 Mode de livraison actuel. ProcessMind ne propose actuellement ni connecteur SIEM natif ni flux poussé. La récupération s'effectue à partir de trois interfaces : l'API de lecture (`GET /v1/tenant/{tenantId}/audit`), la tâche d'exportation limitée (à créer avec `POST /v1/tenant/{tenantId}/audit/exports`, puis récupérer le résultat au moyen de son appel d'état, qui renvoie une URL de téléchargement à durée de validité limitée) et, avec l'archive Enterprise, les objets quotidiens sous le préfixe propre à l'organisation dans le compartiment verrouillé, que le SIEM du client lit au moyen d'un dispositif d'accès. ProcessMind ne livre pas les enregistrements à un emplacement choisi par le client selon son propre calendrier.

9.3 Surveillance propre à ProcessMind. La surveillance de sécurité de ProcessMind utilise les mêmes enregistrements : les échecs d'écriture dans le journal d'audit, les pics d'échecs d'authentification, les modifications de privilèges et les actions administratives destructrices déclenchent des alertes internes.

---

10. Éléments de preuve mis à la disposition des clients

Sur demande et, le cas échéant, sous réserve de confidentialité, ProcessMind fournit la présente déclaration, les Mesures de sécurité, l'Addendum relatif au traitement des données, la Liste des sous-traitants, un échantillon expurgé d'enregistrements d'audit et la procédure utilisée pour les demandes d'accès et d'effacement.

---

11. Limitations

Afin d'éviter toute ambiguïté, ProcessMind affirme utiliser un stockage d'audit en ajout uniquement pour chaque organisation et, lorsque le droit à l'archive d'audit est activé, une copie dans un compartiment verrouillé (WORM) avec rapprochement nocturne du manifeste. ProcessMind n'affirme actuellement pas utiliser une chaîne de hachage, un connecteur SIEM natif avec transmission en temps réel, l'occultation des enregistrements d'audit par utilisateur, une attestation ISO 27001 ou SOC 2 couvrant ce contrôle, ni couvrir chaque consultation des Données client. Les clients peuvent consulter et exporter eux-mêmes les enregistrements au moyen du journal d'audit intégré à l'application et de l'API externe.