Reprise après sinistre, continuité d'activité et réponse aux incidents de ProcessMind

Date d'entrée en vigueur : 14 septembre 2026

Le présent document fournit une synthèse générale des procédures de ProcessMind B.V. en matière de reprise après sinistre (« DR »), de continuité d'activité (« BCP ») et de réponse aux incidents de sécurité pour son service cloud. Il complète les Mesures de sécurité, la Politique d'hébergement SaaS, l'Accord de niveau de service et l'Avenant relatif au traitement des données.

Il explique notre approche actuelle et ne crée pas d'objectifs contractuels distincts en matière de délai de reprise, de point de reprise, de garanties de durabilité des données, de délais de notification, de niveaux de service ou de normes de responsabilité au-delà de ce qui est expressément prévu dans l'accord applicable, le DPA ou le SLA.

---

1. Objectifs et champ d'application

ProcessMind maintient ces procédures afin de :

- protéger la confidentialité, l'intégrité et la disponibilité des Données client pendant un événement perturbateur
- rétablir les composants critiques du service de production après des défaillances dans les systèmes contrôlés par ProcessMind
- assurer la continuité de la gestion des incidents, des communications avec les clients et de la prise de décisions opérationnelles pendant les interruptions de service
- récupérer les défaillances de l'infrastructure, du déploiement, de l'application ou de la couche de données au moyen de procédures documentées et de définitions d'infrastructure contrôlées par le code source
- identifier et évaluer les Incidents de sécurité, contenir les menaces, éliminer les causes profondes, récupérer les systèmes affectés,

communiquer lorsque cela est requis et consigner les enseignements tirés

Ces procédures s'appliquent au service cloud de production de ProcessMind et aux événements de sécurité impliquant des sous-traitants ultérieurs ou des services cloud dans la mesure où ils affectent le Service et relèvent de la capacité raisonnable de ProcessMind à les examiner et à les gérer. Les environnements de développement et de test sont séparés et ne sont pas considérés comme des cibles de reprise pour les engagements de production destinés aux clients.

---

2. Stratégie de résilience

2.1 Conception régionale. Les services de production sont hébergés dans AWS EU (Francfort, Allemagne, `eu-central-1`). L'architecture repose sur des services gérés AWS au sein de cette région, qu'AWS exploite dans plusieurs zones de disponibilité. Le cluster Aurora exécute actuellement une seule instance d'écriture ; la reprise de la base de données repose donc sur des sauvegardes automatisées et une récupération à un instant donné, plutôt que sur une instance de secours dans la région. ProcessMind n'exploite actuellement aucune seconde région active pour les données clients.

2.2 Services gérés et sans serveur. ProcessMind s'appuie sur AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS et Amazon CloudWatch. Cela réduit la dépendance à l'égard de serveurs persistants gérés par les clients et permet une reprise par reconstruction à partir du code source pour les composants applicatifs et statiques.

2.3 Séparation des environnements. Les environnements de production et de développement fonctionnent dans des comptes AWS distincts, avec des bases de données et des piles d'infrastructure distinctes. Cela réduit le risque que les activités de développement affectent les opérations de reprise de la production.

2.4 Surveillance et détection. Les alarmes CloudWatch, les tableaux de bord, les alertes des files d'attente de lettres mortes, la journalisation centralisée et la surveillance synthétique des services contribuent à la détection, au triage et à l'escalade des incidents. Les incidents potentiels peuvent également être identifiés par l'intermédiaire des demandes d'assistance, de signalements d'employés, de notifications de fournisseurs ou d'autres déclencheurs d'enquête.

---

3. Priorités de reprise

Lors d'un incident majeur, les priorités de reprise de ProcessMind sont généralement les suivantes :

1. Protéger l'intégrité des données clients et empêcher tout dommage supplémentaire.
2. Contenir l'incident et stabiliser les systèmes affectés.
3. Rétablir les voies d'accès essentielles à la production et les flux de travail critiques.
4. Valider le comportement du service, l'intégrité des données et la surveillance avant de déclarer la reprise achevée.
5. Communiquer les mises à jour de statut, l'impact sur les clients et les mesures de suivi.

La séquence exacte peut varier selon la nature de l'incident, notamment selon qu'il affecte l'intégrité des données, l'accès des clients, le traitement asynchrone ou l'infrastructure de soutien.

---

4. Procédures de reprise après sinistre

4.1 Déclaration et coordination de l'incident. Les interruptions importantes de service et les incidents de sécurité font l'objet d'un triage au moyen des procédures de réponse aux incidents. ProcessMind désigne un responsable de l'incident, limite la participation à la réponse au personnel autorisé, évalue la gravité et la portée, coordonne les intervenants techniques et suit

les mesures de reprise jusqu'à la résolution ou la rétrogradation de l'incident.

4.2 Confinement. ProcessMind déploie des efforts commercialement raisonnables pour arrêter ou réduire l'impact en cours avant d'entreprendre une restauration plus large. Selon le mode de défaillance, les mesures de confinement peuvent inclure l'annulation de modifications récentes, la désactivation des voies affectées, l'isolement des composants défaillants, la suspension du traitement en arrière-plan pendant l'exécution de contrôles d'intégrité, la révocation ou la rotation des identifiants, ou le blocage des activités abusives.

4.3 Éradication. Une fois l'impact immédiat stabilisé, ProcessMind s'efforce d'éliminer la cause profonde ou la condition contributive. Cela peut inclure l'application de correctifs de code ou de configuration, la suppression d'artefacts malveillants, la rotation des secrets, la restauration d'une configuration fiable ou la fermeture des voies d'accès exposées.

4.4 Reprise de la base de données. Aurora PostgreSQL effectue des sauvegardes automatisées continues avec une durée de conservation de sept (7) jours et prend en charge la récupération à un instant donné. Si une défaillance au niveau de la base de données, un événement de corruption ou une modification destructive accidentelle nécessite une restauration, ProcessMind peut restaurer la sauvegarde appropriée la plus récente ou effectuer une restauration à un instant donné sélectionné, valider l'environnement restauré et rediriger le trafic applicatif vers la base de données récupérée.

4.5 Reprise des objets et artefacts. Les téléversements de fichiers des clients et les artefacts opérationnels sont stockés dans Amazon S3. La gestion des versions est activée sur le compartiment des téléversements et les compartiments de ressources afin de permettre la reprise après des scénarios de suppression ou d'écrasement accidentels. Les compartiments de déploiement du site web et du frontend sont considérés comme des artefacts reproductibles et peuvent être reconstruits à partir du code source plutôt que restaurés à partir de sauvegardes.

4.6 Reprise des charges de travail asynchrones. Les voies de traitement asynchrones utilisent des files d'attente de lettres mortes pour conserver les événements ayant échoué aux fins d'enquête. La reprise peut inclure une nouvelle tentative de traitement des messages ayant échoué, la réexécution de la logique de traitement ou la relecture des tâches lorsque le flux de travail sous-jacent permet un retraitement sûr.

4.7 Reconstruction de l'application et de l'infrastructure. L'infrastructure est gérée au moyen de définitions d'infrastructure en tant que code contrôlées par le code source. Si l'infrastructure applicative ou les ressources statiques doivent être recréées, ProcessMind peut reconstruire et redéployer les composants affectés à partir de définitions contrôlées par version et d'artefacts de compilation.

4.8 Validation avant la remise en service. Avant de clôturer un incident, ProcessMind valide l'état du service au moyen de la surveillance disponible, des journaux, de contrôles synthétiques et d'une vérification fonctionnelle ciblée, et restaure les fonctionnalités affectées au moyen de procédures validées de déploiement, de reprise et d'infrastructure. Un examen supplémentaire peut être effectué lorsque l'incident a impliqué une restauration de données ou un risque pour l'intégrité des données.

---

5. Mesures de continuité d'activité

5.1 Continuité opérationnelle. ProcessMind maintient des procédures opérationnelles documentées afin que la gestion des incidents, la réception des demandes d'assistance client, la réponse de l'ingénierie et la prise de décisions puissent se poursuivre pendant les événements perturbateurs.

5.2 Communications. Pour les incidents de production importants, ProcessMind déploie des efforts commercialement raisonnables pour fournir des mises à jour par l'intermédiaire des canaux d'assistance client et, le cas échéant, de la page publique d'état à l'adresse processmind.com/status.

5.3 Gestion contrôlée des changements. Un cycle de développement logiciel reposant sur une défense en profondeur, avec plusieurs niveaux indépendants de validation automatisée, des déploiements contrôlés, une surveillance centralisée et un examen post-incident, est utilisé afin de réduire les interruptions évitables et d'améliorer la continuité au fil du temps.

5.4 Sécurité pendant la reprise. Les mesures de reprise sont exécutées sous réserve des mêmes principes généraux de sécurité que ceux applicables pendant les opérations normales, notamment l'accès selon le principe du moindre privilège, la journalisation de l'activité opérationnelle lorsqu'elle est disponible et l'accès contrôlé aux systèmes et aux données de production.

---

6. Synthèse des sauvegardes et de la protection des données

6.1 Sauvegardes de la base de données. Les sauvegardes automatisées Aurora sont chiffrées et conservées pendant sept (7) jours, la récupération à un instant donné étant disponible pendant cette période de conservation.

6.2 Protections S3. Amazon S3 offre une grande durabilité pour les objets stockés. Les compartiments de données client modifiables reposent sur la durabilité et la gestion des versions dans la région principale. ProcessMind n'active actuellement pas la réplication S3 interrégionale pour ces compartiments.

6.3 Journaux et diagnostics. Les journaux centralisés, les alarmes et la télémétrie facilitent l'analyse des défaillances et la validation de la reprise. Ces mécanismes soutiennent les opérations de continuité, mais ne sont pas eux-mêmes présentés comme un produit de sauvegarde distinct.

---

7. Identification et triage des incidents

7.1 Évaluation initiale. Les événements signalés font l'objet d'un triage afin de déterminer s'ils répondent à la définition d'un Incident de sécurité, quels systèmes ou données peuvent être affectés, quelle en est l'étendue et la gravité probables, et si un confinement immédiat est nécessaire. La conservation des éléments de preuve est assurée d'une manière adaptée à la nature de l'incident et aux systèmes concernés.

7.2 Astreinte et escalade. ProcessMind assure une couverture d'astreinte pour les incidents de production, y compris une couverture 24 h/24 et 7 j/7 pour les incidents Critiques (tels que définis dans l'Accord de niveau de service), afin que les incidents puissent être pris en compte et faire l'objet d'un triage à tout moment.

7.3 Documentation. ProcessMind documente les conclusions importantes des investigations, les mesures prises en réponse et les décisions de reprise, afin que la chronologie de l'incident et les mesures correctives qui en résultent puissent être examinées après l'événement.

---

8. Communications et notifications

8.1 Communication interne. ProcessMind coordonne les intervenants, les décideurs et les canaux d'assistance afin que la réponse technique et la communication avec les clients restent alignées pendant tout le cycle de vie de l'incident.

8.2 Notification des clients. En cas d'Incident de sécurité nécessitant une notification en vertu de l'APD ou du droit applicable, ProcessMind informe 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. Les notifications comprennent généralement la nature et l'étendue de l'incident, les catégories de données affectées si elles sont connues, les mesures prises pour contenir et remédier à l'incident, ainsi que les mesures recommandées aux clients, le cas échéant.

8.3 Mises à jour continues. Lorsque l'incident reste actif ou que des faits importants évoluent, ProcessMind fournit des mises à jour de suivi à mesure que des informations supplémentaires vérifiées deviennent disponibles. Pour les interruptions plus larges du service de production, ProcessMind peut également utiliser les canaux d'assistance client et, le cas échéant, la page publique d'état à l'adresse processmind.com/status.

---

9. Tests, examen et maintenance

ProcessMind examine ces procédures au moins une fois par an et après les incidents importants ou les changements architecturaux significatifs, met périodiquement à l'épreuve les éléments pertinents de son approche de réponse et de reprise (tels que la restauration des sauvegardes, la reconstruction des déploiements, la surveillance, les alertes et les communications relatives aux incidents), et intègre les enseignements tirés dans ses procédures de sécurité, de fiabilité et de continuité.

---

10. Limitations et limites contractuelles

Le présent document constitue un résumé de haut niveau et ne décrit pas en détail chaque runbook interne, voie d'escalade, méthode d'investigation ou étape de traitement des éléments de preuve dans le cadre opérationnel. Il n'engage pas ProcessMind à mettre en place une conception distincte de basculement interrégional, une conservation sur stockage immuable pour tous les compartiments modifiables, ni des garanties indépendantes de RTO/RPO au-delà de ce qui est expressément stipulé dans l'accord ou la commande applicable.

En cas de conflit entre le présent document et l'Accord client, l'Addendum relatif au traitement des données, l'Accord de niveau de service ou toute disposition légale impérative applicable, ces dernières sources prévalent.