ProcessMind Disaster Recovery, Business Continuity & Incident Response

Effective date: September 14, 2026

This document provides a high-level summary of ProcessMind B.V.'s disaster recovery ("DR"), business continuity ("BCP"), and security incident response procedures for its cloud service. It supplements the Security Measures, the SaaS Hosting Policy, the Service Level Agreement and the Data Processing Addendum.

It explains our current approach and does not create separate contractual recovery time objectives, recovery point objectives, data durability warranties, notification deadlines, service levels or liability standards beyond what is expressly stated in the applicable agreement, DPA or SLA.

---

1. Objectives and Scope

ProcessMind maintains these procedures to:

- protect the confidentiality, integrity, and availability of Customer Data during a disruptive event
- restore critical production service components after failures in ProcessMind-controlled systems
- continue incident management, customer communication, and operational decision-making during service disruptions
- recover from infrastructure, deployment, application, or data-layer failures using documented procedures and source-controlled infrastructure definitions
- identify and assess Security Incidents, contain threats, eradicate root causes, recover affected systems, communicate as required, and capture lessons learned

These procedures apply to the production ProcessMind cloud service and to security events involving sub-processors or cloud services to the extent

they affect the Service and are within ProcessMind's reasonable ability to investigate and manage. Development and test environments are segregated and are not treated as recovery targets for customer-facing production commitments.

---

2. Resilience Strategy

2.1 Regional Design. Production services are hosted in AWS EU (Frankfurt, Germany, `eu-central-1`). The architecture relies on AWS managed services within that region, which AWS operates across multiple Availability Zones. The Aurora cluster currently runs a single writer instance, so database recovery relies on automated backups and point-in-time recovery rather than an in-region standby. ProcessMind does not currently operate a second active customer-data region.

2.2 Managed and Serverless Services. ProcessMind relies on AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS, and Amazon CloudWatch. This reduces dependency on customer-managed long-lived servers and supports rebuild-from-source recovery for application and static components.

2.3 Environment Separation. Production and development environments operate in separate AWS accounts with separate databases and infrastructure stacks. This reduces the risk that development activity affects production recovery operations.

2.4 Monitoring and Detection. CloudWatch alarms, dashboards, dead-letter queue alerts, centralized logging, and synthetic service monitoring support incident detection, triage, and escalation. Potential incidents may also be identified through support intake, employee reports, vendor notifications, or other investigation triggers.

---

3. Recovery Priorities

During a major incident, ProcessMind's recovery priorities are generally:

1. Protect customer data integrity and prevent further damage.
2. Contain the incident and stabilize affected systems.
3. Restore core production access paths and critical workflows.
4. Validate service behavior, data integrity, and monitoring before declaring recovery complete.
5. Communicate status updates, customer impact, and follow-up actions.

The exact sequence may vary depending on the nature of the incident, including whether it affects data integrity, customer access, asynchronous processing, or supporting infrastructure.

---

4. Disaster Recovery Procedures

4.1 Incident Declaration and Coordination. Material service disruptions and security incidents are triaged through incident response procedures. ProcessMind designates an incident lead, limits response participation to authorized personnel, assesses severity and scope, coordinates technical responders, and tracks recovery actions until the incident is resolved or downgraded.

4.2 Containment. ProcessMind uses commercially reasonable efforts to stop or reduce ongoing impact before broader restoration begins. Depending on the failure mode, containment actions may include rolling back recent changes, disabling affected paths, isolating malfunctioning components, pausing background processing while integrity checks are performed, revoking or rotating credentials, or blocking abusive activity.

4.3 Eradication. After the immediate impact is stabilized, ProcessMind works to remove the root cause or contributing condition. This may include applying code or configuration fixes, removing malicious artifacts, rotating secrets, restoring trusted configuration, or closing exposed access paths.

4.4 Database Recovery. Aurora PostgreSQL performs continuous automated backups with a seven (7) day retention window and supports point-in-time recovery. If a database-level failure, corruption event, or accidental destructive change requires restoration, ProcessMind may restore from the latest suitable backup or to a selected point in time, validate the restored environment, and return application traffic to the recovered database path.

4.5 Object and Artifact Recovery. Customer file uploads and operational artifacts are stored in Amazon S3. Versioning is enabled on the uploads bucket and resource buckets to support recovery from accidental deletion or overwrite scenarios. Website and frontend deployment buckets are treated as reproducible artifacts and may be rebuilt from source rather than restored as backups.

4.6 Asynchronous Workload Recovery. Asynchronous processing paths use dead-letter queues to retain failed events for investigation. Recovery may include retrying failed messages, re-running processing logic, or replaying work where the underlying workflow supports safe reprocessing.

4.7 Application and Infrastructure Rebuild. Infrastructure is managed through source-controlled infrastructure-as-code definitions. If application infrastructure or static assets need to be recreated, ProcessMind can rebuild and redeploy affected components from version-controlled definitions and build artifacts.

4.8 Validation Before Return to Service. Before an incident is closed, ProcessMind validates service health using available monitoring, logs, synthetic checks, and targeted functional verification, and restores affected functionality using validated deployment, recovery, and infrastructure procedures. Additional review may be performed when the incident involved data restoration or data-integrity risk.

---

5. Business Continuity Measures

5.1 Operational Continuity. ProcessMind maintains documented operational procedures so that incident handling, customer support intake, engineering response, and decision-making can continue during disruptive events.

5.2 Communications. For material production incidents, ProcessMind uses commercially reasonable efforts to provide updates through customer support channels and, where appropriate, the public status page at processmind.com/status.

5.3 Controlled Change Management. A defense-in-depth software development lifecycle with multiple independent automated validation layers, controlled deployments, centralized monitoring, and post-incident review is used to reduce avoidable outages and to improve continuity over time.

5.4 Security During Recovery. Recovery actions are performed subject to the same general security principles that apply during normal operations, including least-privilege access, logged operational activity where available, and controlled access to production systems and data.

---

6. Backup and Data Protection Summary

6.1 Database Backups. Aurora automated backups are encrypted and retained for seven (7) days, with point-in-time recovery available within that retention window.

6.2 S3 Protections. Amazon S3 provides high durability for stored objects. Mutable customer-data buckets rely on durability and versioning within the primary region. ProcessMind does not currently enable cross-region S3 replication for those buckets.

6.3 Logs and Diagnostics. Centralized logs, alarms, and telemetry support failure investigation and recovery validation. These mechanisms support

continuity operations but are not themselves presented as a separate backup product.

---

7. Incident Identification and Triage

7.1 Initial Assessment. Reported events are triaged to determine whether they meet the definition of a Security Incident, what systems or data may be affected, the likely scope and severity, and whether immediate containment is required. Evidence preservation is handled in a manner appropriate to the nature of the incident and the systems involved.

7.2 On-Call and Escalation. ProcessMind maintains on-call coverage for production incidents, including 24x7 coverage for Critical incidents (as defined in the Service Level Agreement), so that incidents can be acknowledged and triaged at any time.

7.3 Documentation. ProcessMind documents material investigation findings, response actions, and recovery decisions so the incident timeline and resulting corrective actions can be reviewed after the event.

---

8. Communications and Notification

8.1 Internal Communication. ProcessMind coordinates responders, decision-makers, and support channels so that technical response and customer communication remain aligned throughout the incident lifecycle.

8.2 Customer Notification. In the event of a Security Incident requiring notification under the DPA or applicable law, ProcessMind notifies affected customers without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the incident. Notifications generally include the nature and scope of the incident, the data categories affected if known, measures taken to contain and remediate the incident, and recommended customer actions where relevant.

8.3 Ongoing Updates. Where the incident remains active or material facts change, ProcessMind provides follow-up updates as additional verified information becomes available. For broader production service disruptions, ProcessMind may also use customer support channels and, where appropriate, the public status page at processmind.com/status.

---

9. Testing, Review and Maintenance

ProcessMind reviews these procedures at least annually and after material incidents or significant architectural changes, periodically exercises relevant elements of the response and recovery approach (such as backup restoration, deployment rebuild, monitoring, alerting, and incident communications), and incorporates lessons learned into its security, reliability, and continuity procedures.

---

10. Limitations and Contractual Boundaries

This document is a high-level summary and does not describe every internal runbook, escalation path, investigative method, or evidence-handling step in operational detail. It does not commit ProcessMind to a separate cross-region failover design, immutable storage retention for all mutable buckets, or independent RTO/RPO warranties beyond what is expressly stated in the applicable agreement or order.

If there is any conflict between this document and the applicable Customer Agreement, Data Processing Addendum, Service Level Agreement, or mandatory law, those sources control.