

ProcessMind 재해 복구, 업무 연속성 및 사고 대응

시행일: 2026년 9월 14일

본 문서는 ProcessMind B.V.의 클라우드 서비스에 대한 재해 복구("DR"), 업무 연속성("BCP") 및 보안 사고 대응 절차를 개괄적으로 요약합니다. 본 문서는 [보안 조치](#), [SaaS 호스팅 정책](#), [서비스 수준 계약](#) 및 [데이터 처리 부속서](#)를 보완합니다.

본 문서는 당사의 현재 접근 방식을 설명하며, 해당 계약, DPA 또는 SLA에 명시적으로 규정된 사항을 넘어 별도의 계약상 복구 시간 목표, 복구 시점 목표, 데이터 내구성 보증, 통지 기한, 서비스 수준 또는 책임 기준을 설정하지 않습니다.

1. 목적 및 적용 범위

ProcessMind는 다음을 위해 이러한 절차를 유지합니다.

- 중단 사태 발생 시 고객 데이터의 기밀성, 무결성 및 가용성을 보호합니다.
- ProcessMind가 관리하는 시스템의 장애 발생 후 핵심 프로덕션 서비스 구성요소를 복구합니다.
- 서비스 중단 중에도 사고 관리, 고객 커뮤니케이션 및 운영상 의사결정을 지속합니다.
- 문서화된 절차와 소스 관리되는 인프라 정의를 사용하여 인프라, 배포, 애플리케이션 또는 데이터 계층의 장애로부터 복구합니다.
- 보안 사고를 식별하고 평가하며, 위협을 억제하고, 근본 원인을 제거하고, 영향을 받은 시스템을 복구하고, 필요한 경우 관련 내용을 전달하며, 교훈을 기록합니다.

본 절차는 ProcessMind의 프로덕션 클라우드 서비스와, 하위 처리자 또는 클라우드 서비스와 관련된 보안 이벤트가 서비스에 영향을 미치고 ProcessMind가 합리적으로 조사 및 관리할 수 있는 범위 내에 있는 경우 해당 이벤트에 적용됩니다. 개발 및 테스트 환경은 분리되어 있으며, 고객 대상 프로덕션 서비스 약정의 복구 대상으로 취급되지 않습니다.

2. 복원력 전략

2.1 리전 설계. 프로덕션 서비스는 AWS EU(독일 프랑크푸르트, eu-central-1)에서 호스팅됩니다. 아키텍처는 해당 리전 내 AWS 관리형 서비스를 기반으로 하며, AWS는 이를 여러

가용 영역에 걸쳐 운영합니다. Aurora 클러스터는 현재 단일 라이터 인스턴스를 실행하므로, 데이터베이스 복구는 리전 내 대기 인스턴스가 아니라 자동 백업 및 특정 시점 복구에 의존합니다. ProcessMind는 현재 고객 데이터를 보유하는 두 번째 활성 리전을 운영하지 않습니다.

2.2 관리형 및 서버리스 서비스. ProcessMind는 AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS 및 Amazon CloudWatch를 사용합니다. 이를 통해 고객이 관리하는 장기 실행 서버에 대한 의존도를 낮추고 애플리케이션 및 정적 구성 요소를 소스에서 다시 빌드하여 복구할 수 있습니다.

2.3 환경 분리. 프로덕션 환경과 개발 환경은 별도의 AWS 계정에서 각각 별도의 데이터베이스 및 인프라 스택을 사용하여 운영됩니다. 이를 통해 개발 활동이 프로덕션 복구 운영에 영향을 미칠 위험을 줄입니다.

2.4 모니터링 및 탐지. CloudWatch 경보, 대시보드, 데드 레터 큐 경보, 중앙 집중식 로깅 및 합성 서비스 모니터링은 사고 탐지, 분류 및 에스컬레이션을 지원합니다. 잠재적 사고는 지원 요청 접수, 직원 보고, 공급업체 통지 또는 기타 조사 개시 요인을 통해서도 식별될 수 있습니다.

3. 복구 우선순위

중대한 사고가 발생한 경우 ProcessMind의 일반적인 복구 우선순위는 다음과 같습니다.

1. 고객 데이터의 무결성을 보호하고 추가 피해를 방지합니다.
2. 사고를 억제하고 영향을 받은 시스템을 안정화합니다.
3. 핵심 프로덕션 액세스 경로와 중요 워크플로를 복구합니다.
4. 복구 완료 선언하기 전에 서비스 동작, 데이터 무결성 및 모니터링을 검증합니다.
5. 상태 업데이트, 고객 영향 및 후속 조치를 전달합니다.

정확한 순서는 사고의 성격에 따라 달라질 수 있으며, 여기에는 데이터 무결성, 고객 액세스, 비동기 처리 또는 지원 인프라에 영향을 미치는지 여부가 포함됩니다.

4. 재해 복구 절차

4.1 사고 선언 및 조정. 중대한 서비스 중단 및 보안 사고는 사고 대응 절차에 따라 분류됩니다. ProcessMind는 사고 책임자를 지정하고, 대응 참여를 권한이 있는 인원으로 제한하며, 심각도와 범위를 평가하고, 기술 대응 담당자를 조정하며, 사고가 해결되거나 등급이 하향 조정될 때까지 복구 조치를 추적합니다.

4.2 억제. ProcessMind는 광범위한 복구를 시작하기 전에 지속 중인 영향을 중단하거나 줄이기 위해 상업적으로 합리적인 노력을 기울입니다. 장애 유형에 따라 억제 조치에는 최근 변경 사항 롤백, 영향을 받은 경로 비활성화, 오작동 구성 요소 격리, 무결성 검사를 수행하는 동안 백그라운드 처리 일시 중지, 자격 증명 취소 또는 교체, 악의적 활동 차단 등이 포함될 수 있습니다.

4.3 근본 원인 제거. 즉각적인 영향이 안정화된 후 ProcessMind는 근본 원인 또는 기여 요인을 제거하기 위해 노력합니다. 여기에는 코드 또는 구성 수정 적용, 악성 아티팩트 제거, 비밀 정보 교체, 신뢰할 수 있는 구성 복원 또는 노출된 액세스 경로 폐쇄가 포함될 수 있습니다.

4.4 데이터베이스 복구. Aurora PostgreSQL은 7일의 보존 기간으로 지속적인 자동 백업을 수행하며 특정 시점 복구를 지원합니다. 데이터베이스 수준의 장애, 손상 이벤트 또는 실수로 인한 파괴적 변경으로 복원이 필요한 경우, ProcessMind는 가장 최근의 적절한 백업 또는 선택한 특정 시점으로 복원하고, 복원된 환경을 검증한 다음, 애플리케이션 트래픽을 복구된 데이터베이스 경로로 되돌릴 수 있습니다.

4.5 객체 및 아티팩트 복구. 고객 파일 업로드 및 운영 아티팩트는 Amazon S3에 저장됩니다. 업로드 버킷과 리소스 버킷에는 버전 관리가 활성화되어 있어 실수로 삭제하거나 덮어쓰는 경우 복구할 수 있습니다. 웹사이트 및 프런트엔드 배포 버킷은 재현 가능한 아티팩트로 취급되며 백업에서 복원하는 대신 소스에서 재구축할 수 있습니다.

4.6 비동기 워크로드 복구. 비동기 처리 경로는 조사할 수 있도록 실패한 이벤트를 데드 레터 큐에 보관합니다. 복구에는 실패한 메시지 재시도, 처리 로직 재실행 또는 기반 워크플로가 안전한 재처리를 지원하는 경우 작업 재생이 포함될 수 있습니다.

4.7 애플리케이션 및 인프라 재구축. 인프라는 소스 제어되는 인프라 코드 정의를 통해 관리됩니다. 애플리케이션 인프라 또는 정적 자산을 다시 생성해야 하는 경우, ProcessMind는 버전 관리되는 정의 및 빌드 아티팩트에서 영향을 받은 구성 요소를 재구축하고 재배포할 수 있습니다.

4.8 서비스 재개 전 검증. 사고를 종결하기 전에 ProcessMind는 사용 가능한 모니터링, 로그, 합성 검사 및 대상 기능 검증을 사용하여 서비스 상태를 확인하고, 검증된 배포, 복구 및 인프라 절차를 통해 영향을 받은 기능을 복원합니다. 사고에 데이터 복원 또는 데이터 무결성 위험이 관련된 경우 추가 검토를 수행할 수 있습니다.

5. 업무 연속성 조치

5.1 운영 연속성. ProcessMind는 장애 발생 중에도 사고 처리, 고객 지원 요청 접수, 엔지니어링 대응 및 의사결정을 지속할 수 있도록 문서화된 운영 절차를 유지합니다.

5.2 커뮤니케이션. 중대한 프로덕션 사고가 발생한 경우 ProcessMind는 고객 지원 채널을 통해, 그리고 적절한 경우 공개 상태 페이지 processmind.com/status를 통해 업데이트를 제공하기 위해 상업적으로 합리적인 노력을 기울입니다.

5.3 통제된 변경 관리. 방어 심층형 소프트웨어 개발 수명 주기, 여러 독립적인 자동 검증 계층, 통제된 배포, 중앙 집중식 모니터링 및 사고 후 검토를 통해 예방 가능한 서비스 중단을 줄이고 시간이 지남에 따라 연속성을 개선합니다.

5.4 복구 중 보안. 복구 조치는 최소 권한 액세스, 가능한 경우 운영 활동의 기록, 프로덕션 시스템 및 데이터에 대한 통제된 액세스 등 정상 운영 중 적용되는 것과 동일한 일반 보안 원칙에 따라 수행됩니다.

6. 백업 및 데이터 보호 요약

6.1 데이터베이스 백업. Aurora 자동 백업은 암호화되어 7일간 보존되며, 해당 보존 기간 내에 특정 시점 복구를 이용할 수 있습니다.

6.2 S3 보호. Amazon S3는 저장된 객체에 높은 내구성을 제공합니다. 변경 가능한 고객 데이터 버킷은 기본 리전 내의 내구성 및 버전 관리에 의존합니다. ProcessMind는 현재 해당 버킷에 대해 리전 간 S3 복제를 활성화하지 않습니다.

6.3 로그 및 진단. 중앙 집중식 로그, 경고 및 원격 측정 데이터는 장애 조사와 복구 검증을 지원합니다. 이러한 메커니즘은 연속성 운영을 지원하지만 별도의 백업 제품으로 제시되는 것은 아닙니다.

7. 사고 식별 및 분류

7.1 초기 평가. 보고된 이벤트를 분류하여 보안 사고의 정의에 해당하는지, 어떤 시스템 또는 데이터가 영향을 받을 수 있는지, 예상되는 범위와 심각도는 어떠한지, 즉각적인 억제가 필요한지를 판단합니다. 증거 보존은 사고의 성격과 관련 시스템에 적합한 방식으로 처리됩니다.

7.2 대기 대응 및 에스컬레이션. ProcessMind는 프로덕션 사고에 대한 대기 대응 체계를 유지하며, 서비스 수준 계약에 정의된 중대 사고에 대해서는 연중무휴 24시간 대응하여 언제든지 사고를 접수하고 분류할 수 있도록 합니다.

7.3 문서화. ProcessMind는 중요한 조사 결과, 대응 조치 및 복구 결정을 문서화하여 사고 경과와 그에 따른 시정 조치를 사고 발생 후 검토할 수 있도록 합니다.

8. 커뮤니케이션 및 통지

8.1 내부 커뮤니케이션. ProcessMind는 사고 수명 주기 전반에 걸쳐 기술 대응과 고객 커뮤니케이션이 일관되게 이루어지도록 대응 담당자, 의사결정자 및 지원 채널을 조정합니다.

8.2 고객 통지. DPA 또는 관련 법률에 따라 통지가 필요한 보안 사고가 발생한 경우, ProcessMind는 부당한 지체 없이, 그리고 가능한 경우 사고를 인지한 시점부터 72시간 이내에 영향을 받은 고객에게 통지합니다. 통지에는 일반적으로 사고의 성격과 범위, 알려진 경우 영향을 받은 데이터 범주, 사고를 억제하고 시정하기 위해 취한 조치, 관련성이 있는 경우 권고되는 고객 조치가 포함됩니다.

8.3 지속적인 업데이트. 사고가 계속 진행 중이거나 중요한 사실이 변경되는 경우, ProcessMind는 추가로 검증된 정보가 확보되는 대로 후속 업데이트를 제공합니다. 보다 광범위한 프로덕션 서비스 중단인 경우 ProcessMind는 고객 지원 채널을 이용하고, 적절한 경우 공개 상태 페이지 processmind.com/status를 이용할 수도 있습니다.

9. 테스트, 검토 및 유지 관리

ProcessMind는 이 절차를 최소 연 1회 및 중대한 사고나 주요 아키텍처 변경 후에 검토하고, 대응 및 복구 방식의 관련 요소(예: 백업 복원, 배포 재구축, 모니터링, 경보 및 사고 커뮤니케이션)를 주기적으로 시험하며, 얻은 교훈을 보안, 신뢰성 및 연속성 절차에 반영합니다.

10. 제한 사항 및 계약상 경계

이 문서는 개괄적인 요약이며 모든 내부 런북, 에스컬레이션 경로, 조사 방법 또는 증거 처리 단계를 운영상 세부적으로 설명하지 않습니다. 또한 적용되는 계약 또는 주문서에 명시적으로 규정된 범위를 넘어 별도의 리전 간 장애 조치 설계, 모든 변경 가능 버킷에 대한 불변 스토리지 보존 또는 독립적인 RTO/RPO 보증을 ProcessMind가 약정하는 것은 아닙니다.

이 문서와 적용되는 고객 계약, 데이터 처리 부속서, 서비스 수준 계약 또는 강행 법률 간에 상충이 있는 경우 해당 문서 또는 법률이 우선합니다.