

Pemulihan Bencana, Kelangsungan Bisnis & Respons Insiden ProcessMind

Tanggal berlaku: 14 September 2026

Dokumen ini memberikan ringkasan tingkat tinggi mengenai prosedur pemulihan bencana ("DR"), kelangsungan bisnis ("BCP"), dan respons insiden keamanan ProcessMind B.V. untuk layanan cloud-nya. Dokumen ini melengkapi [Langkah-Langkah Keamanan](#), [Kebijakan Hosting SaaS](#), [Perjanjian Tingkat Layanan](#), dan [Adendum Pemrosesan Data](#).

Dokumen ini menjelaskan pendekatan kami saat ini dan tidak menetapkan sasaran waktu pemulihan, sasaran titik pemulihan, jaminan ketahanan data, tenggat pemberitahuan, tingkat layanan, atau standar tanggung jawab kontraktual yang terpisah di luar yang secara tegas dinyatakan dalam perjanjian, DPA, atau SLA yang berlaku.

1. Tujuan dan Cakupan

ProcessMind memelihara prosedur ini untuk:

- melindungi kerahasiaan, integritas, dan ketersediaan Data Pelanggan selama peristiwa yang mengganggu
- memulihkan komponen layanan produksi yang kritis setelah kegagalan pada sistem yang dikendalikan ProcessMind
- melanjutkan manajemen insiden, komunikasi dengan pelanggan, dan pengambilan keputusan operasional selama gangguan layanan
- memulihkan layanan dari kegagalan infrastruktur, penerapan, aplikasi, atau lapisan data dengan menggunakan prosedur terdokumentasi dan definisi infrastruktur yang dikendalikan versi
- mengidentifikasi dan menilai Insiden Keamanan, membatasi ancaman, menghilangkan akar penyebab, memulihkan sistem yang terdampak, menyampaikan komunikasi sebagaimana diwajibkan, dan mencatat pelajaran yang diperoleh

Prosedur ini berlaku untuk layanan cloud produksi ProcessMind dan peristiwa keamanan yang melibatkan subprosesor atau layanan cloud sejauh peristiwa tersebut memengaruhi Layanan dan berada dalam kemampuan wajar ProcessMind untuk menyelidiki dan menanganinya. Lingkungan pengembangan dan pengujian dipisahkan dan tidak diperlakukan sebagai sasaran pemulihan untuk komitmen produksi yang ditujukan kepada pelanggan.

2. Strategi Ketahanan

2.1 Desain Regional. Layanan produksi dihosting di AWS EU (Frankfurt, Jerman, eu-central-1). Arsitektur ini mengandalkan layanan terkelola AWS di wilayah tersebut, yang dioperasikan AWS di beberapa Availability Zone. Kluster Aurora saat ini menjalankan satu instans penulis, sehingga pemulihan basis data mengandalkan pencadangan otomatis dan pemulihan titik waktu, bukan instans siaga di wilayah yang sama. Saat ini ProcessMind tidak mengoperasikan wilayah kedua yang aktif untuk data pelanggan.

2.2 Layanan Terkelola dan Tanpa Server. ProcessMind mengandalkan AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS, dan Amazon CloudWatch. Hal ini mengurangi ketergantungan pada server berumur panjang yang dikelola pelanggan dan mendukung pemulihan melalui pembangunan ulang dari sumber untuk komponen aplikasi dan statis.

2.3 Pemisahan Lingkungan. Lingkungan produksi dan pengembangan beroperasi di akun AWS yang terpisah, dengan basis data dan tumpukan infrastruktur yang terpisah. Hal ini mengurangi risiko aktivitas pengembangan memengaruhi operasional pemulihan produksi.

2.4 Pemantauan dan Deteksi. Alarm CloudWatch, dasbor, peringatan antrean surat mati, pencatatan terpusat, dan pemantauan layanan sintetis mendukung deteksi, triase, dan eskalasi insiden. Potensi insiden juga dapat diidentifikasi melalui penerimaan permintaan dukungan,

laporan karyawan, pemberitahuan vendor, atau pemicu investigasi lainnya.

3. Prioritas Pemulihan

Selama insiden besar, prioritas pemulihan ProcessMind secara umum adalah:

1. Melindungi integritas data pelanggan dan mencegah kerusakan lebih lanjut.
2. Membatasi insiden dan menstabilkan sistem yang terdampak.
3. Memulihkan jalur akses produksi inti dan alur kerja penting.
4. Memvalidasi perilaku layanan, integritas data, dan pemantauan sebelum menyatakan pemulihan selesai.
5. Menyampaikan pembaruan status, dampak terhadap pelanggan, dan tindakan tindak lanjut.

Urutan yang tepat dapat berbeda-beda bergantung pada sifat insiden, termasuk apakah insiden tersebut memengaruhi integritas data, akses pelanggan, pemrosesan asinkron, atau infrastruktur pendukung.

4. Prosedur Pemulihan Bencana

4.1 Deklarasi dan Koordinasi Insiden. Gangguan layanan yang signifikan dan insiden keamanan ditriase melalui prosedur tanggap insiden.

ProcessMind menunjuk pemimpin insiden, membatasi partisipasi dalam penanganan kepada personel yang berwenang, menilai tingkat keparahan dan cakupan, mengoordinasikan petugas teknis, serta melacak tindakan pemulihan hingga insiden diselesaikan atau diturunkan tingkatnya.

4.2 Pembatasan Dampak. ProcessMind melakukan upaya yang wajar secara komersial untuk menghentikan atau mengurangi dampak yang sedang berlangsung sebelum memulai pemulihan yang lebih luas. Bergantung pada jenis kegagalan, tindakan pembatasan dampak dapat

mencakup mengembalikan perubahan terbaru, menonaktifkan jalur yang terdampak, mengisolasi komponen yang tidak berfungsi, menjeda pemrosesan latar belakang saat pemeriksaan integritas dilakukan, mencabut atau merotasi kredensial, atau memblokir aktivitas penyalahgunaan.

4.3 Pemberantasan. Setelah dampak langsung distabilkan, ProcessMind berupaya menghilangkan akar penyebab atau kondisi yang berkontribusi. Hal ini dapat mencakup menerapkan perbaikan kode atau konfigurasi, menghapus artefak berbahaya, merotasi rahasia, memulihkan konfigurasi tepercaya, atau menutup jalur akses yang terekspos.

4.4 Pemulihan Basis Data. Aurora PostgreSQL melakukan pencadangan otomatis berkelanjutan dengan masa retensi tujuh (7) hari dan mendukung pemulihan titik waktu. Jika kegagalan tingkat basis data, peristiwa kerusakan data, atau perubahan destruktif yang tidak disengaja mengharuskan pemulihan, ProcessMind dapat memulihkan dari pencadangan terbaru yang sesuai atau ke titik waktu yang dipilih, memvalidasi lingkungan yang dipulihkan, dan mengalihkan lalu lintas aplikasi kembali ke jalur basis data yang telah dipulihkan.

4.5 Pemulihan Objek dan Artefak. Unggahan berkas pelanggan dan artefak operasional disimpan di Amazon S3. Pembuatan versi diaktifkan pada bucket unggahan dan bucket sumber daya untuk mendukung pemulihan dari penghapusan atau penyimpanan yang tidak disengaja. Bucket penerapan situs web dan frontend diperlakukan sebagai artefak yang dapat direproduksi dan dapat dibangun ulang dari sumber, alih-alih dipulihkan sebagai cadangan.

4.6 Pemulihan Beban Kerja Asinkron. Jalur pemrosesan asinkron menggunakan antrean surat mati untuk menyimpan peristiwa yang gagal agar dapat diselidiki. Pemulihan dapat mencakup mencoba kembali pesan yang gagal, menjalankan ulang logika pemrosesan, atau memutar ulang pekerjaan jika alur kerja yang mendasarinya mendukung pemrosesan ulang yang aman.

4.7 Pembangunan Ulang Aplikasi dan Infrastruktur. Infrastruktur dikelola melalui definisi infrastruktur–sebagai–kode yang dikendalikan sumber. Jika infrastruktur aplikasi atau aset statis perlu dibuat ulang, ProcessMind dapat membangun ulang dan menerapkan kembali komponen yang terdampak dari definisi yang dikendalikan versi dan artefak build.

4.8 Validasi Sebelum Layanan Kembali Beroperasi. Sebelum insiden ditutup, ProcessMind memvalidasi kesehatan layanan menggunakan pemantauan, log, pemeriksaan sintetis, dan verifikasi fungsional terarah yang tersedia, serta memulihkan fungsi yang terdampak menggunakan prosedur penerapan, pemulihan, dan infrastruktur yang telah divalidasi. Peninjauan tambahan dapat dilakukan jika insiden melibatkan pemulihan data atau risiko terhadap integritas data.

5. Langkah–langkah Kelangsungan Bisnis

5.1 Kelangsungan Operasional. ProcessMind memelihara prosedur operasional terdokumentasi agar penanganan insiden, penerimaan permintaan dukungan pelanggan, tanggapan rekayasa, dan pengambilan keputusan dapat terus berlangsung selama peristiwa yang mengganggu.

5.2 Komunikasi. Untuk insiden produksi yang signifikan, ProcessMind melakukan upaya yang wajar secara komersial untuk memberikan pembaruan melalui saluran dukungan pelanggan dan, jika sesuai, halaman status publik di processmind.com/status.

5.3 Manajemen Perubahan Terkendali. Siklus hidup pengembangan perangkat lunak dengan pertahanan berlapis, beberapa lapisan validasi otomatis yang independen, penerapan terkendali, pemantauan terpusat, dan peninjauan pascainsiden digunakan untuk mengurangi gangguan yang dapat dihindari dan meningkatkan kelangsungan dari waktu ke waktu.

5.4 Keamanan Selama Pemulihan. Tindakan pemulihan dilakukan dengan tunduk pada prinsip keamanan umum yang sama dengan yang berlaku

selama operasional normal, termasuk akses dengan hak istimewa minimum, pencatatan aktivitas operasional jika tersedia, serta akses terkendali ke sistem dan data produksi.

6. Ringkasan Pencadangan dan Perlindungan Data

6.1 Pencadangan Basis Data. Pencadangan otomatis Aurora dienkripsi dan disimpan selama tujuh (7) hari, dengan pemulihan titik waktu tersedia dalam masa retensi tersebut.

6.2 Perlindungan S3. Amazon S3 menyediakan daya tahan tinggi untuk objek yang disimpan. Bucket data pelanggan yang dapat diubah mengandalkan daya tahan dan pembuatan versi di wilayah utama. Saat ini ProcessMind tidak mengaktifkan replikasi S3 lintas wilayah untuk bucket tersebut.

6.3 Log dan Diagnostik. Log terpusat, alarm, dan telemetri mendukung investigasi kegagalan dan validasi pemulihan. Mekanisme ini mendukung operasional kelangsungan, tetapi tidak disajikan sebagai produk pencadangan tersendiri.

7. Identifikasi dan Triase Insiden

7.1 Penilaian Awal. Peristiwa yang dilaporkan ditriase untuk menentukan apakah peristiwa tersebut memenuhi definisi Insiden Keamanan, sistem atau data apa yang mungkin terdampak, cakupan dan tingkat keparahan yang mungkin terjadi, serta apakah pembatasan dampak segera diperlukan. Pelestarian bukti ditangani dengan cara yang sesuai dengan sifat insiden dan sistem yang terlibat.

7.2 Petugas Siaga dan Eskalasi. ProcessMind menyediakan petugas siaga untuk insiden produksi, termasuk cakupan 24x7 untuk insiden Kritis (sebagaimana didefinisikan dalam Perjanjian Tingkat Layanan), agar insiden dapat diakui dan ditriase kapan saja.

7.3 Dokumentasi. ProcessMind mendokumentasikan temuan investigasi yang signifikan, tindakan tanggapan, dan keputusan pemulihan agar linimasa insiden dan tindakan korektif yang dihasilkan dapat ditinjau setelah peristiwa tersebut.

8. Komunikasi dan Pemberitahuan

8.1 Komunikasi Internal. ProcessMind mengoordinasikan petugas tanggap, pengambil keputusan, dan saluran dukungan agar tanggapan teknis dan komunikasi pelanggan tetap selaras sepanjang siklus hidup insiden.

8.2 Pemberitahuan kepada Pelanggan. Jika terjadi Insiden Keamanan yang mengharuskan pemberitahuan berdasarkan DPA atau hukum yang berlaku, ProcessMind memberitahukan pelanggan yang terdampak tanpa penundaan yang tidak semestinya dan, jika memungkinkan, dalam waktu tujuh puluh dua (72) jam sejak mengetahui insiden tersebut. Pemberitahuan umumnya mencakup sifat dan cakupan insiden, kategori data yang terdampak jika diketahui, langkah-langkah yang diambil untuk membatasi dampak dan memperbaiki insiden, serta tindakan yang disarankan kepada pelanggan jika relevan.

8.3 Pembaruan Berkelanjutan. Jika insiden masih berlangsung atau fakta penting berubah, ProcessMind memberikan pembaruan lanjutan saat informasi terverifikasi tambahan tersedia. Untuk gangguan layanan produksi yang lebih luas, ProcessMind juga dapat menggunakan saluran dukungan pelanggan dan, jika sesuai, halaman status publik di processmind.com/status.

9. Pengujian, Peninjauan, dan Pemeliharaan

ProcessMind meninjau prosedur ini setidaknya setiap tahun dan setelah insiden signifikan atau perubahan arsitektur yang besar, secara berkala menguji unsur-unsur yang relevan dari pendekatan tanggapan dan

pemulihan (seperti pemulihan pencadangan, pembangunan ulang penerapan, pemantauan, pemberian peringatan, dan komunikasi insiden), serta memasukkan pelajaran yang diperoleh ke dalam prosedur keamanan, keandalan, dan kelangsungan.

10. Batasan dan Batas Kontraktual

Dokumen ini merupakan ringkasan tingkat tinggi dan tidak menjelaskan setiap runbook internal, jalur eskalasi, metode investigasi, atau langkah penanganan bukti secara terperinci dalam operasional. Dokumen ini tidak mengikat ProcessMind untuk menerapkan desain failover lintas wilayah tersendiri, retensi penyimpanan yang tidak dapat diubah untuk semua bucket yang dapat diubah, atau jaminan RTO/RPO independen di luar yang secara tegas dinyatakan dalam perjanjian atau pesanan yang berlaku.

Jika terdapat pertentangan antara dokumen ini dan Perjanjian Pelanggan, Adendum Pemrosesan Data, Perjanjian Tingkat Layanan, atau hukum wajib yang berlaku, ketentuan dalam sumber-sumber tersebut yang berlaku.