ProcessMind Felaket Kurtarma, İş Sürekliliği ve Olaylara Müdahale

Yürürlük tarihi: 14 Eylül 2026

Bu belge, ProcessMind B.V.'nin bulut hizmetine ilişkin felaket kurtarma ("DR"), iş sürekliliği ("BCP") ve güvenlik olaylarına müdahale prosedürlerinin üst düzey bir özetini sunar. Güvenlik Önlemlerini, SaaS Barındırma Politikasını, Hizmet Seviyesi Sözleşmesini ve Veri İşleme Ekini tamamlar.

Bu belge mevcut yaklaşımımızı açıklar ve geçerli sözleşmede, DPA'da veya SLA'da açıkça belirtilenlerin ötesinde ayrı sözleşmesel kurtarma süresi hedefleri, kurtarma noktası hedefleri, veri dayanıklılığı garantileri, bildirim süreleri, hizmet seviyeleri veya sorumluluk standartları oluşturmaz.

---

1. Amaçlar ve Kapsam

ProcessMind bu prosedürleri aşağıdaki amaçlarla sürdürür:

- kesintiye yol açan bir olay sırasında Müşteri Verilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak
- ProcessMind tarafından kontrol edilen sistemlerdeki arızaların ardından kritik üretim hizmeti bileşenlerini geri yüklemek
- hizmet kesintileri sırasında olay yönetimini, müşteri iletişimini ve operasyonel karar almayı sürdürmek
- belgelenmiş prosedürleri ve kaynak denetimli altyapı tanımlarını kullanarak altyapı, dağıtım, uygulama veya veri katmanı arızalarından kurtulmak
- Güvenlik Olaylarını belirlemek ve değerlendirmek, tehditleri kontrol altına almak, temel nedenleri ortadan kaldırmak, etkilenen sistemleri kurtarmak, gerektiğinde iletişim kurmak ve edinilen dersleri kaydetmek

Bu prosedürler, üretim ProcessMind bulut hizmeti için ve Hizmeti etkiledikleri ve ProcessMind'in makul ölçüde soruşturma ve yönetme yetkisi dahilinde

oldukları ölçüde alt işleyicileri veya bulut hizmetlerini içeren güvenlik olayları için geçerlidir. Geliştirme ve test ortamları birbirinden ayrıdır ve müşteriye yönelik üretim taahhütleri bakımından kurtarma hedefleri olarak değerlendirilmez.

---

2. Dayanıklılık Stratejisi

2.1 Bölgesel Tasarım. Üretim hizmetleri AWS EU'da (Frankfurt, Almanya, `eu-central-1`) barındırılır. Mimari, AWS'nin birden fazla Kullanılabilirlik Alanı genelinde işlettiği bu bölgedeki AWS tarafından yönetilen hizmetlere dayanır. Aurora kümesi şu anda tek bir yazıcı örneği çalıştırmaktadır; bu nedenle veritabanı kurtarması, bölge içi bir yedek sunucu yerine otomatik yedeklemelere ve belirli bir zamana kurtarmaya dayanır. ProcessMind şu anda müşteri verileri için ikinci bir etkin bölge işletmemektedir.

2.2 Yönetilen ve Sunucusuz Hizmetler. ProcessMind; AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS ve Amazon CloudWatch'a dayanır. Bu, müşteri tarafından yönetilen uzun ömürlü sunuculara bağımlılığı azaltır ve uygulama ile statik bileşenler için kaynaktan yeniden oluşturma yoluyla kurtarmayı destekler.

2.3 Ortamların Ayrılması. Üretim ve geliştirme ortamları ayrı AWS hesaplarında, ayrı veritabanları ve altyapı yığınlarıyla çalışır. Bu, geliştirme faaliyetlerinin üretim kurtarma operasyonlarını etkileme riskini azaltır.

2.4 İzleme ve Tespit. CloudWatch alarmları, panoları, ölü harf kuyruğu uyarıları, merkezi günlük kaydı ve sentetik hizmet izleme; olayların tespitini, önceliklendirilmesini ve üst makama aktarılmasını destekler. Olası olaylar ayrıca destek başvuruları, çalışan bildirimleri, tedarikçi bildirimleri veya diğer soruşturma tetikleyicileri aracılığıyla da belirlenebilir.

---

3. Kurtarma Öncelikleri

Büyük bir olay sırasında ProcessMind'in kurtarma öncelikleri genel olarak şunlardır:

1. Müşteri verilerinin bütünlüğünü korumak ve daha fazla zararı önlemek.
2. Olayı kontrol altına almak ve etkilenen sistemleri istikrara kavuşturmak.
3. Temel üretim erişim yollarını ve kritik iş akışlarını geri yüklemek.
4. Kurtarmanın tamamlandığını ilan etmeden önce hizmet davranışını, veri bütünlüğünü ve izlemeyi doğrulamak.
5. Durum güncellemelerini, müşteri etkisini ve takip eylemlerini iletmek.

Kesin sıra, olayın veri bütünlüğünü, müşteri erişimini, eşzamansız işlemeyi veya destekleyici altyapıyı etkileyip etkilemediği de dahil olmak üzere olayın niteliğine bağlı olarak değişebilir.

---

4. Felaket Kurtarma Prosedürleri

4.1 Olayın İlanı ve Koordinasyon. Önemli hizmet kesintileri ve güvenlik olayları, olaylara müdahale prosedürleri aracılığıyla önceliklendirilir. ProcessMind bir olay lideri belirler, müdahaleye katılımı yetkili personelle sınırlar, önem derecesini ve kapsamı değerlendirir, teknik müdahale ekiplerini koordine eder ve olay çözülene veya daha düşük bir seviyeye indirilene kadar kurtarma eylemlerini izler.

4.2 Kontrol Altına Alma. ProcessMind, daha kapsamlı kurtarma başlamadan önce devam eden etkiyi durdurmak veya azaltmak için ticari açıdan makul çabalar gösterir. Arıza türüne bağlı olarak kontrol altına alma eylemleri; son değişiklikleri geri almayı, etkilenen yolları devre dışı bırakmayı, arızalı bileşenleri izole etmeyi, bütünlük kontrolleri gerçekleştirilirken arka plan işlemeyi duraklatmayı, kimlik bilgilerini iptal etmeyi veya yenilemeyi ya da kötüye kullanım niteliğindeki faaliyetleri engellemeyi içerebilir.

4.3 Ortadan Kaldırma. Acil etki istikrara kavuşturulduktan sonra ProcessMind, temel nedeni veya katkıda bulunan koşulu ortadan kaldırmak için çalışır. Bu; kod veya yapılandırma düzeltmelerinin uygulanmasını, kötü amaçlı unsurların kaldırılmasını, gizli bilgilerin yenilenmesini, güvenilir yapılandırmanın geri yüklenmesini veya açık erişim yollarının kapatılmasını içerebilir.

4.4 Veritabanı Kurtarması. Aurora PostgreSQL, yedi (7) günlük saklama süresiyle sürekli otomatik yedeklemeler gerçekleştirir ve belirli bir zamana kurtarmayı destekler. Veritabanı düzeyinde bir arıza, bozulma olayı veya kazara gerçekleştirilen yıkıcı bir değişiklik geri yükleme gerektirirse ProcessMind, uygun en son yedekten veya seçilen bir zamandan geri yükleme yapabilir, geri yüklenen ortamı doğrulayabilir ve uygulama trafiğini kurtarılan veritabanı yoluna geri yönlendirebilir.

4.5 Nesne ve Yapıt Kurtarması. Müşteri dosyası yüklemeleri ve operasyonel yapıtlar Amazon S3'te saklanır. Yanlışlıkla silme veya üzerine yazma senaryolarından kurtarmayı desteklemek üzere yükleme klasöründe ve kaynak klasörlerinde sürüm oluşturma etkinleştirilmiştir. Web sitesi ve frontend dağıtım klasörleri yeniden üretilebilir yapıtlar olarak değerlendirilir ve yedeklerden geri yüklenmek yerine kaynaktan yeniden oluşturulabilir.

4.6 Eşzamansız İş Yükü Kurtarması. Eşzamansız işleme yolları, başarısız olayları soruşturma amacıyla saklamak için ölü harf kuyruklarını kullanır. Kurtarma; başarısız mesajların yeniden denenmesini, işleme mantığının yeniden çalıştırılmasını veya temel iş akışının güvenli yeniden işlemeyi desteklediği durumlarda işin yeniden oynatılmasını içerebilir.

4.7 Uygulama ve Altyapının Yeniden Oluşturulması. Altyapı, kaynak denetimli altyapı-kod tanımları aracılığıyla yönetilir. Uygulama altyapısının veya statik varlıkların yeniden oluşturulması gerekirse ProcessMind, etkilenen bileşenleri sürüm denetimli tanımlardan ve derleme yapıtlarından yeniden oluşturabilir ve yeniden dağıtabilir.

4.8 Hizmete Dönüşten Önce Doğrulama. Bir olay kapatılmadan önce ProcessMind, mevcut izleme, günlükler, sentetik kontroller ve hedefli işlevsel

doğrulama kullanarak hizmet sağlığını doğrular ve etkilenen işlevleri doğrulanmış dağıtım, kurtarma ve altyapı prosedürlerini kullanarak geri yükler. Olay veri geri yükleme veya veri bütünlüğü riski içeriyorsa ek inceleme yapılabilir.

---

5. İş Sürekliliği Önlemleri

5.1 Operasyonel Süreklilik. ProcessMind, kesintiye yol açan olaylar sırasında olayların ele alınmasının, müşteri destek başvurularının alınmasının, mühendislik müdahalesinin ve karar almanın devam edebilmesi için belgelenmiş operasyonel prosedürleri sürdürür.

5.2 İletişim. Önemli üretim olayları için ProcessMind, müşteri destek kanalları ve uygun olduğu durumlarda processmind.com/status adresindeki herkese açık durum sayfası aracılığıyla güncellemeler sağlamak için ticari açıdan makul çabalar gösterir.

5.3 Kontrollü Değişiklik Yönetimi. Önlenebilir kesintileri azaltmak ve zaman içinde sürekliliği iyileştirmek için birden fazla bağımsız otomatik doğrulama katmanı, kontrollü dağıtımlar, merkezi izleme ve olay sonrası inceleme içeren derinlemesine savunma yaklaşımına sahip bir yazılım geliştirme yaşam döngüsü kullanılır.

5.4 Kurtarma Sırasında Güvenlik. Kurtarma eylemleri, normal operasyonlar sırasında geçerli olan aynı genel güvenlik ilkelerine tabi olarak gerçekleştirilir; bunlara en az ayrıcalıkla erişim, mevcut olduğu ölçüde operasyonel faaliyetlerin günlüğe kaydedilmesi ve üretim sistemlerine ve verilerine kontrollü erişim dahildir.

---

6. Yedekleme ve Veri Koruma Özeti

6.1 Veritabanı Yedeklemeleri. Aurora otomatik yedeklemeleri şifrelenir ve yedi (7) gün boyunca saklanır; bu saklama süresi içinde belirli bir zamana kurtarma kullanılabilir.

6.2 S3 Protections. Amazon S3, depolanan nesneler için yüksek dayanıklılık sağlar. Değiştirilebilir müşteri verisi bucket'ları, birincil bölge içindeki dayanıklılığa ve sürüm oluşturmaya dayanır. ProcessMind şu anda bu bucket'lar için bölgeler arası S3 replikasyonunu etkinleştirmemektedir.

6.3 Logs and Diagnostics. Merkezi günlükler, alarmlar ve telemetri; arıza incelemesini ve kurtarma doğrulamasını destekler. Bu mekanizmalar süreklilik operasyonlarını destekler; ancak kendileri ayrı bir yedekleme ürünü olarak sunulmamaktadır.

---

7. Olayların Belirlenmesi ve Önceliklendirilmesi

7.1 Initial Assessment. Bildirilen olaylar; Security Incident tanımını karşılayıp karşılamadıklarını, hangi sistemlerin veya verilerin etkilenmiş olabileceğini, muhtemel kapsamı ve ciddiyeti ve derhâl sınırlama gerekip gerekmediğini belirlemek üzere önceliklendirilir. Kanıtların korunması, olayın ve ilgili sistemlerin niteliğine uygun şekilde gerçekleştirilir.

7.2 On-Call and Escalation. ProcessMind, üretim olayları için nöbetçi kapsamı sağlar; buna, Critical olaylar için (Service Level Agreement'ta tanımlandığı üzere) 7/24 kapsam da dahildir; böylece olaylar her zaman kabul edilip önceliklendirilebilir.

7.3 Documentation. ProcessMind, olay zaman çizelgesinin ve bunun sonucunda alınan düzeltici önlemlerin olay sonrasında incelenebilmesi için önemli inceleme bulgularını, müdahale faaliyetlerini ve kurtarma kararlarını belgeler.

---

8. İletişim ve Bildirim

8.1 Internal Communication. ProcessMind, teknik müdahale ile müşteri iletişiminin olayın tüm yaşam döngüsü boyunca uyumlu kalması için müdahale ekiplerini, karar vericileri ve destek kanallarını koordine eder.

8.2 Customer Notification. DPA veya yürürlükteki hukuk uyarınca bildirim gerektiren bir Security Incident meydana gelmesi hâlinde ProcessMind, etkilenen müşterileri gereksiz gecikme olmaksızın ve mümkün olduğu durumlarda olaydan haberdar olmasından itibaren yetmiş iki (72) saat içinde bilgilendirir. Bildirimler genel olarak olayın niteliğini ve kapsamını, biliniyorsa etkilenen veri kategorilerini, olayı sınırlamak ve gidermek için alınan önlemleri ve ilgili olduğu durumlarda müşterilere önerilen eylemleri içerir.

8.3 Ongoing Updates. Olay devam ediyorsa veya önemli olgular değişiyorsa ProcessMind, doğrulanmış ek bilgiler elde edildikçe takip güncellemeleri sağlar. Daha geniş kapsamlı üretim hizmeti kesintileri için ProcessMind ayrıca müşteri destek kanallarını ve uygun olduğu durumlarda processmind.com/status adresindeki herkese açık durum sayfasını kullanabilir.

---

9. Test, İnceleme ve Bakım

ProcessMind, bu prosedürleri en az yılda bir kez ve önemli olaylardan veya önemli mimari değişikliklerden sonra gözden geçirir; müdahale ve kurtarma yaklaşımının ilgili unsurlarını (yedeklerin geri yüklenmesi, dağıtımın yeniden oluşturulması, izleme, uyarı ve olay iletişimi gibi) periyodik olarak uygular ve edinilen dersleri güvenlik, güvenilirlik ve süreklilik prosedürlerine dâhil eder.

---

10. Sınırlamalar ve Sözleşmesel Sınırlar

Bu belge, üst düzey bir özettir ve her bir dahili runbook'u, eskalasyon yolunu, inceleme yöntemini veya kanıtların işlenmesine ilişkin adımı operasyonel ayrıntılarıyla açıklamaz. Belge, yürürlükteki sözleşmede veya siparişte açıkça belirtilenlerin ötesinde ProcessMind'ı ayrı bir bölgeler arası yük devretme tasarımına, tüm değiştirilebilir bucket'lar için değiştirilemez

depolama saklama süresine veya bağımsız RTO/RPO garantilerine bağlamaz.

Bu belge ile yürürlükteki Customer Agreement, Data Processing Addendum, Service Level Agreement veya emredici hukuk arasında herhangi bir çelişki olması hâlinde, söz konusu kaynaklar geçerli olur.