

Bezpečnostní opatření ProcessMind

Datum účinnosti: 14. září 2026

Tento dokument popisuje technická a organizační opatření („TOM“), která společnost ProcessMind B.V. udržuje za účelem ochrany důvěrnosti, integrity a dostupnosti zákaznických dat. ProcessMind uplatňuje přístup vícevrstvé ochrany, v jehož rámci zákaznická data na každé úrovni chrání několik nezávislých bezpečnostních vrstev – od sítě a infrastruktury přes identitu, autorizaci, izolaci dat, šifrování a monitorování až po vývoj softwaru. Tato opatření doplňují [Dodatek o zpracování údajů](#), [Zásady ochrany osobních údajů](#) a [Zásady hostingu SaaS](#). ProcessMind tato opatření přezkoumává a aktualizuje nejméně jednou ročně.

Zákaznická data se nikdy neprodávají třetím stranám, nesdílejí se s nimi ani je třetí strany nepoužívají pro vlastní účely.

1. Zabezpečení infrastruktury

1.1 Cloudová platforma. ProcessMind je hostován výhradně na Amazon Web Services (AWS) v EU (Frankfurt, Německo, eu-central-1). AWS má certifikace ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 a PCI DSS. Úplný seznam naleznete v [programech shody AWS](#).

1.2 Bezserverová architektura. Aplikační logika ProcessMind běží na AWS Lambda a službách spravovaných AWS. ProcessMind neprovozuje dlouhodobě běžící aplikační servery spravované zákazníkem, čímž odpadá značná část práce spojené s instalací oprav operačního systému a zabezpečením serverů.

1.3 Hranice sítě. ProcessMind udržuje AWS VPC pro databázové a síťové kontroly. Aurora PostgreSQL běží v privátních podsítích bez odchozího přístupu k internetu, není veřejně přístupná a jsou povoleny protokoly toku VPC. ProcessMind ve výchozím nastavení neumísťuje aplikační funkce

Lambda do VPC. Funkce Lambda přistupují k Aurora prostřednictvím AWS RDS Data API přes TLS s ověřováním pomocí IAM a Secrets Manager.

1.4 Doručování obsahu a řízení na okraji sítě. Webové stránky určené zákazníkům, frontendová SPA a provoz veřejných zdrojů jsou obsluhovány prostřednictvím Amazon CloudFront. Všechny distribuce CloudFront vynucují minimální zásady TLS ve verzi TLS 1.2 (2021). Distribuce webových stránek a frontendové SPA navíc přidávají bezpečnostní hlavičky odpovědí, včetně HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, zásad pro předávání informací o odkazujícím zdroji a zásad oprávnění. Distribuce veřejných zdrojů používá CloudFront Origin Access Control, aby zdrojový bucket zůstal soukromý. Provoz API určený zákazníkům je zpracováván samostatně prostřednictvím Amazon API Gateway: provoz požadavků a odpovědí HTTPS je obsluhován prostřednictvím HTTP API na vyhrazené subdoméně API a připojení klientů v reálném čase jsou obsluhována prostřednictvím samostatného WebSocket API služby API Gateway na vyhrazené subdoméně WebSocket.

1.5 Oddělení prostředí. Produkční a vývojová prostředí používají samostatné účty AWS, samostatné databáze a samostatné zásobníky infrastruktury. Přihlašovací údaje vývojářů neumožňují přístup k produkčním zákaznickým datům.

2. Šifrování dat

2.1 Šifrování při přenosu. Veškerá data přenášená mezi klienty a službami ProcessMind jsou šifrována pomocí TLS 1.2 nebo vyšší verze. Koncové body určené zákazníkům jsou zpřístupněny prostřednictvím HTTPS. Buckety S3, témata SNS a fronty SQS vytvořené přímo společností ProcessMind vynucují přístup pouze přes SSL. Přístup k databázi prostřednictvím RDS Data API a další volání služeb AWS používají HTTPS/TLS.

2.2 Šifrování uložených dat. Aurora PostgreSQL je šifrována v klidovém stavu pomocí klíčů AWS KMS spravovaných zákazníkem s automatickou

rotací klíčů. Buckety S3 pro zákaznická data a provozní účely vytvořené přímo společností ProcessMind, včetně bucketů pro nahrané soubory, zdroje a protokoly přístupu, používají klíče KMS spravované zákazníkem. Skupiny protokolů CloudWatch, témata SNS a fronty SQS vytvořené přímo společností ProcessMind rovněž používají klíče KMS spravované zákazníkem. Zdrojové buckety webových stránek a frontendu spravované SST používají šifrování na straně serveru S3 spravované AWS (SSE-S3 / AES-256), nikoli klíče KMS spravované zákazníkem.

2.3 Správa klíčů a tajných údajů. Šifrovací klíče databáze jsou spravovány centrálně prostřednictvím AWS KMS a přístup ke klíčům se řídí zásadami IAM založenými na principu nejnižších oprávnění. Přihlašovací údaje k databázi jsou uloženy v AWS Secrets Manager. Hlavní tajný údaj Aurora a tajný údaj pro omezeného aplikačního uživatele se automaticky obměňují každých třicet (30) dní. Produkční klíče a tajné údaje se nikdy neukládají do zdrojového kódu; přihlašovací údaje určené pouze pro vývoj jsou odděleny od produkčního prostředí. Některé podpůrné prostředky spravované AWS/CDK/SST nadále používají šifrování spravované AWS, pokud služba nebo framework neumožňuje konfiguraci klíčů spravovaných zákazníkem.

3. Izolace a umístění dat

3.1 Izolace tenantů. Každý zákaznický tenant má vyhrazenou izolovanou instanci databáze. Zákaznická data se na úrovni databáze nikdy neslučují s daty jiných zákazníků. Sdílená metadata (např. záznamy účtů, fakturace a mapování uživatelů na tenanty) jsou uložena v samostatné databázi pro více tenantů s přísným řízením přístupu. Sdílené tabulky s rozsahem tenantů a organizací jsou navíc chráněny zásadami zabezpečení na úrovni řádků PostgreSQL (RLS), které se vynucují prostřednictvím kontextu databáze vymezeného pro jednotlivé požadavky.

3.2 Umístění dat. Veškerá zákaznická data, včetně databází, nahraných souborů, záloh a výsledků dotazů, jsou ukládána výhradně v EU (Frankfurt, Německo). Pokud je pro konkrétní činnost zpracování využíván dílčí

zpracovatel se sídlem mimo EHP (například pro zpracování modelů AI nebo zpracování plateb), je předání pokryto příslušným mechanismem předávání, jak je popsáno v Dodatku o zpracování údajů, a dílčí zpracovatel i místo zpracování jsou uvedeny v Seznamu dílčích zpracovatelů.

3.3 Uchovávání a výmaz dat. Lhůty uchovávání a výmazu jsou stanoveny v oddílu 6 [Dodatku o zpracování údajů](#). Zákazníci mohou svá data kdykoli vymazat prostřednictvím aplikace nebo kontaktováním společnosti ProcessMind. Záložní kopie se odstraňují po uplynutí příslušných lhůt uchovávání záloh (oddíl 7.1).

4. Správa identit a přístupu

4.1 Ověřování. ProcessMind podporuje jednotné přihlašování (SSO) prostřednictvím Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC a LinkedIn OAuth 2.0/OIDC. ProcessMind vystupuje jako spoléhající se strana a neukládá hesla uživatelů. Vícefaktorové ověřování vynucuje poskytovatel identity — například pokud organizace propojí Microsoft Entra ID (Azure AD), uplatní se vlastní zásady MFA a přístupu této organizace.

4.2 Správa relací. Relace prohlížeče používají podepsané JSON Web Tokens (JWT), které se přenášejí prostřednictvím zabezpečených souborů cookie HttpOnly s příznaky SameSite a Secure. Podpisy tokenů se ověřují při každém ověřeném požadavku.

4.3 Model autorizace. ProcessMind u svých základních aplikačních API nespolehá na nativní autorizátory API Gateway. Autorizace je vynucována ve sdílených obalech obslužných funkcí Lambda, které před spuštěním obchodní logiky ověřují stav relace a rozsah tenanta. Veřejné trasy jsou výslovně povoleny pro neověřené toky, webhooky, příjem událostí a předběžné požadavky CORS. Externí koncové body API používají vyhrazené obslužné funkce ověřování. Přístup k zákaznickým datům je omezen na kontext ověřeného tenanta nebo organizace.

4.4 Nejnižší oprávnění. Interní systémy se řídí zásadou nejnižších oprávnění. Role IAM jsou omezeny na minimum potřebných prostředků, pokud framework umožňuje přesné vymezení rozsahu. Některé role generované SST/CDK používají širší spravované nebo vložené zásady pro vazby a provoz za běhu; tyto případy se přezkoumávají, jejich rozsah se podle možností omezuje na konkrétní prostředky a evidují se jako výslovné výjimky.

4.5 Řízení přístupu zaměstnanců. Přístup zaměstnanců k interním systémům se spravuje prostřednictvím Active Directory s jednotným přihlašováním a povinným MFA. Řízení přístupu na základě rolí (RBAC) zajišťuje, že přístup k zákaznickým datům mají pouze oprávněné osoby, které jej potřebují znát. Přístupová práva se pravidelně přezkoumávají.

5. Protokolování, monitorování a audit

5.1 Centralizované protokolování. Protokolování přístupu k HTTP API a WebSocket je povoleno se strukturovanými poli JSON a záznamy se ukládají do Amazon CloudWatch Logs s dobou uchovávání jeden (1) rok. Tyto skupiny protokolů přístupu jsou šifrovány klíčem AWS KMS spravovaným zákazníkem. Protokoly aplikace se centralizují ve skupinách protokolů Amazon CloudWatch šifrovaných klíčem AWS KMS spravovaným zákazníkem a uchovávají se po dobu deseti (10) let. Samostatné skupiny protokolů auditu a telemetrie jsou rovněž šifrovány klíčem AWS KMS spravovaným zákazníkem a uchovávají se po dobu deseti (10) let. Skupina pro export protokolů databázového stroje Aurora PostgreSQL se uchovává po dobu jednoho (1) týdne.

5.2 Co se zaznamenává a co nikoli. ProcessMind zaznamenává události přístupu k HTTP API a WebSocket — čas požadavku, identifikátory požadavku, trasu nebo cestu, stav odpovědi a latenci. Protokoly přístupu neobsahují zdrojovou IP adresu volajícího ani jeho uživatelského agenta. ProcessMind také zaznamenává události ověřování, cesty asynchronních selhání a podpůrnou činnost aplikace Lambda do centralizovaných skupin

protokolů CloudWatch. Protokoly toku VPC jsou povoleny. ProcessMind v současnosti nepovoluje standardní protokolování přístupu CloudFront u distribucí webových stránek, frontendové SPA ani veřejných zdrojů.

5.3 Monitorování a upozorňování. Alarmy a dashboardy CloudWatch monitorují stav systému, fronty nedoručených zpráv a selhání relevantní z hlediska bezpečnosti. Selhání asynchronního zpracování se směřují do šifrovaných front nedoručených zpráv (doba uchovávání čtrnáct (14) dní; u front miniatur a vyhledávacího indexu dva (2) dny) a alarmy DLQ spouštějí oznámení SNS za účelem prošetření. ProcessMind navíc používá Sentry ke sledování chyb frontendu v reálném čase, monitorování výkonu a přehrávání relací. Záznamy relací se pořizují pouze u relací, při nichž dojde k chybě, a text, vstupy formulářů a média jsou v záznamech maskovány nebo blokovány. Data Sentry se přijímají v EU (Frankfurt) a omezují se na údaje o používání ProcessMind (chyby prohlížeče, záznamy výkonu, metadata zařízení a maskované záznamy přehrávání). Sentry je uvedeno v [seznamu dílčích zpracovatelů](#).

5.4 Ochrana protokolů. Protokoly se ukládají do vyhrazených skupin protokolů CloudWatch s řízeným přístupem a jsou šifrovány v klidovém stavu. Produkční a vývojové protokoly jsou odděleny podle prostředí a hranic účtů.

6. Automatizované ověřování kontrol a správa zranitelností

6.1 Činnost ProcessMind. ProcessMind spouští cdk-nag v rámci syntézy infrastruktury a workflow nasazení s využitím několika sad pravidel pro dané odvětví (včetně AWS Solutions, NIST 800-53 a PCI DSS). Pro každý zásobník se vytvářejí zprávy, které se přezkoumávají v rámci řízení změn infrastruktury. Zjištění se třídí jako opravená, přijaté riziko nebo plánované zlepšení.

6.2 Správa výjimek. Potlačení zjištění se zaznamenávají v centrálním registru, pokud to framework umožňuje, jejich rozsah se omezuje na dotčené zásobníky a vyžadují písemné odůvodnění; pokud zásobník

obsahuje vložené potlačení, je zdokumentováno u daného zásobníku. Po nápravě zjištění se příslušné potlačení aktualizuje nebo odstraní. ProcessMind nepovažuje potlačení za plošné vyjmutí z přezkumu.

6.3 Činnosti, které ProcessMind v současnosti neprovádí. ProcessMind eviduje a přezkoumává podstatné výjimky z kontrol infrastruktury. Mezi hlavní patří:

- aplikační funkce Lambda nejsou ve výchozím nastavení umístěny ve VPC; k Aurora přistupují prostřednictvím RDS Data API přes TLS s ověřováním pomocí IAM a Secrets Manager
- žádná část služby není chráněna AWS WAF: AWS WAF nepodporuje HTTP API služby API Gateway a ani zbývající vstupní body nejsou chráněny WAF (připojení WebSocket používají krátkodobé tokeny HMAC; geografická omezení související s platbami jsou vynucována v platebním systému); statické distribuce také nemají standardní protokolování přístupu CloudFront
- obnova databáze se opírá o automatické zálohy Aurora a obnovu k určitému okamžiku, nikoli o samostatný plán AWS Backup nebo Aurora Enhanced Monitoring
- neexistuje replikace S3 mezi regiony ani S3 Object Lock pro měnitelné buckety
- některé podpůrné zdroje spravované AWS/CDK/SST používají šifrování spravované AWS nebo širší automaticky generované zásady IAM, pokud služba nenabízí alternativu pod kontrolou zákazníka

Úplný registr potlačení se udržuje společně s kódem infrastruktury a je k dispozici na vyžádání. Použití sad pravidel `cdk-nag` představuje technické ověřování kontrol, nikoli externí certifikaci, auditorský výrok ani právní atestaci shody s HIPAA, NIST nebo PCI DSS.

6.4 Správa závislostí. Softwarové závislosti jsou průběžně monitorovány z hlediska známých zranitelností. Kritické zranitelnosti a zranitelnosti s

vysokou závažností se opravují s cílovou lhůtou sedmi (7) dnů. Závislosti se aktualizují v pravidelných intervalech.

6.5 Životní cyklus bezpečného vývoje softwaru (SDLC). ProcessMind uplatňuje při vývoji softwaru přístup vícevrstvé ochrany. Každá změna produkčního prostředí musí před nasazením projít několika nezávislými vrstvami automatizovaného ověřování:

- **Statická analýza a typová bezpečnost:** Přísný režim TypeScriptu a ESLint při kompilaci vynucují správnost typů, bezpečnost při práci s hodnotami null a bezpečnostně relevantní vzorce kódování.
- **Kontrola kódu s podporou AI:** Analýza s podporou AI poskytuje při kontrole požadavků na začlenění další pohled, který pomáhá odhalovat bezpečnostní rizika, logické chyby a odchylky od konvencí, a doplňuje tak automatizované testování.
- **Jednotkové a integrační testy:** Komplexní sada testů Vitest ověřuje obchodní logiku, vzorce přístupu k datům, chování API a zpracování chyb vůči aktivním prostředkům AWS ve vývojovém prostředí.
- **Testy od začátku do konce:** Testy prohlížeče založené na Playwright ověřují kritické workflow uživatelů, včetně ověřování, nahrávání dat, modelování procesů, simulace a izolace více tenantů.
- **Skenování shody infrastruktury:** cdk-nag při každé změně ověřuje infrastrukturu jako kód podle několika rámců shody.
- **Skenování zranitelností závislostí:** Automatizované audit y závislostí bloku jí nasazení známých kritických zranitelností a zranitelností s vysokou závažností do produkčního prostředí.

Lidská kontrola se zaměřuje na architekturu, bezpečnostní hranice a rozhodnutí na úrovni návrhu, nikoli na kontrolu jednotlivých řádků kódu. U strukturálních změn, změn citlivých z hlediska bezpečnosti nebo změn infrastruktury je kromě automatizovaného ověřování vyžadováno výslovné schválení člověkem.

Všechny vrstvy ověřování se vynucují prostřednictvím CI jako povinné podmínky sloučení změn aplikace a infrastruktury do hlavní větve. Obsah

webových stránek a vydávání statických prostředků se řídí samostatným zdokumentovaným procesem vydávání s kontrolami při nasazení — včetně automatizované kontroly aktuálnosti právních dokumentů — nikoli kontrolní podmínkou CI aplikace. Nouzové opravy produkčního prostředí mohou obejít kontrolní podmínku CI, musí však do dvaceti čtyř (24) hodin následovat úplné spuštění pipeline a přezkum po incidentu.

7. Zálohování a obnova po havárii

7.1 Automatické zálohy. Amazon Aurora provádí průběžné automatické zálohování s dobou uchovávání sedm (7) dní. Zálohy jsou šifrovány pomocí stejných klíčů KMS spravovaných zákazníkem jako zdrojové databáze.

7.2 Obnova k určitému okamžiku. Aurora podporuje obnovu k určitému okamžiku na libovolnou sekundu v rámci doby uchovávání záloh, což umožňuje rychlou obnovu v případě poškození dat nebo jejich neúmyslného odstranění.

7.3 Odolnost a verzování S3. Nahrané soubory a provozní artefakty se ukládají v Amazon S3, který poskytuje odolnost 99,999999999 % (11 devítek). Ve bucketu pro nahrané soubory a bucketech zdrojů je povoleno verzování, které podporuje obnovu a návrat k předchozím verzím. Buckety pro nasazení webových stránek a frontendu obsahují reprodukovatelné artefakty sestavení a nepovažují se za zálohovací systém. ProcessMind v současnosti nepovoluje replikaci S3 mezi regiony.

7.4 Kontinuita podnikání. Postupy obnovy po havárii jsou zdokumentovány a pravidelně testovány. Souhrn je k dispozici v dokumentu [Obnova po havárii, kontinuita podnikání a reakce na incidenty](#). Architektura využívá spravované služby AWS v rámci regionu eu-central-1, který AWS provozuje napříč několika zónami dostupnosti; cluster Aurora v současnosti používá jedinou instanci zapisovače, takže obnova databáze se opírá o automatické zálohy a obnovu k určitému okamžiku, nikoli o záložní instanci v rámci regionu. Zálohy Aurora, odolnost S3, fronty nedoručených zpráv a

statické prostředky obnovitelné ze zdrojového kódu jsou součástí strategie obnovy.

8. Reakce na incidenty

8.1 Oznámení incidentu. V případě bezpečnostního incidentu (jak je definován v DPA) ProcessMind bez zbytečného odkladu a, je-li to proveditelné, do sedmdesáti dvou (72) hodin od okamžiku, kdy se o incidentu dozví, vyrozumí dotčené zákazníky.

8.2 Řešení incidentů. ProcessMind udržuje zdokumentované postupy reakce na incidenty, které zahrnují identifikaci, omezení dopadů, odstranění příčiny, obnovu a přezkum po incidentu. Souhrn je k dispozici v dokumentu [Obnova po havárii, kontinuita podnikání a reakce na incidenty](#). Získané poznatky z incidentů se promítají do bezpečnostních kontrol a procesů.

8.3 Komunikace. Oznámení incidentu obsahují povahu a rozsah incidentu, dotčené kategorie údajů, opatření přijatá k omezení dopadů incidentu a doporučené kroky pro zákazníka.

9. Organizační opatření

9.1. Řízení bezpečnosti informací. ProcessMind udržuje systém řízení bezpečnosti informací v souladu se zásadami normy ISO 27001. ProcessMind si zvolil postup vedoucí k certifikaci podle ISO 27001 a atestaci SOC 2 Type II; formální certifikační proces zatím nebyl zahájen.

9.2 Povědomí o bezpečnosti. Veškerý personál s přístupem k zákaznickým datům absolvuje školení zaměřené na bezpečnost. Osvědčené bezpečnostní postupy jsou začleněny do zaškolování, workflow vývoje a provozních postupů.

9.3 Správa dodavatelů a dílčích zpracovatelů. Dílčí zpracovatelé jsou smluvně zavázáni dodržovat standardy ochrany údajů rovnocenné standardům popsáným v tomto dokumentu. ProcessMind udržuje veřejný

[seznam dílčích zpracovatelů](#) a před zapojením nového dílčího zpracovatele poskytuje oznámení nejméně třicet (30) dní předem. Dílčí zpracovatelé jsou každoročně přezkoumáváni z hlediska shody.

9.4 Důvěrnost. Veškerý personál oprávněný zpracovávat zákaznická data je vázán písemnými povinnostmi mlčenlivosti.

10. Shoda a certifikace

Rámec / standard	Stav
GDPR (obecné nařízení EU o ochraně osobních údajů)	V souladu
Umístění dat v EU (Frankfurt, Německo)	Vynucováno
Certifikace infrastruktury AWS (ISO 27001, SOC 2, PCI DSS)	Převzato prostřednictvím AWS
ISO 27001 (ProcessMind)	Plánováno – postup k certifikaci zvolen; formální proces dosud nebyl zahájen
SOC 2 Type II (ProcessMind)	Plánováno – postup k certifikaci zvolen; formální proces dosud nebyl zahájen
Automatizované ověřování kontrol infrastruktury (cdk-nag napříč AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Zavedeno jako technické ověřování kontrol, nikoli jako certifikace
Standardní smluvní doložky (SCC) pro mezinárodní předávání	Zavedeno (viz DPA)
Dodatek o zpracování údajů (DPA)	Veřejně dostupný

Použití sad pravidel cdk-nag neznamená, že je ProcessMind formálně certifikován nebo nezávisle auditován podle HIPAA, NIST nebo PCI DSS. Tyto sady pravidel se používají jako technické ochranné prvky k ověřování návrhu infrastruktury a výslovnému sledování nedostatků.

V případě dotazů týkajících se bezpečnosti nebo shody, případně chcete-li požádat o dokumentaci, například auditorské zprávy nebo vyplněné bezpečnostní dotazníky, kontaktujte support@processmind.com.