

A ProcessMind biztonsági intézkedései

Hatálybalépés dátuma: 2026. szeptember 14.

Ez a dokumentum ismerteti azokat a műszaki és szervezési intézkedéseket („TOM-ok”), amelyeket a ProcessMind B.V. az ügyfeladatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme érdekében alkalmaz. A ProcessMind többrétegű védekezési megközelítést követ, amelyben több, egymástól független biztonsági réteg védi az ügyfeladatokat minden szinten – a hálózattól és az infrastruktúrától kezdve az identitáskezelésen, a jogosultságkezelésen, az adatok elkülönítésén, a titkosításon és a felügyeleten át a szoftverfejlesztésig. Ezek az intézkedések kiegészítik az [Adatfeldolgozási kiegészítést](#), az [Adatvédelmi tájékoztatót](#) és a [SaaS-tárhelyszolgáltatási szabályzatot](#). A ProcessMind legalább évente felülvizsgálja és frissíti ezeket az intézkedéseket.

Az ügyfeladatokat soha nem értékesítjük harmadik feleknek, nem osztjuk meg velük, és nem használjuk fel harmadik felek saját céljaira.

1. Infrastruktúra-biztonság

1.1 Felhőplatform. A ProcessMind kizárólag az Európai Unióban (Frankfurt, Németország, eu-central-1) található Amazon Web Services (AWS) infrastruktúrán van üzemeltetve. Az AWS ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 és PCI DSS tanúsítványokkal rendelkezik. A teljes listát az [AWS megfelelési programjai](#) oldalon találja.

1.2 Szerver nélküli architektúra. A ProcessMind alkalmazáslogikája AWS Lambda és AWS által felügyelt szolgáltatások használatával fut. A ProcessMind nem üzemeltet ügyfél által kezelt, hosszú élettartamú alkalmazásszervereket, így elmarad az operációs rendszerek javításával és a szerverek megerősítésével kapcsolatos feladatok jelentős része.

1.3 Hálózati határok. A ProcessMind adatbázis- és hálózati kontrollok céljára AWS VPC-t tart fenn. Az Aurora PostgreSQL privát alhálózatokban

fut, internetes kimenő forgalom nélkül, nyilvánosan nem érhető el, és engedélyezve vannak a VPC-forgalmi naplók. A ProcessMind alapértelmezés szerint nem helyezi az alkalmazás Lambda-függvényeit a VPC-be. A Lambda-függvények az AWS RDS Data API-n keresztül, TLS használatával, IAM- és Secrets Manager-hitelesítéssel érik el az Aurorát.

1.4 Tartalomszolgáltatás és peremhálózati vezérlők. Az ügyfelek számára elérhető webhely, frontend SPA és nyilvános erőforrások forgalmát az Amazon CloudFront szolgálja ki. Valamennyi CloudFront-disztribúció legalább TLS 1.2 (2021) verziójú TLS-házirendet ír elő. A webhely és a frontend SPA disztribúciói emellett biztonsági válaszfelvételeket is hozzáadnak, többek között HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), frame-ancestors 'none', X-Frame-Options: DENY, X-Content-Type-Options, hivatkozásházirend és engedélyezési házirend felvételeket. A nyilvános erőforrások disztribúciója a CloudFront Origin Access Control használatával biztosítja, hogy az eredeti tároló privát maradjon. Az ügyfelek számára elérhető API-forgalmat külön kezeli az Amazon API Gateway: a HTTPS-kérés-/válaszforgalmat egy dedikált API-aldomainen működő HTTP API szolgálja ki, a valós idejű klienskapcsolatokat pedig egy külön API Gateway WebSocket API szolgálja ki egy dedikált WebSocket-aldomainen.

1.5 Környezetek elkülönítése. Az éles és a fejlesztői környezet külön AWS-fiókokat, külön adatbázisokat és külön infrastruktúra-veremeket használ. A fejlesztői hitelesítő adatok nem biztosítanak hozzáférést az éles ügyféladatokhoz.

2. Adattitkosítás

2.1 Titkosítás továbbítás közben. Az ügyfelek és a ProcessMind szolgáltatásai között továbbított összes adat TLS 1.2 vagy újabb verzió használatával titkosított. Az ügyfelek számára elérhető végpontok HTTPS-en keresztül érhetők el. A közvetlenül a ProcessMind által létrehozott S3-tárolók, SNS-témák és SQS-sorok kizárólag SSL-en keresztüli hozzáférést

tesznek lehetővé. Az adatbázis-hozzáférés az RDS Data API-n keresztül, valamint az AWS-szolgáltatások egyéb hívásai HTTPS/TLS használatával történnek.

2.2 Titkosítás tárolás közben. Az Aurora PostgreSQL tárolás közben, ügyfél által kezelt AWS KMS-kulcsokkal van titkosítva, automatikus kulcsrotációval. A közvetlenül a ProcessMind által létrehozott, ügyféladatokat és működési adatokat tároló S3-tárolók – beleértve a feltöltések, az erőforrások és a hozzáférési naplók tárolóit – ügyfél által kezelt KMS-kulcsokat használnak. A közvetlenül a ProcessMind által létrehozott CloudWatch-naplócsoportok, SNS-témák és SQS-sorok szintén ügyfél által kezelt KMS-kulcsokat használnak. Az SST által kezelt webhely- és frontendforrás-tárolók ügyfél által kezelt KMS-kulcsok helyett AWS által kezelt S3 szerveroldali titkosítást (SSE-S3 / AES-256) használnak.

2.3 Kulcskezelés és titkok. Az adatbázis-titkosítási kulcsokat központilag, az AWS KMS-en keresztül kezeljük, a kulcsokhoz való hozzáférést pedig a legkisebb jogosultság elvét követő IAM-szabályzatok szabályozzák. Az adatbázis hitelesítő adatait az AWS Secrets Manager tárolja. Az Aurora főtitka és a korlátozott jogosultságú alkalmazásfelhasználói titok harminc (30) naponta automatikusan rotálódik. Az éles kulcsokat és titkokat soha nem tároljuk forráskódban; a kizárólag fejlesztésre használt hitelesítő adatok el vannak különítve az éles környezettől. Egyes AWS/CDK/SST által kezelt támogató erőforrások továbbra is AWS által kezelt titkosítást használnak, ha a szolgáltatás vagy a keretrendszer nem teszi lehetővé az ügyfél által kezelt kulcsok beállítását.

3. Adatok elkülönítése és tárolási helye

3.1 Bérlok elkülönítése. Minden ügyfélbérlo dedikált, elkülönített adatbázis-példányt kap. Az ügyféladatokat adatbázisszinten soha nem keverjük össze más ügyfelek adataival. A megosztott metaadatokat (például a fiókadatokat, a számlázási adatokat és a felhasználók bérlokhöz rendelését) külön, több bérlo által használt adatbázisban tároljuk, szigorú

hozzáférés-vezérlés mellett. A bérlőhöz és szervezethez kötött megosztott táblákat emellett a PostgreSQL sorszintű biztonsági (RLS) szabályzatai védik, amelyeket a kérésekhez kötött adatbázis-kontextus érvényesít.

3.2 Adatok tárolási helye. Minden ügyféladatot – beleértve az adatbázisokat, a fájlfeltöltéseket, a biztonsági mentéseket és a lekérdezési eredményeket – kizárólag az Európai Unióban (Frankfurt, Németország) tárolunk. Ha egy konkrét adatkezelési tevékenységhez az EGT-n kívül található adatfeldolgozót veszünk igénybe (például AI-modell feldolgozásához vagy fizetésfeldolgozáshoz), az adattovábbításra az Adatfeldolgozási kiegészítésben ismertetett megfelelő adattovábbítási mechanizmus vonatkozik, az adatfeldolgozó és az adatkezelés helye pedig szerepel az Adatfeldolgozók listáján.

3.3 Adatmegőrzés és törlés. Az adatmegőrzési és törlési határidőket az [Adatfeldolgozási kiegészítés](#) 6. szakasza határozza meg. Az ügyfelek bármikor törölhetik adataikat az alkalmazáson keresztül vagy a ProcessMind megkeresésével. A biztonsági mentések másolatait a vonatkozó biztonsági mentési megőrzési időszak lejártakor távolítjuk el (7.1. szakasz).

4. Identitás- és hozzáférés-kezelés

4.1 Hitelesítés. A ProcessMind támogatja az egyszeri bejelentkezést (SSO) a Microsoft Entra ID (Azure AD), a Google OAuth 2.0/OIDC és a LinkedIn OAuth 2.0/OIDC használatával. A ProcessMind megbízó félként jár el, és nem tárol felhasználói jelszavakat. A többtényezős hitelesítést az identitásszolgáltató írja elő – például ha egy szervezet csatlakoztatja a Microsoft Entra ID-t (Azure AD), az adott szervezet saját MFA- és hozzáférési szabályzatai érvényesek.

4.2 Munkamenet-kezelés. A böngésző-munkamenetek aláírt JSON Web Tokeneket (JWT) használnak, amelyeket biztonságos, HttpOnly cookie-k továbbítanak SameSite és Secure jelölőkkel. A tokenek aláírását minden hitelesített kérésnél ellenőrizzük.

4.3 Engedélyezési modell. A ProcessMind az alapvető alkalmazás-API-k esetében nem támaszkodik az API Gateway natív engedélyezőire. Az engedélyezést megosztott Lambda-kezelőburkolók érvényesítik, amelyek az üzleti logika futtatása előtt ellenőrzik a munkamenet állapotát és a bérlői hatókört. A nyilvános útvonalak kifejezetten engedélyezőlistán szerepelnek a nem hitelesített folyamatok, webhookok, eseményfogadás és CORS-előzetes kérések számára. A külső API-végpontok dedikált hitelesítési kezelőket használnak. Az Ügyféladatokhoz való hozzáférés a hitelesített bérlő vagy szervezet kontextusára korlátozódik.

4.4 A legkisebb jogosultság elve. A belső rendszerek a legkisebb jogosultság elvét követik. Ahol a keretrendszer lehetővé teszi a pontos hatókör-meghatározást, az IAM-szerepkörök a szükséges minimális erőforrásokra korlátozódnak. Egyes, az SST/CDK által létrehozott szerepkörök a kötési és futásidejű működéshez szélesebb körű, felügyelt vagy beágyazott szabályzatokat használnak; ezeket az eseteket felülvizsgáljuk, ahol lehetséges, erőforrásokra korlátozzuk, és kifejezett kivételként nyilvántartjuk.

4.5 Munkavállalói hozzáférés-vezérlés. A munkavállalók belső rendszerekhez való hozzáférését Active Directory kezeli SSO-val és kötelező MFA-val. A szerepköralapú hozzáférés-vezérlés (RBAC) biztosítja, hogy az ügyféladatokhoz csak a jogosult személyek férhessenek hozzá, kizárólag a feladataik ellátásához szükséges mértékben. A hozzáférési jogosultságokat rendszeresen felülvizsgáljuk.

5. Naplózás, felügyelet és audit

5.1 Központosított naplózás. A HTTP API-hozzáférések és a WebSocket-hozzáférések naplózása strukturált JSON-mezőkkel engedélyezett; a naplókat egy (1) éves megőrzési idővel az Amazon CloudWatch Logs szolgáltatásba írjuk. Ezeket a hozzáférési naplócsoportokat ügyfél által kezelt AWS KMS-kulccsal titkosítjuk. Az alkalmazásnaplókat ügyfél által kezelt AWS KMS-kulccsal titkosított Amazon CloudWatch-

naplócsoporthoz központosítjuk, és tíz (10) évig őrizzük meg. A különálló audit- és telemetriai naplócsoporthoz szintén ügyfél által kezelt AWS KMS-kulccsal titkosítjuk, és tíz (10) évig őrizzük meg. Az Aurora PostgreSQL-motor naplóexport-csoportját egy (1) hétig őrizzük meg.

5.2 Mit naplózunk és mit nem. A ProcessMind naplózza a HTTP API- és WebSocket-hozzáférési eseményeket – a kérés időpontját, a kérésazonosítókat, az útvonalat vagy elérési utat, a válasz állapotát és késleltetését. A hozzáférési naplók nem tartalmazzák a hívó forrás-IP-címét vagy felhasználói ügynökét. A ProcessMind a hitelesítési eseményeket, az aszinkron hibautakat és a támogató Lambda-alkalmazástevékenységeket is központosított CloudWatch-naplócsoporthoz naplózza. A VPC-forgalmi naplók engedélyezve vannak. A ProcessMind jelenleg nem engedélyezi a CloudFront szabványos hozzáférési naplózását a webhely, a frontend SPA vagy a nyilvános erőforrások disztribúciói esetében.

5.3 Felügyelet és riasztások. A CloudWatch-riasztások és -dashboardok figyelik a rendszer állapotát, a sikertelen üzenetek sorait és a biztonsági szempontból releváns hibákat. Az aszinkron feldolgozási hibák titkosított, sikertelen üzeneteket tároló sorokba kerülnek (tizennégy (14) napos megőrzés; a bélyegkép- és keresésiindex-sorok esetében két (2) nap), a DLQ-riasztások pedig SNS-értesítéseket indítanak a kivizsgáláshoz. Emellett a ProcessMind a Sentryt használja a frontendhibák valós idejű nyomon követésére, a teljesítmény felügyeletére és a munkamenetek visszajátszására. Munkamenet-visszajátszás csak olyan munkamenetekről készül, amelyekben hiba történik; a szövegek, az űrlapmezők és a média maszkolva vagy blokkolva vannak a visszajátszásokban. A Sentry-adatok fogadása az Európai Unióban (Frankfurt) történik, és kizárólag a ProcessMind használati adataira korlátozódik (böngészőhibák, teljesítmény-nyomkövetések, eszközmétaadatok és maszkolt visszajátszási felvételek). A Sentry szerepel az [adatfeldolgozók listáján](#).

5.4 Naplóvédelem. A naplókat dedikált, hozzáférés-vezérelt CloudWatch-naplócsoporthoz tároljuk, és tárolás közben titkosítjuk. Az éles és a fejlesztői naplókat környezet- és fiókhatárok szerint elkülönítjük.

6. Automatizált kontrollérvényesítés és sérülékenységi-kezelés

6.1 Mit tesz a ProcessMind. A ProcessMind az infrastruktúra összeállítási és telepítési munkafolyamatának részeként futtatja a cdk-nag eszközt, több iparági szabálykészletet használva (többek között AWS Solutions, NIST 800-53 és PCI DSS). Az egyes vermekről jelentések készülnek, amelyeket az infrastruktúra-változáskezelés részeként felülvizsgálunk. A megállapításokat javított, elfogadott kockázatként vagy tervezett fejlesztésként soroljuk be.

6.2 A kivételek kezelése. Ahol a keretrendszer ezt lehetővé teszi, a kivételeket központi nyilvántartásban rögzítjük, az érintett vermekre korlátozzuk, és írásbeli indoklást követelünk meg; ha egy verem beágyazott kivételt tartalmaz, azt az adott verem mellett dokumentáljuk. A megállapítás orvoslása során a kapcsolódó kivételt frissítjük vagy eltávolítjuk. A ProcessMind nem tekinti a kivétel rögzítését a felülvizsgálat alóli általános mentesülésnek.

6.3 Amit a ProcessMind jelenleg nem tesz. A ProcessMind nyomon követi és felülvizsgálja az infrastruktúra-kontrollok lényeges kivételeit. A főbb kivételek a következők:

- az alkalmazás Lambda-i alapértelmezés szerint nem kerülnek a VPC-be; az Aurora szolgáltatást az RDS Data API-n keresztül, TLS használatával, IAM- és Secrets Manager-hitelesítéssel érik el
- a szolgáltatás egyetlen részét sem védi az AWS WAF: az AWS WAF nem támogatja az API Gateway HTTP API-kat, és a fennmaradó belépési pontokat sem védi WAF (a WebSocket-kapcsolatok rövid élettartamú HMAC-tokeneket használnak; a fizetéssel kapcsolatos földrajzi korlátozásokat a fizetési rendszer érvényesíti); a statikus disztribúciók esetében a CloudFront szabványos hozzáférési naplózása sem áll rendelkezésre
- az adatbázis helyreállítása az Aurora automatizált biztonsági mentéseire és időpontra történő helyreállítására támaszkodik, nem

pedig külön AWS Backup-csomagra vagy Aurora Enhanced Monitoringra

- nincs régiók közötti S3-replikáció, és a módosítható tárolók esetében nincs S3 Object Lock
- egyes, AWS/CDK/SST által kezelt támogató erőforrások AWS által kezelt titkosítást vagy szélesebb körű, automatikusan létrehozott IAM-házirendeket használnak, ha a szolgáltatás nem tesz elérhetővé ügyfél által szabályozható alternatívát

A kivételek teljes nyilvántartását az infrastruktúra-kóddal együtt tartjuk fenn, és kérésre rendelkezésre bocsátjuk. A cdk-nag szabálykészletek használata mérnöki kontrollérvényesítés, nem pedig külső tanúsítás, auditvélemény vagy a HIPAA, a NIST vagy a PCI DSS szerinti megfelelésről szóló jogi tanúsítvány.

6.4 Függőségkezelés. A szoftverfüggőségeket folyamatosan figyeljük az ismert sérülékenységek szempontjából. A kritikus és magas súlyosságú sérülékenységeket hét (7) napon belül javítjuk. A függőségeket rendszeres ciklusban frissítjük.

6.5 Biztonságos szoftverfejlesztési életciklus (SDLC). A ProcessMind a szoftverfejlesztés során többrétegű védekezési megközelítést követ. Az éles környezetet érintő minden módosításnak több, egymástól független automatizált ellenőrzési rétegen kell átmennie a telepítés előtt:

- **Statikus elemzés és típusbiztonság:** A TypeScript szigorú módja és az ESLint fordítási időben érvényesíti a típushelyességet, a nullbiztonságot és a biztonság szempontjából releváns kódolási mintákat.
- **AI-támogatott kódellenőrzés:** Az AI-támogatott elemzés további ellenőrzési szempontokat biztosít a pull requestekhez, hogy az automatizált tesztelést kiegészítve azonosítsa a biztonsági kockázatokat, a logikai hibákat és a konvencióktól való eltéréseket.
- **Egység- és integrációs tesztek:** Egy átfogó Vitest-tesztcsomag élő AWS-erőforrásokkal ellenőrzi az üzleti logikát, az adathozzáférési

mintákat, az API működését és a hibakezelést a fejlesztői környezetben.

- **Végpontok közötti tesztek:** A Playwright-alapú böngészőtesztek ellenőrzik a kritikus felhasználói munkafolyamatokat, beleértve a hitelesítést, az adatfeltöltést, a folyamatmodellezést, a szimulációt és a több bérllő közötti elkülönítést.
- **Infrastruktúra-megfelelőségi vizsgálat:** A cdk-nag minden módosításkor több megfelelőségi keretrendszer alapján ellenőrzí az infrastruktúra-kódot.
- **Függőségi sérülékenységek vizsgálata:** Az automatizált függőségi auditok megakadályozzák, hogy ismert kritikus és magas súlyosságú sérülékenységek kerüljenek az éles környezetbe.

Az emberi felülvizsgálat az architektúrára, a biztonsági határookra és a tervezési szintű döntésekre összpontosít, nem pedig a kód soronkénti ellenőrzésére. Szerkezeti, biztonsági szempontból érzékeny vagy infrastrukturális módosítások esetén az automatizált ellenőrzés mellett kifejezett emberi jóváhagyás is szükséges.

Minden ellenőrzési réteget a CI érvényesít az alkalmazás- és infrastruktúra-módosítások fő ágba történő egyesítésének kötelező feltételeként. A webhelytartalom és a statikus eszközök kiadásai külön, dokumentált kiadási folyamatot követnek, amely telepítéskori ellenőrzéseket is tartalmaz – többek között annak automatizált ellenőrzését, hogy a jogi dokumentumok naprakészek-e –, nem pedig az alkalmazás CI-kapuja alá tartoznak. A sürgős éles javítások megkerülhetik a CI-kaput, de ezt huszonnégy (24) órán belül teljes folyamatfuttatásnak és incidens utáni felülvizsgálatnak kell követnie.

7. Biztonsági mentés és katasztrófa utáni helyreállítás

7.1 Automatikus biztonsági mentések. Az Amazon Aurora folyamatos, automatikus biztonsági mentéseket készít, amelyek megőrzési ideje hét (7)

nap. A biztonsági mentéseket a forrásadatbázisokkal azonos, ügyfél által kezelt KMS-kulcsokkal titkosítjuk.

7.2 Időpontra történő helyreállítás. Az Aurora támogatja a biztonsági mentési megőrzési időszakon belüli bármely másodpercre történő helyreállítást, lehetővé téve az adatsérülés vagy véletlen törlés esetén a gyors visszaállítást.

7.3 Az S3 tartóssága és verziókezelése. A fájlfeltöltéseket és a működési adatokat az Amazon S3-ban tároljuk, amely 99,999999999%-os (11 kilences) tartósságot biztosít. A feltöltési tárolón és az erőforrás-tárolókon engedélyezve van a verziókezelés a helyreállítás és a visszaállítás támogatására. A webhely és a frontend telepítési tárolói reprodukálható buildtermékeket tartalmaznak, és nem tekintjük őket biztonsági mentési rendszernek. A ProcessMind jelenleg nem engedélyezi a régiók közötti S3-replikációt.

7.4 Üzletmenet-folytonosság. A katasztrófa utáni helyreállítási eljárások dokumentáltak, és időszakosan teszteljük őket. Összefoglalójuk a [Katasztrófa utáni helyreállítás, üzletmenet-folytonosság és incidenskezelés](#) című dokumentumban található. Az architektúra az eu-central-1 régión belüli, AWS által felügyelt szolgáltatásokra támaszkodik, amelyeket az AWS több rendelkezésre állási zónában üzemeltet; az Aurora-fürt jelenleg egyetlen írópéldánnyal fut, ezért az adatbázis helyreállítása automatikus biztonsági mentésekre és időpontra történő helyreállításra támaszkodik, nem pedig régió belüli készenléti példányra. Az Aurora biztonsági mentései, az S3 tartóssága, a sikertelen üzenetek sorai és a forrásból újraépíthető statikus eszközök a helyreállítási stratégia részét képezik.

8. Incidenskezelés

8.1 Incidensértesítés. Biztonsági incidens (a DPA-ban meghatározottak szerint) esetén a ProcessMind indokolatlan késedelem nélkül, és amennyiben megvalósítható, az incidensről való tudomásszerzéstől számított hetvenkét (72) órán belül értesíti az érintett ügyfeleket.

8.2 Incidenskezelés. A ProcessMind dokumentált incidenskezelési eljárásokat tart fenn, amelyek kiterjednek az azonosításra, a korlátozásra, a felszámolásra, a helyreállításra és az incidens utáni felülvizsgálatra. Összefoglalójuk a [Katasztrófa utáni helyreállítás, üzletmenet-folytonosság és incidenskezelés](#) című dokumentumban található. Az incidensekből levont tanulságokat beépítjük a biztonsági kontrollokba és folyamatokba.

8.3 Kommunikáció. Az incidensértesítések tartalmazzák az incidens jellegét és hatókörét, az érintett adatkategóriákat, az incidens korlátozása érdekében tett intézkedéseket, valamint az ügyfél számára javasolt lépéseket.

9. Szervezési intézkedések

9.1. Információbiztonság-irányítás. A ProcessMind az ISO 27001 alapelveivel összhangban álló információbiztonság-irányítási rendszert tart fenn. A ProcessMind kiválasztotta az ISO 27001 tanúsításhoz és a SOC 2 Type II tanúsításhoz vezető utat; a hivatalos tanúsítási folyamat még nem kezdődött meg.

9.2 Biztonságtudatosság. Minden, ügyfeladatokhoz hozzáférő munkatárs biztonságtudatossági képzésben részesül. A biztonsági bevált gyakorlatok beépülnek a beléptetésbe, a fejlesztési munkafolyamatokba és az operatív eljárásokba.

9.3 Szállítók és adatfeldolgozók kezelése. Az adatfeldolgozókat szerződés kötelezi az e dokumentumban ismertetettekkel egyenértékű adatvédelmi normák betartására. A ProcessMind nyilvános [adatfeldolgozói listát](#) tart fenn, és legalább harminc (30) nappal korábban értesítést ad új adatfeldolgozó igénybevételéről. Az adatfeldolgozók megfelelését évente felülvizsgáljuk.

9.4 Titoktartás. Az ügyfeladatok kezelésére jogosult valamennyi munkatársat írásbeli titoktartási kötelezettség terheli.

10. Megfelelés és tanúsítványok

Keretrendszer / szabvány	Állapot
GDPR (az EU általános adatvédelmi rendelete)	Megfelel
EU-n belüli adattárolás (Frankfurt, Németország)	Érvényesítve
AWS-infrastruktúra tanúsítványai (ISO 27001, SOC 2, PCI DSS)	Az AWS révén örökölt
ISO 27001 (ProcessMind)	Tervezett — a tanúsítási út kiválasztva; a hivatalos folyamat még nem kezdődött meg
SOC 2 Type II (ProcessMind)	Tervezett — a tanúsítási út kiválasztva; a hivatalos folyamat még nem kezdődött meg
Automatizált infrastruktúra-kontrollérvényesítés (cdk-nag AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1 és Serverless szabálykészletek alapján)	Mérnöki kontrollérvényesítésként bevezetve, nem tanúsításként
Nemzetközi adattovábbításra vonatkozó általános szerződési feltételek (SCC-k)	Bevezetve (lásd: DPA)
Adatfeldolgozási kiegészítés (DPA)	Nyilvánosan elérhető

A cdk-nag szabálykészletek használata nem jelenti azt, hogy a ProcessMind hivatalosan tanúsított vagy független auditon esett át a HIPAA, a NIST vagy a PCI DSS szerint. Ezeket a szabálykészleteket mérnöki védőkorlátként használjuk az infrastruktúra kialakításának ellenőrzésére és a hiányosságok kifejezett nyomon követésére.

Biztonsággal vagy megfeleléssel kapcsolatos kérdéseivel, illetve auditjelentésekhez vagy kitöltött biztonsági kérdőívekhez hasonló dokumentumok igénylésével forduljon a support@processmind.com címhez.