# ProcessMind安全措施

生效日期：2026年9月14日

本文件说明ProcessMind B.V.为保护客户数据的机密性、完整性和可用性而维护的技术和组织措施（“TOM”）。ProcessMind采用纵深防御方法，通过多个相互独立的安全层，在每个层面保护客户数据——从网络和基础设施，到身份、授权、数据隔离、加密、监控和软件开发。这些措施补充数据处理附录、隐私政策和SaaS托管政策。ProcessMind至少每年审查和更新这些措施。

客户数据绝不会出售给第三方、与第三方共享或被第三方用于其自身目的。

---

**1. 基础设施安全**

**1.1 云平台。**ProcessMind专门托管在欧盟（法兰克福，德国，`eu-central-1`）的Amazon Web Services（AWS）上。AWS持有ISO 27001、ISO 27017、ISO 27018、SOC 1/2/3和PCI DSS认证。完整列表请参阅AWS合规计划。

**1.2 无服务器架构。**ProcessMind应用程序逻辑运行在AWS Lambda和AWS托管服务上。ProcessMind不运营由客户管理的长期运行应用程序服务器，因此减少了大量操作系统修补和服务器加固工作。

**1.3 网络边界。**ProcessMind维护用于数据库和网络控制的AWS VPC。Aurora PostgreSQL运行在无互联网出口的私有子网中，不可公开访问，并已启用VPC流日志。ProcessMind默认不将应用程序Lambda函数置于VPC内。Lambda通过AWS RDS Data API，经由TLS并使用IAM和Secrets Manager身份验证访问Aurora。

**1.4 内容交付和边缘控制。**面向客户的网站、前端SPA和公共资源流量通过Amazon CloudFront提供。所有CloudFront分配均强制执行最低TLS 1.2（2021）策略。网站和前端SPA分配还会添加安全响应标头，包括HTTP严格传输安全（HSTS）、内容安全策略（CSP）、`frame-ancestors 'none'`、`X-Frame-Options: DENY`、`X-Content-Type-Options`、引用来源策略和权限策略。公共资源分配使用CloudFront Origin Access Control，以保持源存储桶为私有。面向客户的API流量通过Amazon API Gateway单独处理：HTTPS请求/响应流量通过专用API子域上的HTTP API提供，实时客户端连接则通过专用WebSocket子域上的独立API Gateway WebSocket API提供。

**1.5 环境隔离。**生产环境和开发环境使用独立的AWS账户、独立的数据库和独立的基础设施堆栈。开发人员凭据不提供对生产客户数据的访问权限。

---

**2. 数据加密**

**2.1 传输中加密。** 客户端与 ProcessMind 服务之间传输的所有数据均使用 TLS 1.2 或席位等级为流程架构或以上进行加密。面向客户的端点通过 HTTPS 提供服务。由 ProcessMind 直接创建的 S3 存储桶、SNS 主题和 SQS 队列强制仅允许通过 SSL 访问。通过 RDS Data API 进行的数据库访问以及其他 AWS 服务调用均使用 HTTPS/TLS。

**2.2 静态数据加密。**Aurora PostgreSQL使用客户管理的AWS KMS密钥进行静态加密，并自动轮换密钥。由ProcessMind直接创建的客户数据和运营S3存储桶，包括上传、资源和访问日志存储桶，均使用客户管理的KMS密钥。由ProcessMind直接创建的CloudWatch日志组、SNS主题和SQS队列也使用客户管理的KMS密钥。SST管理的网站和前端源存储桶使用AWS管理的S3服务器端加密（SSE-S3 / AES-256），而非客户管理的KMS密钥。

**2.3 密钥管理和机密信息。**数据库加密密钥通过AWS KMS集中管理，密钥访问遵循最小权限原则并由IAM策略控制。数据库凭据存储在AWS Secrets Manager中。Aurora主机密钥和受限应用程序用户密钥每三十（30）天自动轮换。生产密钥和机密信息绝不存储在源代码中；仅供开发使用的凭据与生产环境隔离。部分由AWS/CDK/SST管理的支持资源在服务或框架未提供客户管理密钥配置时，仍继续使用AWS管理的加密。

---

**3. 数据隔离和驻留**

**3.1 租户隔离。**每个客户租户均获得专用且隔离的数据库实例。客户数据在数据库层面绝不与其他客户的数据混合存储。共享元数据（例如账户记录、计费信息、用户与租户的映射）存储在独立的多租户数据库中，并受到严格的访问控制。租户和组织范围的共享表还受到通过请求范围数据库上下文实施的PostgreSQL行级安全（RLS）策略的额外保护。

**3.2 数据驻留。**所有客户数据，包括数据库、文件上传、备份和查询结果，均专门存储在欧盟（法兰克福，德国）。如果为特定处理活动（例如AI模型处理或支付处理）

聘用位于欧洲经济区（EEA）以外的子处理者，则该传输由《数据处理附录》中所述的适当传输机制覆盖，且该子处理者及其处理地点列于《子处理者列表》中。

**3.3 数据保留和删除。**保留和删除期限载于数据处理附录第6节。客户可以随时通过应用程序或联系ProcessMind删除其数据。备份副本将在适用的备份保留期限届满时删除（第7.1节）。

---

**4. 身份和访问管理**

**4.1 身份验证。**ProcessMind支持通过Microsoft Entra ID（Azure AD）、Google OAuth 2.0/OIDC和LinkedIn OAuth 2.0/OIDC实现单点登录（SSO）。ProcessMind作为依赖方运行，不存储用户密码。多因素身份验证由身份提供商强制执行——例如，当组织连接Microsoft Entra ID（Azure AD）时，该组织自身的MFA和访问策略适用。

**4.2 会话管理。**浏览器会话使用签名的JSON Web Token（JWT），通过带有SameSite和Secure标志的安全HttpOnly Cookie传输。每次经过身份验证的请求都会验证令牌签名。

**4.3 授权模型。**ProcessMind的核心应用程序API不依赖API Gateway原生授权方。授权在共享Lambda处理程序包装器中执行，该包装器在业务逻辑运行前验证会话状态和租户范围。公共路由明确列入允许列表，用于未经过身份验证的流程、webhook、事件摄取和CORS预检。外部API端点使用专用身份验证处理程序。对客户数据的访问限定于经过身份验证的租户或组织上下文。

**4.4 最小权限。**内部系统遵循最小权限原则。在框架允许精确限定范围的情况下，IAM角色限定为所需的最少资源。部分SST/CDK生成的角色为绑定和运行时操作使用范围更广的托管策略或内联策略；这些情况会经过审查，在可能的情况下限定资源范围，并作为明确例外进行跟踪。

**4.5 员工访问控制。**员工对内部系统的访问通过Active Directory以及SSO和强制MFA进行管理。基于角色的访问控制（RBAC）确保只有获授权人员在确有必要知悉的基础上访问客户数据。访问权限会定期审查。

---

**5. 日志记录、监控和审计**

**5.1 集中式日志记录。**HTTP API访问日志和WebSocket访问日志已启用结构化JSON字段，并写入Amazon CloudWatch Logs，保留一（1）周。这些访问日志组使用客户管理的AWS KMS密钥加密。应用程序日志集中存储在使用客户管理的AWS KMS密钥加密的Amazon CloudWatch日志组中，并保留十（10）年。独立的审计和遥测日志组也使用客户管理的AWS KMS密钥加密，并保留十（10）年。Aurora PostgreSQL引擎日志导出组保留一（1）周。

**5.2 记录的内容和未记录的内容。**ProcessMind记录HTTP API和WebSocket访问事件，包括请求时间、请求标识符、路由或路径、响应状态、延迟、源IP和用户代理。ProcessMind还将身份验证事件、异步失败路径和支持性的Lambda应用程序活动记录到集中式CloudWatch日志组中。VPC流日志已启用。ProcessMind目前未在网站、前端SPA或公共资源分配上启用CloudFront标准访问日志记录。

**5.3 监控和告警。**CloudWatch警报和仪表板监控系统运行状况、死信队列和安全相关故障。异步处理故障会路由至加密的死信队列（保留十四（14）天；缩略图和搜索索引队列保留两（2）天），DLQ警报会触发SNS通知以供调查。此外，ProcessMind使用Sentry进行实时前端错误跟踪、性能监控和会话重放。会话重放仅针对发生错误的会话进行记录，且重放中的文本、表单输入和媒体会被遮蔽或阻止。Sentry数据在欧盟（法兰克福）摄取，并仅限于ProcessMind使用数据（浏览器错误、性能跟踪、设备元数据和经过遮蔽的重放记录）。Sentry列于子处理者列表中。

**5.4 日志保护。**日志存储在专用且受访问控制的CloudWatch日志组中，并进行静态加密。生产日志和开发日志按照环境和账户边界分开。

---

**6. 自动化控制验证和漏洞管理**

**6.1 ProcessMind所做的工作。**ProcessMind在其基础设施合成和部署工作流程中运行`cdk-nag`，使用多个行业规则包（包括AWS Solutions、NIST 800-53和PCI DSS）。每个堆栈均生成报告，并作为基础设施变更管理的一部分进行审查。发现项被分类为已修复、已接受风险或计划改进。

**6.2 例外的管理方式。**在框架允许的情况下，抑制项会记录在中央登记册中，限定于受影响的堆栈，并要求提供书面理由；如果某个堆栈包含内联抑制项，则会在该堆

栈旁进行记录。发现项得到补救后，相应的抑制项会被更新或删除。ProcessMind不会将抑制视为免于审查的全面选择退出。

**6.3 ProcessMind目前未开展的工作。**ProcessMind跟踪并审查重大的基础设施控制例外。主要例外包括：

- 默认情况下，application Lambdas 不置于 VPC 内；它们通过采用 TLS 的 RDS Data API，并使用 IAM 和 Secrets Manager 进行身份验证来访问 Aurora
- WebSocket API 和静态分发不位于 AWS WAF 后方（WebSocket 连接使用短期 HMAC 令牌；支付相关的地理限制在支付系统中执行），且静态分发未启用 CloudFront 标准访问日志记录
- 数据库恢复依赖 Aurora 自动备份和时间点恢复，而非单独的 AWS Backup 计划或 Aurora Enhanced Monitoring
- 可变存储桶未配置跨区域 S3 复制或 S3 Object Lock
- 部分由 AWS/CDK/SST 管理的支持资源使用 AWS 管理的加密，或使用范围更广的生成式 IAM policy（在服务未提供由客户控制的替代方案时）

完整的抑制注册表与基础设施代码一并维护，并可应要求提供。使用 `cdk-nag` 规则包属于工程控制验证，并非外部认证、审计意见，也不是对 HIPAA、NIST 或 PCI DSS 合规性的法律证明。

**6.4 依赖项管理。** 软件依赖项会持续监测已知漏洞。严重和高严重性漏洞的修补目标为七（7）天内完成。依赖项按定期周期更新。

**6.5 安全软件开发生命周期（SDLC）。** ProcessMind 对软件开发采用纵深防御方法。生产环境中的每项变更在部署前都必须通过多个相互独立的自动化验证层：

- **静态分析和类型安全：** TypeScript 严格模式和 ESLint 在编译时强制执行类型正确性、空值安全性以及与安全相关的编码模式。
- **AI 辅助代码审查：** AI 辅助分析为拉取请求提供额外的审查视角，以识别安全风险、逻辑错误和约定偏差，并补充自动化测试。
- **单元测试和集成测试：** 全面的 Vitest 测试套件在开发环境中针对实时 AWS 资源验证业务逻辑、数据访问模式、API 行为和错误处理。
- **端到端测试：** 基于 Playwright 的浏览器测试验证关键用户工作流，包括身份验证、数据上传、流程建模、模拟和多租户隔离。

- **基础设施合规扫描：** `cdk-nag`在每次变更时根据多个合规框架验证基础设施即代码。
- **依赖项漏洞扫描：**自动化依赖项审计会阻止已知的严重和高严重性漏洞进入生产环境。

人工审查重点关注架构、安全边界和设计层面的决策，而非逐行检查代码。涉及结构性变更、安全敏感变更或基础设施变更时，除自动化验证外，还必须取得明确的人工批准。

所有验证层均通过 CI 执行，作为对主分支变更的必需合并门禁。紧急生产修复可以绕过 CI 门禁，但必须在二十四（24）小时内完成完整流水线运行并进行事后事件审查。

---

**7. 备份和灾难恢复**

**7.1 自动备份。** Amazon Aurora 执行持续的自动备份，保留期限为七（7）天。备份使用与源数据库相同的客户管理 KMS 密钥进行加密。

**7.2 时间点恢复。** Aurora 支持恢复至备份保留窗口内的任意一秒，从而能够在数据损坏或意外删除的情况下快速恢复。

**7.3 S3 持久性和版本控制。** 文件上传和运营工件存储在 Amazon S3 中，其持久性为 99.999999999%（11 个 9）。上传存储桶和资源存储桶已启用版本控制，以支持恢复和回滚。网站和前端部署存储桶属于可复现的构建工件，不作为备份系统处理。ProcessMind 目前未启用跨区域 S3 复制。

**7.4 业务连续性。** 灾难恢复程序已形成文件并定期测试。摘要载于 [灾难恢复、业务连续性和事件响应]文件中。该架构依赖 `eu-central-1`区域内的 AWS 托管服务，AWS 在多个可用区之间运行这些服务；Aurora 集群目前运行单个写入器实例，因此数据库恢复依赖自动备份和时间点恢复，而非区域内备用实例。Aurora 备份、S3 持久性、死信队列以及从源重新构建的静态资产均属于恢复策略的一部分。

---

**8. 事件响应**

**8.1 事件通知。**发生安全事件（定义见 DPA）时，ProcessMind 将在不无故延迟的情况下通知受影响的客户，并在可行的情况下，于知悉事件后七十二（72）小时内

通知。

**8.2 事件处理。** ProcessMind 维护成文的事件响应程序，涵盖识别、遏制、根除、恢复和事后审查。摘要载于 灾难恢复、业务连续性和事件响应文件中。事件中获得的经验教训将纳入安全控制和流程。

**8.3 沟通。**事件通知包括事件的性质和范围、受影响的数据类别、为遏制事件所采取的措施以及建议客户采取的行动。

---

### 9. 组织措施

**9.1 信息安全管理。** ProcessMind 维护与 ISO 27001 原则一致的信息安全管理体系。ProcessMind 已选择 ISO 27001 认证和 SOC 2 Type II 鉴证的认证路径；正式认证流程尚未开始。

**9.2 安全意识。**所有可访问客户数据的人员均接受安全意识培训。安全最佳实践已融入入职、开发工作流和运营程序。

**9.3 供应商和子处理者管理。**子处理者在合同上受约束，须遵守与本文件所述标准等同的数据保护标准。ProcessMind 维护公开的 子处理者列表，并在聘用新的子处理者前至少三十（30）天发出通知。每年审查子处理者的合规性。

**9.4 保密性。**所有获授权处理客户数据的人员均受书面保密义务约束。

---

### 10. 合规与认证

| 框架/标准 | 状态 |
| --- | --- |
| GDPR（欧盟《通用数据保护条例》） | 合规 |
| 欧盟数据驻留（德国法兰克福） | 已执行 |
| AWS 基础设施认证（ISO 27001、SOC 2、PCI DSS） | 通过 AWS 继承 |
| ISO 27001（ProcessMind） | 计划中——已选择认证路径；正式流程尚未开始 |

| 框架/标准 | 状态 |
| --- | --- |
| SOC 2 Type II（ProcessMind） | 计划中——已选择认证路径；正式流程尚未开始 |
| 自动化基础设施控制验证（cdk-nag涵盖 AWS Solutions、HIPAA Security、NIST 800-53 R4/R5、PCI DSS 3.2.1、Serverless） | 作为工程控制验证实施，而非认证 |
| 国际传输的标准合同条款（SCC） | 已实施（见 DPA） |
| 数据处理附录（DPA） | 公开提供 |

使用 cdk-nag 规则包并不意味着 ProcessMind 已通过 HIPAA、NIST 或 PCI DSS 的正式认证或独立审计。这些规则包用作工程防护措施，以验证基础设施设计并明确跟踪差距。

如有关于安全、合规的问题，或希望索取审计报告、已完成的安全问卷等文件，请联系 **support@processmind.com**。