ProcessMind 审计日志和 SIEM 声明

生效日期：2026 年 11 月 12 日

本声明说明 ProcessMind B.V. 如何记录针对客户数据执行的与安全相关及管理操作（“审计日志”）。本声明是对安全措施、数据处理附录、客户协议及子处理者清单的补充。

---

1. 范围

1.1 单一审计日志。ProcessMind 针对客户数据和 ProcessMind 服务维护一份用于记录与安全相关及管理操作的审计日志。该审计日志独立于运营（应用程序）日志记录、HTTP 访问日志记录以及产品活动流；这些数据流用途各异，不作为审计跟踪记录。

1.2 不包括的内容。审计日志并非对每次读取客户数据的记录，也不是产品中流程模型、图表、文档或模拟的变更历史。这些内容记录在产品内提供的流程变更历史中。

---

2. 每条审计记录包含的内容

2.1 字段。每条记录均包含以下字段。字段集合由记录架构固定：记录不得增加此列表之外的字段，操作也不得添加其在注册表中未声明的字段。

- *schemaVersion*（数字）：记录架构版本，目前为 1。
- *eventId*（字符串）：唯一记录标识符。新记录使用 ULID；从早期存储迁移的行保留其 UUID。
- *occurredAt*、*ingestedAt*（时间戳）：操作发生的时间，以及审计写入器存储记录的时间。两者均为 UTC。
- *eventClass*（枚举）：security、auth、admin、data、api、ai 或 platform。
- *action*（枚举）：来自封闭且经过审核的操作注册表中的一个代码，例如 auth.login.blocked 或 api.key.revoked。
- *outcome*（枚举）：success、failure、denied 或 error。

- *severity*（枚举）：info、notice、warning 或 critical，根据结果确定。成功操作使用其注册表默认值（除非操作另有规定，否则为 info）；failure 记录为 notice；denied 或 error 记录为 warning。
- *actor*（对象）：执行操作的主体。type（user、apiKey、service、system 或 anonymous）、id、email、displayName；若操作代表另一账户执行，还包括 onBehalfOf 和 onBehalfOfEmail。
- *actorContext*（对象）：执行操作的会话。sessionId、authMethod（oidc、password、loginToken、apiKey 或 none）以及支持会话标记。
- *organizationId*、*tenantId*（标识符，可为空）：操作所属的组织和环境。对于不涉及客户或位于环境层级之上的记录，该值为 Null。
- *resource*（对象，可为空）：受影响的对象。包括 type、id 和 name，其中 type 为 apiKey、artifact、connection、database、datatable、export、lead、model、organization、process、role、session、setting、storage、tenant 或 user 之一。
- *source*（对象）：记录的生成位置。包括 service（api、externalApi、superadminApi、worker、cron 或 webSocket）、function 和 version。
- *stage*、*region*（字符串）：生成记录的部署阶段（例如 prod）和 AWS 区域（客户记录为 eu-central-1）。
- *correlation*（对象）：requestId、traceId 和 parentEventId，用于将记录关联至引发该记录的请求，以及同一流程中先前的记录。
- *network*（对象，可为空）：sourceIp 和 userAgent。仅针对注册表条目选择启用此项的操作采集：登录、访问决策、管理和设置变更、数据上传、下载和导出、API 密钥变更以及 AI 政策变更。
- *detail*（对象）：操作自身的有效负载，并根据该操作的架构进行验证。值仅限基本类型（字符串、数字、布尔值、null），以确保记录可查询且可编辑删除敏感信息。

2.2 封闭词汇表。操作取自固定且经过审核的操作代码列表；审计记录中不包含自由文本消息。每项操作还会声明其可携带的其他字段，因此记录不会在不知情的情况下增加新的内容类型。

---

3. 记录哪些操作

3.1 当前记录的操作。ProcessMind 记录的操作包括：

- **身份验证：**登录成功和失败、登录受阻（账户锁定、域名不允许、提供商电子邮件未经验证）、登出、登录令牌签发和移交。
- **授权：**访问拒绝，包括每次被拒绝的外部 API 凭据、范围和租户状态，以及来源（CORS）拒绝。
- **支持访问：**ProcessMind 支持人员开始在客户账户上进行支持会话时，记录操作人员和受影响账户双方的信息。
- **API 凭据：**API 密钥的创建、范围变更和撤销，包括授予的范围。
- **账户和角色管理：**用户创建、邀请、管理员资料编辑、删除、角色授予和撤销，以及租户或组织成员资格变更。
- **组织生命周期：**创建、删除、恢复、安排删除和取消删除，以及完成擦除。
- **数据上传、下载和导出：**工件上传、下载和删除，表格数据上传和更新，导出下载，数据表删除，以及 webhook（连接）的创建、变更和删除。
- **账单状态：**计划变更、因付款导致的暂停和恢复，以及订阅取消。
- **ProcessMind 的提供商控制台：**特权查询执行、用户和组织管理、设置和功能变更、账单同步请求及迁移。
- **ProcessMind 定时作业执行的管理和破坏性操作：**租户、组织、用户和潜在客户删除、保留期限清理，以及管道故障。
- **审计日志完整性：**审计日志自身写入路径发生故障。

3.2 工作区编辑。工作区内的编辑（流程模型、文档、模拟、仪表板、评论和书签）记录在产品自身的流程变更历史中，而非审计日志中。审计日志记录谁上传、下载、导出或删除了数据；变更历史记录模型内部发生了哪些变更。可应要求向 ProcessMind 索取当前记录的操作代码清单。

---

4. 永不记录的内容

密码、身份验证令牌、API 密钥值、Cookie、授权标头、请求或响应正文、文件内容、预签名 URL 以及 AI 提示或生成内容绝不会写入审计日志。审计记录可能包含归属所必需的个人数据：操作主体的电子邮件地址，以及对于注册表条目选择启用此项的操作（登录、访问决策、管理和设置变更、数据传输、API 密钥和 AI 政策变更）的来源 IP 地址和用户代理。每项操作允许记录的字段均有定义，并在新增操作时进行审核。

---

5. 完整性

5.1 仅追加。审计日志仅允许追加。任何应用程序角色均无权更新或删除日志，且数据库约束会拒绝这两种操作。

5.2 单一写入器。记录由单一组件写入，该组件会在写入前验证操作代码及其有效负载。未通过验证的记录将被拒绝并报告，而不会部分写入。

5.3 故障处理。审计写入失败绝不会导致其所描述的业务操作失败。该故障会通过带警报的运营路径记录，且记录本身会保存在辅助副本中，以便恢复。

---

6. 保留期限和存储位置

6.1 保留期限。审计记录自事件发生之日起至少保留十（10）年。

6.2 存储位置和加密。审计记录存储在欧盟（德国法兰克福，`eu-central-1`），并使用客户管理的 AWS KMS 密钥进行静态加密。另有一份实时副本写入访问受控的 Amazon CloudWatch 日志组，以便在事件发生期间进行调查。

6.3 不进行跨区域复制。审计记录不会复制到欧盟以外。

---

7. 访问审计记录

7.1 访问权限。应用内审计日志包含在 Process Architecture 计划及更高级别计划中。组织管理员可读取整个组织的记录；限定于租户范围的管理员可读取其自身租户的记录。访问范围根据经过身份验证的会话确定，并在查询前进行检查，因此请求无法将范围扩大至其他租户或组织。

7.2 ProcessMind 人员。ProcessMind 人员仅在支持、事件响应或履行法律义务所需时，基于知情必要原则访问审计记录。跨客户访问仅限专门的支持角色，且此类访问本身也属于管理操作。

7.3 如何获取记录。组织和租户管理员可在应用内审计日志中读取其审计记录，并通过外部 API 提取或导出记录。对于较大规模或需要协助的请求，ProcessMind 支持团队会提供指定组织、租户和时间范围的 CSV 或 JSON 格式记录；标准请求的目标处理时间为五（5）个工作日。

---

8. 删除审计记录

8.1 应请求删除。收到经核实的书面请求后，ProcessMind 会从审计存储中擦除属于客户组织的审计记录，并以书面形式确认已完成擦除。运营用 CloudWatch 副本无法逐条编辑；该副本会根据自身保留期限到期。

8.2 保留的内容。擦除操作本身的记录（组织标识符、日期、请求人、原因以及删除的记录数量）将作为平台级审计记录予以保留，且不包含客户数据。客户擦除请求不影响不属于任何客户的记录（ProcessMind 平台事件）。

8.3 个人擦除请求。如果请求涉及仍在使用服务的客户组织内的个人，则根据 GDPR 第 17(3)(b) 和 (e) 条，在法律主张的确立、行使或抗辩所允许的范围内保留安全记录；该依据会记录在处理活动记录和隐私政策中。

---

9. SIEM 集成和导出

9.1 可用性。不可变审计归档是 Enterprise 选项，可应要求为客户组织启用。该选项会在 Object-Locked（WORM）S3 存储桶中，按每个组织的前缀写入每日压缩的 NDJSON 对象，并附带清单和每夜对账。

9.2 当前交付方式。ProcessMind 目前不提供原生 SIEM 连接器或推送数据流。交付采用拉取方式，可通过三个渠道进行：读取 API（`GET /v1/tenant/{tenantId}/audit`）、有范围限制的导出作业（使用 `POST /v1/tenant/{tenantId}/audit/exports`创建，并通过其状态调用获取结果；该调用会返回短时有效的下载 URL），以及启用 Enterprise 归档后，存储在 Object-Locked 存储桶中组织专属前缀下的每日对象；客户的 SIEM 通过访问安排读取这些对象。ProcessMind 不会自行按其安排将记录交付至客户指定的位置。

9.3 ProcessMind 自身的监控。ProcessMind 的安全监控会使用相同记录：审计写入失败、身份验证失败激增、权限变更和破坏性管理操作会触发内部警报。

---

10. 可向客户提供的证明材料

应要求，并在适用时遵守保密义务，ProcessMind 会提供本声明、安全措施、数据处理附录、子处理者清单、经删节的审计记录样本，以及用于处理访问和擦除请求的程序。

11. 限制

为免生疑义，ProcessMind 声明每个组织均使用仅允许追加的审计存储；在启用审计归档权限的情况下，还使用带有每夜清单对账的 Object-Locked（WORM）副本。ProcessMind 目前不声明采用哈希链、提供原生实时 SIEM 推送连接器、对审计记录进行逐用户删节、具有涵盖此项控制的 ISO 27001 或 SOC 2 鉴证，或覆盖对客户数据的每次读取。客户可通过应用内审计日志和外部 API 自行读取和导出记录。