

ProcessMind SaaS托管

生效日期：2026年9月14日

1. 引言

ProcessMind B.V. (“我们”) 在位于**德国法兰克福**的Amazon Web Services (AWS) 基础设施上提供软件即服务 (SaaS) 解决方案。本托管政策概述我们对客户作出的承诺，以及我们为确保托管环境的可靠性、安全性和合规性而遵循的标准。

2. 托管基础设施

我们的SaaS解决方案托管在AWS上，利用Amazon Web Services提供的稳健、可扩展且安全的基础设施。我们服务的主要数据中心位于德国法兰克福，确保您的数据存储在欧盟 (EU) 境内。

3. 数据安全

我们致力于维护客户数据的安全性和完整性。AWS提供高度安全的环境及全面的安全服务套件，包括但不限于：

- **物理安全**：AWS数据中心受到广泛的物理安全措施保护，以防止未经授权的访问。
- **网络安全**：防火墙、网络监控以及加密通信保护传输中和静态存储的数据。
- **访问控制**：实施严格的访问控制和身份验证机制，以确保只有获授权人员能够访问客户数据。

4. 数据隐私

您的隐私对我们很重要。我们遵守所有相关的数据保护法律，包括《通用数据保护条例》(GDPR)。有关我们如何处理您的个人数据的更多详情，请参阅我们的[隐私政策](#)。

5. 服务可用性

我们通过冗余、监控、受控发布和运营响应程序，为生产环境设计高可用性。本托管政策仅供参考，其本身不构成合同性正常运行时间承诺。

ProcessMind在processmind.com/status发布当前状态、正常运行时间百分比和响应时间历史记录。状态页面与应用程序前端分开托管；其实时状态数据由我们的API提供，因此在API发生事件期间，页面本身仍可访问，但可能显示有限的状态信息。有关正常运行时间的衡量方式，请参阅[服务级别协议](#)。

合同性可用性承诺、事件响应目标、服务抵扣额和支持条款载于[服务级别协议](#)中。

6. 备份与灾难恢复

- **备份：**生产客户数据的自动备份至少每日运行一次，并在AWS区域内持久存储；备份目前不会复制到第二个区域。
- **灾难恢复：**恢复措施和优先级载于《灾难恢复、业务连续性与事件响应摘要》。

7. 合规

ProcessMind托管在持有以下认证的AWS基础设施上：

- **ISO 27001：**信息安全管理
- **ISO 27017：**云专属控制
- **ISO 27018：**云中个人数据保护
- **SOC 1、SOC 2、SOC 3：**服务组织控制

这些认证适用于ProcessMind运营所依托的AWS基础设施。ProcessMind通过使用AWS托管服务继承这些控制措施。ProcessMind已为其自身的ISO 27001认证和SOC 2 Type II鉴证选择认证路径；正式流程尚未开始。

ProcessMind遵守《通用数据保护条例》（GDPR）关于数据保护和隐私的要求。有关ProcessMind自身技术和组织安全措施的细节，请参阅[安全措施](#)文件。

8. 客户责任

客户负责维护其账户凭据的安全，并对使用其账户采取的任何行动负责。客户应：

- 为其账户使用强度高且唯一的密码。
- 在可用时使用多因素身份验证（MFA）。
- 定期更新和审查访问权限。
- 立即向我们的支持团队报告任何可疑活动或安全漏洞。

9. 托管政策的变更

我们可能会不时更新本托管政策，以反映我们实践或法律要求的变化。我们将通过网站或直接通信通知客户任何重大变更。

相关政策

有关支持受理、请求优先级排序和合同承诺，请参阅服务级别协议。

联系信息

如对本托管政策有任何问题或疑虑，请通过以下方式联系我们：

ProcessMind B.V.

Willem Sandbergstraat 33,

7425RC, Deventer,

The Netherlands

电话：+31 85 060 68 09

电子邮件：support@processmind.com

使用我们的服务即表示您确认已阅读本托管政策。本政策仅供参考，除《客户协议》、《数据处理附录》、《服务级别协议》和《安全措施》规定的承诺外，不构成任何合同性承诺。