

# 结论

## 数据隐私影响评估 (DPIA)

Pre-DPIA 评估个人数据的处理计划是否对数据主体构成高风险。根据管辖范围、项目规模和性质以及要处理的数据类型，它可以帮助确定是否有必要进行全面的 DPIA。

全面的数据隐私影响评估 (DPIA) 旨在评估隐私风险。在当地法律或法规要求的情况下，在开始新项目、引入新项目或对个人数据产生重大影响的现有应用程序、产品或服务时，需要完成 DPIA。

## 处理活动记录 (ROPA)

个人数据的处理必须记录在处理活动记录 (ROPA) 中。它详细说明了正在处理的个人数据类型、保存地点和原因，以及哪些人可以访问这些数据。如需了解更多信息，请联系您当地的信息管理与隐私团队或当地合规团队。

## 人工智能的风险

使用人工智能会带来一些风险，需要加以降低。其中包括：

- 偏见和歧视：人工智能只能根据它所获取的数据做出决策，而不是根据全局做出决策。
- 缺乏透明度：很难解释决定是如何做出的，尤其是在决策过程中没有人为干预的情况下。
- 信息安全：大型系统有可能被黑客攻击，获取并泄露大量个人数据。

苏黎世按照安全、透明、负责任和可靠等“负责任人工智能”原则开展工作。

## 风险管理框架

除了遵循“负责任的人工智能”原则之外，我们对人工智能的使用还受到我们的风险管理框架（包括数据隐私和信息安全政策）以及 AIAF 指南的约束。该指南纳入了行业最佳实践，用于在人工智能系统的整个生命周期内，从准确性、可解释性和公平性等方面对其进行评估。

如需了解更多信息，请联系您当地的人工智能治理专家或当地合规团队。

## 联系人

如对人工智能的使用有任何疑问，请联系当地的人工智能治理专家或当地合规团队。

