

まとめ

データ・プライバシー影響評価（DPIA）

事前データ・プライバシー影響評価（Pre-DPIA）は、計画された個人データの処理がデータ主体に高いリスクをもたらすかどうかを評価します。国や地域、プロジェクトの規模や性質、処理されるデータの種類に応じて、全面的なデータ・プライバシー影響評価（DPIA）が必要かどうかを判断するのに役立ちます。

全面的なデータ・プライバシー影響評価（DPIA）は、プライバシーリスクを評価するために設計されています。その国の法規制で義務付けられている場合、個人データに大きな影響を与えるような新規プロジェクトの開始や、新規アプリケーション、商品、サービスの導入、または既存のものに対する大幅な変更の際して、全面的なデータ・プライバシー影響評価（DPIA）を完了する必要があります。

処理活動記録（ROPA）

個人データの処理は、処理活動記録（ROPA）に記録されなければなりません。これは、どのような種類の個人データが処理され、どこで、何のために保有され、誰がアクセスできるのかについて記載したものです。詳細は、各地域のインフォメーションガバナンスやプライバシーチームまたはローカルのコンプライアンス部にお問い合わせください。

AIのリスク

AIの使用には、軽減すべきいくつかのリスクが伴います。それらリスクには以下が含まれます。

- 偏見と差別：AIはアクセスできるデータに基づいてのみ判断するため、全体像を把握することはできません。
- 透明性の欠如：特に意思決定に人が介在しない場合、どのように意思決定がなされたかを説明するのは難しいことがあります。
- 情報セキュリティ：大規模なシステムがハッキングされ、大量の個人データにアクセスし、漏えいする恐れがあります。

チューリッヒは、「安全性」「透明性」「説明責任」「信頼性」といった「AIの責任ある活用」の原則に基づき、責任を持って業務に取り組んでいます。

リスク管理の枠組み

AIの責任ある活用の原則に取り組むだけでなく、AIの使用は、データ・プライバシーおよび情報セキュリティポリシー、ならびに人工知能評価・フレームワーク（AIAF）ガイダンスを含むリスク管理フレームワークによって管理されています。このガイダンスは、AIシステムのライフサイクル全体にわたって、正確性、説明可能性、公正性の観点からAIシステムを評価するための業界のベストプラクティスを組み込んでいます。

詳細については、AIガバナンスのローカルエキスパートまたはローカルのコンプライアンス部にお問い合わせください。

連絡先

AIに関するお問い合わせは、AIガバナンスのローカルエキスパートまたはローカルのコンプライアンス部までご連絡ください。

