

Wnioski

Ocena wpływu na prywatność danych (DPIA)

Pre-DPIA ocenia, czy planowane przetwarzanie danych osobowych stwarza wysokie ryzyko dla osoby, której dane dotyczą. W zależności od jurysdykcji, rozmiaru i charakteru projektu oraz rodzaju danych, które mają być przetwarzane, może to pomóc w ustaleniu, czy pełna ocena skutków dla ochrony danych może być konieczna.

Pełna ocena wpływu na prywatność danych (DPIA) ma na celu ocenę zagrożeń dla prywatności. Tam, gdzie jest to wymagane przez lokalne przepisy lub regulacje, ocena skutków dla ochrony danych musi zostać przeprowadzona przy rozpoczynaniu nowego projektu, wprowadzaniu nowej lub znaczącej modyfikacji istniejącej aplikacji, produktu lub usługi o dużym wpływie na dane osobowe.

Rejestr czynności przetwarzania (ROPA)

Przetwarzanie danych osobowych musi być udokumentowane w Rejestrze czynności przetwarzania (ROPA). Zawiera on szczegółowe informacje na temat tego, jakiego rodzaju dane osobowe są przetwarzane, gdzie i dlaczego są przechowywane oraz kto ma do nich dostęp. Skontaktuj się z lokalnym zespołem ds. zarządzania informacjami i prywatnością lub lokalnym zespołem ds. zgodności, aby uzyskać więcej informacji.

Zagrożenia związane ze sztuczną inteligencją

Wykorzystanie sztucznej inteligencji wiąże się z pewnym ryzykiem, które należy ograniczyć. Obejmuje ono:

- Uprzedzenia i dyskryminację: Sztuczna inteligencja może podejmować decyzje tylko na podstawie danych, do których ma dostęp, a nie na podstawie pełnego obrazu.
- Brak przejrzystości: może być trudno wyjaśnić, w jaki sposób podejmowane są decyzje, zwłaszcza gdy nie ma interwencji człowieka w podejmowaniu decyzji.
- Bezpieczeństwo informacji: istnieje możliwość włamania się do dużych systemów, uzyskując dostęp do dużych ilości danych osobowych i ujawniając je.

Zurich działa odpowiedzialnie zgodnie z zasadami Odpowiedzialnej Sztucznej Inteligencji, takimi jak bezpieczeństwo, przejrzystość, odpowiedzialność i niezawodność.

Ramy zarządzania ryzykiem

Oprócz pracy zgodnie z zasadami odpowiedzialnej sztucznej inteligencji, nasze wykorzystanie sztucznej inteligencji podlega naszym ramom zarządzania ryzykiem, w tym polityce prywatności danych i bezpieczeństwa informacji, a także naszym wytycznym AIAF. Wytyczne te obejmują najlepsze praktyki branżowe w zakresie oceny systemów sztucznej inteligencji między innymi pod względem dokładności, zrozumiałości i uczciwości, przez cały cykl ich życia.

Aby uzyskać więcej informacji, skontaktuj się z lokalnym ekspertem ds. zarządzania sztuczną inteligencją lub lokalnym zespołem ds. zgodności.

Z kim się skontaktować

Skontaktuj się z lokalnym ekspertem ds. zarządzania sztuczną inteligencją lub lokalnym zespołem ds. zgodności w przypadku jakichkolwiek pytań dotyczących sztucznej inteligencji.

