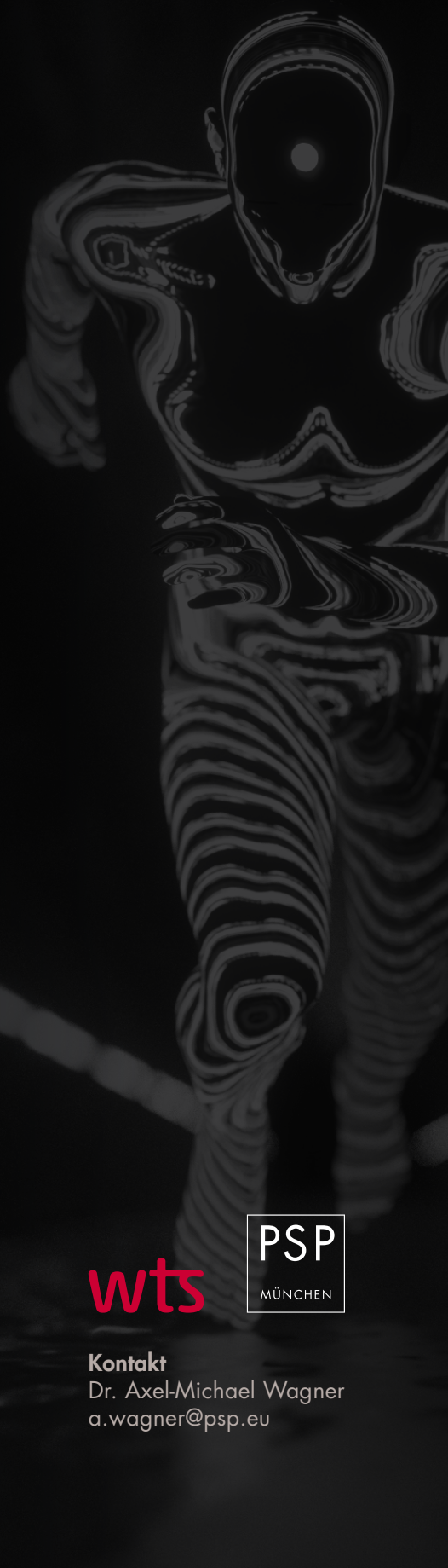
Was zu beachten ist: **KI-Anwendungen und Datenschutz**



1. **Risikoanalyse**

→ „make or buy"-Entscheidung nach „privacy by design"- Kriterien: Welche Produkte / Services gibt es am Markt, welches datenschutzrechtliche Risikoprofil nach den folgenden Punkten weisen diese auf? Welche Vor- und Nachteile hat im Verhältnis dazu eine Eigenentwicklung?

→ Technische Analyse der KI-Anwendung: Wird ein eigenes KI-Modell trainiert oder ein vorbestehendes Modell eines Dritten verwendet („KI-as-a-Service")?

→ Technische Analyse der KI-Anwendung: Welche Input-Daten werden wie verarbeitet, welche Output-Daten werden wie generiert? Wie verändert sich der Datenbestand im Zeitverlauf? Was ist der „worst case" bei fehlerhaftem Output, insbesondere für einzelne Personen?

→ Analyse der personenbezogenen Daten: Wessen Daten und welche Kategorien von Daten werden verarbeitet? Bei Nutzung eines vorbestehenden Modells: Welche personenbezogenen Daten sind schon Teil des Modells selbst?

→ Gibt es die Möglichkeit, den Personenbezug vor der Verarbeitung zu eliminieren oder zumindest teilweise zu bereinigen?

→ Schwellwertanalyse: Muss in der konkreten Verarbeitungssituation eine Datenschutz-Folgenabschätzung durchgeführt werden?

→ Wie wird ein „akzeptables" Maß an Restrisiken nachgewiesen (Metrik)?

2. **Risikoabhängige Festlegung der Protokollierung von Ein- und Ausgabedaten und Absicherung der Protokolldaten (inkl. Pseudonymisierung)**

3. **Prüfung der formalen datenschutzrechtlichen Aspekte**

→ Wer ist Verantwortlicher? Gibt es gemeinsame Verantwortlichkeiten? Wer ist Auftragsverarbeiter? Welche Verträge müssen abgeschlossen werden?

→ Ist die Information der Betroffenen sichergestellt?

→ Werden automatisierte Einzelfallentscheidungen (einschließlich) „Profiling" getroffen, sodass den Betroffenen die „involvierte Logik" erläutert werden muss?

→ Besteht eine Legitimationsgrundlage für die Verarbeitung?

→ Können die Betroffenenrechte (Löschung, Auskunft etc.) erfüllt werden?

→ Welche technisch-organisatorischen Maßnahmen (Datensicherheit) sind notwendig?

→ Werden alle sonstigen relevanten datenschutzrechtliche Vorgaben erfüllt?

4. **Erarbeitung interner Vorgaben (Berechtigungskonzept, Einsatzziele und Ergebnisverwendung, Verhaltensregeln etc.)**

5. **Erarbeitung interner Dokumentation (einschließlich der Dimensionen Fairness, Autonomie und Kontrolle, Transparenz, Verlässlichkeit, Sicherheit, formaler Datenschutz)**

6. **Formale Dokumentation (Verzeichnis der Verarbeitungstätigkeiten etc.)**

7. **Periodische und anlassbezogene Aktualisierung der Risikoanalyse und ggf. Nachschärfen der Prozesse / Dokumentation**

wts PSP MÜNCHEN

Kontakt
Dr. Axel-Michael Wagner
a.wagner@psp.eu