Wolff Applied AI
APPLIED ARTIFICIAL INTELLIGENCE

A-02

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO

Version 1.0 · Stand 06.07.2026

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO, die der Ingenieurbüro Wolff, Inhaber Patrick Wolff (Marke „Wolff Applied AI“) zum Schutz personenbezogener Daten trifft. Der Anbieter ist ein Einzelunternehmen ohne angestelltes Personal; die Verarbeitung erfolgt in einer überwiegend cloudbasierten Microsoft-365-Umgebung mit Datenhaltung in der EU. Die Maßnahmen sind auf diese Struktur eines Solo-Beraters zugeschnitten und werden regelmäßig überprüft und an den Stand der Technik angepasst.

1. Zutritts- und Zugangskontrolle

Ziel ist es, Unbefugten den physischen Zutritt zu Arbeitsmitteln und den logischen Zugang zu Systemen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

- Arbeit in nicht öffentlich zugänglichen, abschließbaren Räumlichkeiten.
- Verschlüsselung aller Endgeräte mittels Geräteverschlüsselung (BitLocker bzw. gleichwertig).
- Automatische Bildschirmsperre bei Inaktivität sowie manuelle Sperre beim Verlassen des Arbeitsplatzes.
- Anmeldung an Geräten und Diensten mit starken, individuellen Passwörtern und Mehr-Faktor-Authentifizierung (MFA), insbesondere für Microsoft 365.
- Keine dauerhafte Speicherung von Zugangsdaten im Klartext; Einsatz eines Passwortmanagers.

2. Zugriffskontrolle

Ziel ist es sicherzustellen, dass nur berechtigte Personen ausschließlich auf die ihrer Berechtigung unterliegenden Daten zugreifen können.

- Zugriff auf personenbezogene Daten ausschließlich durch den Inhaber im erforderlichen Umfang (Grundsatz der Erforderlichkeit).
- Rollen- und rechtebasierte Freigaben in Microsoft 365 / SharePoint / OneDrive; restriktive Vergabe von Freigabelinks.
- Trennung privater und geschäftlicher Nutzung; verschlüsselte Ablage geschäftlicher Daten.

- Kontrollierte Löschung nicht mehr benötigter Daten.

3. Weitergabe- und Transportkontrolle

Ziel ist der Schutz personenbezogener Daten bei elektronischer Übertragung, während des Transports und bei der Speicherung auf Datenträgern.

- Transportverschlüsselung (TLS/HTTPS) bei der Übertragung von Daten und beim Zugriff auf Cloud-Dienste.
- Verschlüsselte Ablage in OneDrive/SharePoint mit Serverstandort in der EU.
- Für vertrauliche Inhalte werden bei Bedarf verschlüsselte Übermittlungswege oder passwortgeschützte Dateien vereinbart, da E-Mail-Transport nicht durchgehend Ende-zu-Ende-verschlüsselt ist.
- Keine Speicherung personenbezogener Kundendaten auf ungeschützten mobilen Datenträgern.

4. Eingabekontrolle

Ziel ist die Nachvollziehbarkeit, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.

- Nutzung der Protokollierungs- und Versionsfunktionen von Microsoft 365 (Aktivitäts- und Versionsverlauf in SharePoint/OneDrive).
- Da die Verarbeitung durch eine einzelne Person erfolgt, ist die Zuordnung von Eingaben eindeutig; systemseitige Protokolle dokumentieren wesentliche Änderungen.
- Aufbewahrung von E-Mail- und Dokumentenständen zur Nachvollziehbarkeit von Weisungen.

5. Auftragskontrolle

Ziel ist, dass im Auftrag verarbeitete Daten nur weisungsgemäß und durch sorgfältig ausgewählte Dienstleister verarbeitet werden.

- Sorgfältige Auswahl von Unterauftragsverarbeitern nach Datenschutz- und Sicherheitsniveau.
- Abschluss von Verträgen zur Auftragsverarbeitung (Art. 28 DSGVO) mit eingesetzten Dienstleistern (u. a. Microsoft 365, IONOS SE).
- Bevorzugung von Anbietern mit EU-Datenverarbeitung und anerkannten Zertifizierungen.
- Verarbeitung von Kundendaten ausschließlich nach den dokumentierten Weisungen des Auftraggebers.

6. Verfügbarkeitskontrolle und Belastbarkeit

Ziel ist der Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust sowie die rasche Wiederherstellbarkeit.

- Regelmäßige, automatisierte Sicherung (Backup) der Daten über die Cloud-Infrastruktur.
- Versionierung von Dokumenten und Papierkorb-/Wiederherstellungsfunktionen in Microsoft 365.
- Aktueller Virenschutz und zeitnahe Installation von Sicherheitsupdates.

- Nutzung der Redundanz- und Verfügbarkeitsmechanismen der eingesetzten EU-Rechenzentren.

7. Trennungskontrolle

Ziel ist, dass zu unterschiedlichen Zwecken oder für unterschiedliche Auftraggeber erhobene Daten getrennt verarbeitet werden.

- Getrennte Ablagestruktur je Mandant/Kunde (eigene Ordner-/Bibliotheksstruktur).
- Logische Trennung von Projekt-, Verwaltungs- und Übungsdaten.
- Keine Vermischung von Kundendaten unterschiedlicher Auftraggeber in gemeinsamen Dateien.

8. Besondere Maßnahmen beim Einsatz von KI-Diensten

Aufgrund des Tätigkeitsschwerpunkts im Bereich Künstlicher Intelligenz gelten für den Einsatz von KI-Diensten besondere Schutzmaßnahmen.

- Keine Eingabe personenbezogener oder vertraulicher Kundendaten in öffentliche KI-Dienste ohne vorherige Freigabe des Auftraggebers und – soweit erforderlich – ohne Auftragsverarbeitungsvertrag.
- Pseudonymisierung bzw. Anonymisierung von Daten in Schulungen, Übungen und Demonstrationen.
- Bevorzugung von KI-Diensten mit EU-Datenresidenz sowie mit vertraglich ausgeschlossenem Training auf Kundendaten.
- Bewusste Auswahl und Dokumentation der eingesetzten KI-Dienste je Auftrag.

9. Datenschutzfreundliche Voreinstellungen und Überprüfung

Der Anbieter berücksichtigt die Grundsätze Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO). Datensparsamkeit ist Leitprinzip: Es werden nur die für den jeweiligen Zweck erforderlichen Daten erhoben und verarbeitet.

Die vorstehenden Maßnahmen werden regelmäßig sowie anlassbezogen überprüft und an Veränderungen der Technik, der Rechtslage und der Auftragslage angepasst.

Diese Maßnahmenbeschreibung ist Anlage zu Verträgen zur Auftragsverarbeitung (Dokument A-03). Stand: 06.07.2026 (Version 1.0).