Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO für den PII-Pseudonymisierungsdienst

Stand: 06.11.2026 · Version 1.5

§ 1 Vertragsparteien

Verantwortlicher (Auftraggeber): Der Nutzer des PII-Pseudonymisierungsdienstes (nachfolgend „Auftraggeber")

Auftragsverarbeiter:
Michael SCHILLER - Organisation. Digital.
Speicherstraße 33, 44147 Dortmund
info@schiller-partners.de
Michael Schiller (Geschäftsführer)

§ 2 Gegenstand und Dauer der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen des PII-Pseudonymisierungsdienstes.

- **Zweck:** Automatisierte Erkennung und Pseudonymisierung personenbezogener Daten in Texten, bevor diese an KI-Sprachmodelle (LLMs) übermittelt werden.
- **Dauer:** Texte werden nur für die Dauer des einzelnen API-Aufrufs verarbeitet und nicht gespeichert (Ausnahme: nächtliche Prüfung, § 5). Zuordnungstabellen werden im Arbeitsspeicher gehalten und 30 Minuten nach der letzten Nutzung, spätestens 8 Stunden nach der ersten Nutzung, automatisch gelöscht.
- **Art der Verarbeitung:** Automatisierte Texterkennung, Musterabgleich (Pattern Matching), KI-basierte Named Entity Recognition, Pseudonymisierung in zwei Modi: **Tagged-Modus** für API-Outputs (eindeutig erkennbare Marker wie [PERSON:abc12345]) und **Faker-Modus** für interne KI-Pipelines (plausible Pseudonyme; serverseitige Reverse-Resolution vor Auslieferung an Endnutzer). In beiden Modi verlassen erkannte Original-Daten den Verarbeitungsprozess weder als Klartext zu Cloud-KI-Diensten noch zu externen Konsumenten.

§ 3 Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten können im Rahmen der Verarbeitung betroffen sein:

- Vollständige Namen, Vor- und Nachnamen
- E-Mail-Adressen, Telefonnummern
- Postadressen (Straße, PLZ, Stadt)
- IBANs, Kreditkartennummern, Kryptowährungs-Wallets
- Personalausweisnummern, Steuernummern, Sozialversicherungsnummern (EU-weit)
- Geburtsdaten
- IP-Adressen
- Profil-URLs auf Social-Media- und Entwicklerplattformen (35+ Plattformen, nur Username-Teil)

§ 4 Kategorien betroffener Personen

Betroffene Personen sind diejenigen natürlichen Personen, deren personenbezogene Daten in den vom Auftraggeber übermittelten Texten enthalten sind. Dies können insbesondere sein:

- Mitarbeiter und Beschäftigte des Auftraggebers
- Kunden und Geschäftspartner des Auftraggebers
- Kontaktpersonen und Ansprechpartner
- Sonstige in Texten erwähnte natürliche Personen

§ 5 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

- **Weisungsgebundenheit:** Die Verarbeitung erfolgt ausschließlich auf Grundlage der dokumentierten Weisungen des Auftraggebers. Die Nutzung der API stellt eine solche Weisung dar.
- **Vertraulichkeit:** Alle mit der Verarbeitung betrauten Personen sind zur Vertraulichkeit verpflichtet.
- **Sicherheit der Verarbeitung:** Der Auftragsverarbeiter trifft die in der Anlage TOM beschriebenen technisch-organisatorischen Maßnahmen (Art. 32 DSGVO).
- **Unterauftragsverarbeiter:** Der Dienst läuft auf gemieteten Servern der dataforest GmbH in Frankfurt am Main. Die dataforest GmbH sitzt in der Taunusstraße 52, 65830 Kriftel (auch unter der Marke PHP-Friends). Weil dort die Texte während der Verarbeitung liegen, ist die dataforest GmbH Unterauftragsverarbeiter. Weitere Unterauftragsverarbeiter setzt der Dienst nicht ein: Er legt keine Dateien ab und versendet keine E-Mails. Texte gibt er nicht an andere Dienste weiter. Ausnahme ist die nächtliche Prüfung: Aufrufe mit

einem Schlüssel, den der Betreiber dafür freigegeben hat, werden mit ihrem pseudonymisierten Text bis zu 48 Stunden verschlüsselt gespeichert (bei einem gemeldeten Fund bis zu 30 Tage) und auf gemieteten GPU-Servern der IONOS SE in Frankfurt am Main auf übersehene Angaben geprüft. Dafür ist die IONOS SE Unterauftragsverarbeiter. Aufrufe ohne Schlüssel oder mit einem nicht freigegebenen Schlüssel sind davon ausgenommen. Über eine beabsichtigte Änderung informiert der Auftragsverarbeiter den Auftraggeber vorab, der Auftraggeber kann ihr widersprechen.

- **Unterstützung:** Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten nach Art. 32-36 DSGVO.
- **Löschung:** Originaltexte werden nicht gespeichert. Zuordnungstabellen werden 30 Minuten nach der letzten Nutzung, spätestens 8 Stunden nach der ersten Nutzung, automatisch gelöscht. Protokolleinträge ohne Klartext werden je nach Prüfergebnis gelöscht: Aufrufe ohne freigegebenen Schlüssel nach 7 Tagen, sonst nach 30 Tagen (unauffällig), 90 Tagen (Fehler, Fehlalarme) oder 3 Jahren (übersehene Angaben). Texte der nächtlichen Prüfung werden nach spätestens 48 Stunden gelöscht, bei einem gemeldeten Fund nach 30 Tagen.
- **Nachweispflicht:** Der Auftragsverarbeiter stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung.

§ 6 Pflichten des Auftraggebers

Der Auftraggeber ist dafür verantwortlich, dass:

- die Übermittlung der personenbezogenen Daten an den Auftragsverarbeiter rechtmäßig erfolgt
- die Rechte der betroffenen Personen gewährleistet sind
- der Dienst nur für Texte genutzt wird, deren Verarbeitung der Auftraggeber verantworten darf

§ 7 Technisch-organisatorische Maßnahmen

Die konkreten technisch-organisatorischen Maßnahmen sind in einem separaten TOM-Dokument beschrieben:

→ TOM-Dokument anzeigen

Zusammenfassung der wichtigsten Maßnahmen:

- **Verschlüsselung und Zugriff:** TLS für alle Übertragungen. Die Session-ID vergibt und signiert der Dienst oder sie ist an den API-Schlüssel gebunden.
- **Lokale Verarbeitung:** Alle Server in Deutschland, kein Datentransfer in Drittländer, außer bei der nächtlichen Prüfung (§ 5, § 8)
- **Datenminimierung:** Keine Speicherung von Originaltexten, Zuordnungstabellen nur im Arbeitsspeicher ohne Kopie auf der Festplatte
- **Keine Klartext-Logs:** Protokolliert werden Zeitpunkt, eine gehashte Sitzungskennung, die Zahl der erkannten Angaben und Prüfsummen mit geheimem Schlüssel (HMAC-SHA256) der erkannten Werte, je nach Prüfergebnis 7 Tage bis 3 Jahre (§ 5)
- **Automatische Löschung:** Zuordnungstabellen 30 Minuten nach der letzten Nutzung, spätestens 8 Stunden nach der ersten Nutzung

§ 8 Datenübermittlung in Drittländer

Eine Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen findet nicht statt. Die Verarbeitung erfolgt ausschließlich auf Servern in Deutschland. Die eingesetzten KI-Modelle (GLiNER NER, PII-spezialisiert) laufen lokal auf denselben Servern.

§ 9 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich über jede Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO. Kontakt: info@schiller-partners.de

§ 10 Beendigung

Nach Beendigung der Nutzung des Dienstes werden alle temporären Daten automatisch gelöscht. Da Zuordnungstabellen 30 Minuten nach der letzten Nutzung, spätestens 8 Stunden nach der ersten Nutzung, und Protokolleinträge ohne Klartext nach den in § 5 genannten Fristen gelöscht werden, entfällt eine gesonderte Lösch- oder Rückgabepflicht.

§ 11 Haftung

Die Haftung richtet sich nach Art. 82 DSGVO. Der Auftragsverarbeiter haftet für Schäden, die durch eine nicht den Weisungen des Auftraggebers entsprechende Verarbeitung oder durch Verstöße gegen seine Pflichten aus diesem Vertrag entstehen.

§ 12 Schlussbestimmungen

- Es gilt deutsches Recht.
- Gerichtsstand ist Dortmund.
- Änderungen und Ergänzungen bedürfen der Schriftform.
- Dieser AVV tritt mit der ersten Nutzung des PII-Pseudonymisierungsdienstes durch den Auftraggeber in Kraft.

Unterschriften

Auftragsverarbeiter:

Michael SCHILLER - Organisation. Digital.
Michael Schiller (Geschäftsführer)

Ort, Datum

Unterschrift

Auftraggeber:

Firma / Name

Ort, Datum

Unterschrift

Dieser AVV gilt als angenommen mit der Nutzung des PII-Pseudonymisierungsdienstes (API-Aufruf). Eine separate Unterschrift ist nicht erforderlich.

Anlage: Technisch-organisatorische Maßnahmen (TOM)

Die detaillierten technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind im separaten TOM-Dokument beschrieben.