

# AUFTRAGSVERARBEITUNGSVERTRAG

Auftragsverarbeitungsvertrag (AVV)

zwischen

**INTECH Automation & Intelligence GmbH**

empowergpt.ai · Auftragsverarbeiter

und

**[NAME DES KUNDENUNTERNEHMENS]**

[Anschrift des Kunden] · Verantwortlicher

Dokumentenversion  
v2.2 (2026)

Inkrafttretensdatum  
[ ]

Regulatorische Grundlage  
DSGVO (EU) 2016/679

**VERTRAULICH — NICHT ZUR WEITERGABE BESTIMMT**

## Präambel

Dieser Auftragsverarbeitungsvertrag („AVV“ oder „Vertrag“) wird zwischen der INTECH Automation & Intelligence GmbH („Auftragsverarbeiter“ oder „INTECH Automation & Intelligence“) und der in Anlage I als Verantwortlicher bezeichneten Stelle („Verantwortlicher“ oder „Kunde“) – jeweils eine „Partei“ und gemeinsam die „Parteien“ – geschlossen.

Dieser AVV ist integraler Bestandteil des Master Services Agreement („MSA“) oder des Abonnementvertrags zwischen den Parteien, der die Nutzung der Plattform von INTECH Automation & Intelligence sowie der damit verbundenen Dienste („Dienste“) durch den Verantwortlichen regelt. Im Falle eines Widerspruchs zwischen diesem AVV und dem MSA in datenschutzrechtlichen Belangen hat dieser AVV Vorrang.

Dieser AVV ist darauf ausgerichtet, der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (die „DSGVO“) zu entsprechen, einschließlich aller einschlägigen nationalen Umsetzungsvorschriften und nachfolgender Regelungen. Die hierin enthaltene Struktur und die hierin festgelegten Pflichten spiegeln die im KI-Unternehmenssektor etablierten Best Practices wider und stehen im Einklang mit den Leitlinien des Europäischen Datenschutzausschusses („EDSA“).

Die Parteien erkennen an, dass INTECH Automation & Intelligence eine KI-gestützte Unternehmensplattform betreibt, die personenbezogene Daten verarbeiten kann, welche vom Verantwortlichen oder seinen autorisierten Nutzern während der bestimmungsgemäßen Nutzung der Dienste übermittelt werden. Zweck und Art der Verarbeitung sind in Anlage I beschrieben.

---

## 1. Begriffsbestimmungen und Auslegung

1.1 In diesem AVV haben die nachstehenden Begriffe die ihnen jeweils zugewiesene Bedeutung. Großgeschriebene Begriffe, die hierin nicht definiert sind, haben die ihnen in der DSGVO oder im MSA zugeschriebene Bedeutung.

Begriff	Definition
„Anwendbares Datenschutzrecht“	Die DSGVO sowie alle anwendbaren nationalen Datenschutzgesetze der EU-/EWR-Mitgliedstaaten, die UK-DSGVO, das schweizerische Bundesgesetz über den Datenschutz (revDSG) – soweit anwendbar – sowie alle nachfolgenden oder ergänzenden Rechtsvorschriften.
„Verantwortlicher“	Die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DSGVO).
„Betroffene Person“	Eine identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten im Rahmen dieses AVV verarbeitet werden (Art. 4 Nr. 1 DSGVO).
„EWR“	Der Europäische Wirtschaftsraum, bestehend aus den EU-Mitgliedstaaten sowie Island, Liechtenstein und Norwegen.
„Personenbezogene Daten“	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wie in Art. 4 Nr. 1 DSGVO definiert.
„Verletzung des Schutzes personenbezogener Daten“	Eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt (Art. 4 Nr. 12 DSGVO).
„Auftragsverarbeiter“	Eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO).

„Verarbeitung“	Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten, einschließlich Erhebung, Speicherung, Verwendung, Offenlegung oder Löschung (Art. 4 Nr. 2 DSGVO).
„Beschränkte Übermittlung“	Eine Übermittlung personenbezogener Daten in ein Drittland, dem nach Kapitel V DSGVO kein angemessenes Schutzniveau zuerkannt wurde.
„SCCs“ (Standardvertragsklauseln)	Die von der Europäischen Kommission gemäß Art. 46 Abs. 2 DSGVO erlassenen Standardvertragsklauseln.
„Dienste“	Die KI-Unternehmensplattform von INTECH Automation & Intelligence sowie sämtliche damit verbundene Dienste, wie sie im MSA beschrieben sind.
„Besondere Kategorien personenbezogener Daten“	Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung (Art. 9 Abs. 1 DSGVO).
„Unterauftragsverarbeiter“	Jeder dritte Auftragsverarbeiter, der von INTECH Automation & Intelligence zur Durchführung von Verarbeitungstätigkeiten im Auftrag des Verantwortlichen herangezogen wird (Art. 28 Abs. 4 DSGVO).
„TOMs“	Technische und organisatorische Maßnahmen, die zur Gewährleistung der Sicherheit personenbezogener Daten ergriffen werden (Art. 32 DSGVO).

## 2. Anwendungsbereich und Rolle der Parteien

2.1 Rollen. Der Verantwortliche bestimmt die Zwecke und Mittel der Verarbeitung personenbezogener Daten, die an die Dienste übermittelt werden. INTECH Automation & Intelligence handelt in Bezug auf personenbezogene Daten, die im Rahmen der Dienste im Auftrag des Verantwortlichen verarbeitet werden, gemäß Art. 28 DSGVO als Auftragsverarbeiter.

2.2 Weisungen. INTECH Automation & Intelligence verarbeitet personenbezogene Daten ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen, zu denen gehören: (a) dieser AVV; (b) der MSA; (c) die Konfiguration und Einstellungen der Dienste; sowie (d) sämtliche zusätzlichen schriftlichen Weisungen, die von den Parteien vereinbart wurden. Eine Verarbeitung zu anderen Zwecken bedarf der vorherigen schriftlichen Zustimmung.

2.3 Unzulässige Weisungen. Ist INTECH Automation & Intelligence der Auffassung, dass eine Weisung gegen anwendbares Datenschutzrecht verstößt, so teilt sie dies dem Verantwortlichen unverzüglich mit. INTECH Automation & Intelligence ist nicht verpflichtet, Weisungen zu befolgen, die einen Rechtsverstoß zur Folge hätten.

2.4 Pflichten des Verantwortlichen. Der Verantwortliche sichert zu und versichert, dass: (a) er über eine gültige Rechtsgrundlage für jede Verarbeitung personenbezogener Daten verfügt, mit deren Durchführung er INTECH Automation & Intelligence beauftragt; (b) er sämtliche erforderlichen Informationen gegenüber den betroffenen Personen erteilt hat; (c) er keine besonderen Kategorien personenbezogener Daten hochlädt, sofern kein gesonderter schriftlicher Nachtrag abgeschlossen wurde; und (d) er die Dienste in Übereinstimmung mit dem anwendbaren Datenschutzrecht nutzen wird.

2.5 Anwendungsbereich dieses AVV. Dieser AVV gilt für sämtliche Verarbeitungen personenbezogener Daten, die INTECH Automation & Intelligence als Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit den Diensten durchführt. Er gilt nicht für Verarbeitungen, in deren Rahmen INTECH Automation & Intelligence als eigenständig Verantwortliche handelt (z. B. Kontoverwaltung, Rechnungsstellung, Rechtspflichten).

## 3. Pflichten des Auftragsverarbeiters

### 3.1 Allgemeine Pflichten

INTECH Automation & Intelligence verpflichtet sich in Bezug auf personenbezogene Daten, die im Auftrag des Verantwortlichen verarbeitet werden:

- personenbezogene Daten ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen zu verarbeiten, sofern die Verarbeitung nicht nach dem Recht der Union oder eines Mitgliedstaats, dem INTECH Automation & Intelligence unterliegt, erforderlich ist (Art. 28 Abs. 3 Buchst. a);
- sicherzustellen, dass sich zur Verarbeitung personenbezogener Daten befugte Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Buchst. b);
- geeignete technische und organisatorische Maßnahmen gemäß Abschnitt 5 und Anlage II dieses AVV zu ergreifen und aufrechtzuerhalten (Art. 28 Abs. 3 Buchst. c, Art. 32);
- die in Abschnitt 7 dieses AVV festgelegten Bedingungen für die Heranziehung von Unterauftragsverarbeitern einzuhalten (Art. 28 Abs. 3 Buchst. d);
- den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Ausübung ihrer Rechte zu unterstützen (Art. 28 Abs. 3 Buchst. e);
- den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß Art. 32 bis Art. 36 DSGVO (Sicherheit, Meldung von Verletzungen, DSFAs, vorherige Konsultation) zu unterstützen (Art. 28 Abs. 3 Buchst. f);
- nach Wahl des Verantwortlichen sämtliche personenbezogene Daten nach Beendigung der Dienste zu löschen oder zurückzugeben und bestehende Kopien zu vernichten, sofern keine Verpflichtung nach Unions- oder Mitgliedstaatenrecht zur Speicherung besteht (Art. 28 Abs. 3 Buchst. g);
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO zur Verfügung zu stellen sowie Überprüfungen, einschließlich Inspektionen, zu ermöglichen und zu diesen beizutragen (Art. 28 Abs. 3 Buchst. h).

## 4. Rechte der betroffenen Personen

4.1 Unterstützung bei der Wahrnehmung von Rechten. INTECH Automation & Intelligence unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung bei der Erfüllung seiner Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte nach Kapitel III DSGVO zu beantworten, einschließlich der Rechte auf: Auskunft (Art. 15); Berichtigung (Art. 16); Löschung / Recht auf Vergessenwerden (Art. 17); Einschränkung der Verarbeitung (Art. 18); Datenübertragbarkeit (Art. 20); Widerspruch (Art. 21); und Rechte im Zusammenhang mit automatisierten Entscheidungen (Art. 22).

4.2 Fristen. Geht ein Antrag einer betroffenen Person unmittelbar bei INTECH Automation & Intelligence ein, so: (a) leitet INTECH Automation & Intelligence diesen Antrag unverzüglich, in jedem Fall jedoch innerhalb von drei (3) Werktagen, an den Verantwortlichen weiter; und (b) antwortet INTECH Automation & Intelligence nicht unmittelbar gegenüber der betroffenen Person, sofern nicht eine schriftliche Befugnis des Verantwortlichen oder eine gesetzliche Verpflichtung besteht.

4.3 Technische Maßnahmen. INTECH Automation & Intelligence hält technische Fähigkeiten vor, die es dem Verantwortlichen ermöglichen: (a) personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu exportieren (Art. 20); (b) bestimmte Nutzer-Datensätze auf Anfrage zu löschen oder zu anonymisieren; (c) die Verarbeitung für bestimmte Nutzer oder Kategorien einzuschränken; und (d) betroffenen Personen eine Kopie ihrer Daten zur Verfügung zu stellen.

4.4 Kosten. Die Unterstützung von INTECH Automation & Intelligence bei Anträgen auf Wahrnehmung von Rechten der betroffenen Personen ist in der Vergütung für die Dienste enthalten. Sind Anträge offenkundig unbegründet oder exzessiv, so kann INTECH Automation & Intelligence – vorbehaltlich vorheriger schriftlicher Mitteilung und Einigung – angemessene Kosten für außergewöhnlichen Aufwand in Rechnung stellen.

4.5 Keine eigenständige Entscheidung. INTECH Automation & Intelligence trifft keine Entscheidungen im Namen des Verantwortlichen darüber, ob den Rechten einer betroffenen Person stattzugeben ist oder diese abzulehnen sind. Eine solche Entscheidung obliegt ausschließlich dem Verantwortlichen.

---

## 5. Sicherheit der Verarbeitung

5.1 Allgemeine Sicherheitspflicht. INTECH Automation & Intelligence ergreift geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei werden der Stand der Technik, die Implementierungskosten sowie die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt (Art. 32 Abs. 1 DSGVO).

5.2 Konkrete Maßnahmen. Unbeschadet der Allgemeingültigkeit von Ziffer 5.1 ergreift INTECH Automation & Intelligence die in Anlage II zu diesem AVV beschriebenen Maßnahmen, zu denen mindestens gehören:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 Buchst. a);
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste auf Dauer sicherzustellen (Art. 32 Abs. 1 Buchst. b);
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Vorfall rasch wiederherzustellen (Art. 32 Abs. 1 Buchst. c);
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 Buchst. d).

5.3 Sicherheitsüberprüfungen. INTECH Automation & Intelligence überprüft und aktualisiert ihre Sicherheitsmaßnahmen regelmäßig, um Veränderungen hinsichtlich der Risiken, der Technologie und der bewährten Praxis Rechnung zu tragen. INTECH Automation & Intelligence unterhält einschlägige Sicherheitszertifizierungen (einschließlich ISO 27001 und SOC 2 Typ II) und stellt dem Verantwortlichen auf Anfrage Kopien der Zertifikate oder einschlägiger Auditberichte zur Verfügung.

5.4 Mandantentrennung. INTECH Automation & Intelligence stellt eine strikte logische Trennung zwischen den Daten des Verantwortlichen und den Daten anderer Kunden sicher. Die personenbezogenen Daten des Verantwortlichen sind für keinen anderen Kunden von INTECH Automation & Intelligence zugänglich.

5.5 KI-spezifische Sicherheit. Im Zusammenhang mit der KI-Verarbeitung gilt: (a) Die Daten des Verantwortlichen werden ohne ausdrückliche schriftliche Zustimmung nicht zum Training von KI-Grundmodellen verwendet; (b) Modellausgaben, die personenbezogene Daten enthalten, unterliegen Filtermechanismen; (c) Schutzmaßnahmen gegen Prompt Injection und gegen feindliche Eingaben werden aufrechterhalten; und (d) der Zugriff der Modelle auf personenbezogene Daten ist auf das für die Erbringung der Dienste streng erforderliche Maß beschränkt.

---

## 6. Meldung von Verletzungen des Schutzes personenbezogener Daten

6.1 Erkennung und Bewertung. INTECH Automation & Intelligence hält Verfahren zur Erkennung, Bewertung und Reaktion auf Verletzungen des Schutzes personenbezogener Daten vor. INTECH Automation & Intelligence hält Fähigkeiten zur Reaktion auf Sicherheitsvorfälle vor, wie sie in Anlage II näher beschrieben sind.

6.2 Mitteilung an den Verantwortlichen. INTECH Automation & Intelligence unterrichtet den Verantwortlichen unverzüglich, sofern dies durchführbar ist innerhalb von 36 Stunden, nachdem ihr eine bestätigte Verletzung des Schutzes personenbezogener Daten bekannt geworden ist. Die Mitteilung enthält, soweit bekannt:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und ungefähren Zahl der betroffenen Personen sowie der Kategorien und ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Anlaufstelle, bei der weitere Informationen erlangt werden können;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung, gegebenenfalls einschließlich Maßnahmen zur Abmilderung möglicher nachteiliger Folgen.

6.4 Zusammenarbeit. INTECH Automation & Intelligence arbeitet vollumfänglich mit dem Verantwortlichen zusammen, um diesen bei der Erfüllung seiner Meldepflichten gegenüber den Aufsichtsbehörden (Art. 33 DSGVO) und gegenüber den betroffenen Personen (Art. 34 DSGVO) zu unterstützen. INTECH Automation & Intelligence informiert weder betroffene Personen noch Aufsichtsbehörden über eine Verletzung des Schutzes personenbezogener Daten ohne vorherige schriftliche Zustimmung des Verantwortlichen, sofern nicht eine entsprechende gesetzliche Verpflichtung besteht.

## 7. Unterauftragsverarbeiter

7.1 Allgemeine Genehmigung. Der Verantwortliche erteilt INTECH Automation & Intelligence hiermit die allgemeine schriftliche Genehmigung zur Heranziehung von Unterauftragsverarbeitern vorbehaltlich der Bedingungen dieses Abschnitts 7. Die aktuelle Liste der Unterauftragsverarbeiter ist in Anlage III aufgeführt.

7.2 Anforderungen an Unterauftragsverarbeiter. INTECH Automation & Intelligence wird vor der Heranziehung eines Unterauftragsverarbeiters:

- eine geeignete Sorgfaltsprüfung hinsichtlich der Fähigkeit des Unterauftragsverarbeiters durchführen, den erforderlichen Schutz personenbezogener Daten zu gewährleisten;
- jeden Unterauftragsverarbeiter durch schriftlichen Vertrag denselben Datenschutzpflichten unterwerfen, denen INTECH Automation & Intelligence nach diesem AVV unterliegt, insbesondere die Verpflichtung, hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen zu bieten, sodass die Verarbeitung den Anforderungen des Art. 28 Abs. 4 DSGVO entspricht;
- sicherstellen, dass Verträge mit Unterauftragsverarbeitern Auditrechte, Sicherheitsanforderungen, Beschränkungen der Weiterbeauftragung, Vertraulichkeitspflichten und die Kooperation bei Rechten betroffener Personen enthalten.

7.3 Neue Unterauftragsverarbeiter. INTECH Automation & Intelligence informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern, indem sie: (a) eine aktualisierte Anlage III im Trust Center von INTECH Automation & Intelligence ([trust.empowergpt.ai](https://trust.empowergpt.ai)) veröffentlicht; und (b) den vom Verantwortlichen benannten Datenschutz-Ansprechpartner mindestens 30 Kalendertage im Voraus per individueller E-Mail benachrichtigt („Mitteilungsfrist“).

7.4 Widerspruchsrecht. Während der Mitteilungsfrist kann der Verantwortliche aus angemessenen datenschutzbezogenen Gründen Widerspruch gegen den neuen Unterauftragsverarbeiter einlegen. Die Parteien bemühen sich in gutem Glauben, den Widerspruch des Verantwortlichen zu klären. Können die Parteien den

Widerspruch nicht innerhalb von 15 Tagen nach Eingang klären, so kann der Verantwortliche die betroffenen Dienste innerhalb von 30 Tagen nach der Mitteilung durch INTECH Automation & Intelligence durch schriftliche Erklärung ohne Vertragsstrafe kündigen.

7.5 Haftung. INTECH Automation & Intelligence bleibt dem Verantwortlichen gegenüber für die Erfüllung der Pflichten der Unterauftragsverarbeiter nach diesem AVV vollumfänglich verantwortlich. Erfüllt ein Unterauftragsverarbeiter seine Datenschutzpflichten nicht, so bleibt INTECH Automation & Intelligence gegenüber dem Verantwortlichen vollumfänglich haftbar (Art. 28 Abs. 4 DSGVO).

7.6 Beschränkung der LLM-Anbieter (KI-spezifische Klausel). In Anlage III aufgeführte Anbieter von Large Language Models (LLM) werden nur dann im Zusammenhang mit Daten des Verantwortlichen aktiviert und eingesetzt, wenn der Verantwortliche den jeweiligen LLM-Anbieter ausdrücklich in den Plattformkonfigurationseinstellungen oder durch schriftliche Vereinbarung ausgewählt bzw. aktiviert hat. INTECH Automation & Intelligence leitet personenbezogene Daten des Verantwortlichen an keinen vom Verantwortlichen nicht ausgewählten LLM-Anbieter weiter und stellt dem Verantwortlichen klare Steuerungsmöglichkeiten zum Aktivieren, Deaktivieren oder Wechseln zwischen LLM-Anbietern zur Verfügung. Jeder neu hinzukommende LLM-Anbieter unterliegt unabhängig vom Bestehen einer allgemeinen Genehmigung dem Mitteilungs- und Widerspruchsverfahren gemäß Ziffer 7.3 bis 7.4.

---

## 8. Internationale Datenübermittlungen

8.1 Allgemeine Beschränkung. INTECH Automation & Intelligence übermittelt personenbezogene Daten nicht in ein Drittland außerhalb des EWR, es sei denn:

- die Übermittlung erfolgt in ein Land, für das die Europäische Kommission gemäß Art. 45 DSGVO einen Angemessenheitsbeschluss erlassen hat;
- die Übermittlung unterliegt geeigneten Garantien gemäß Art. 46 DSGVO (z. B. Standardvertragsklauseln); oder
- eine konkrete Ausnahmeregelung nach Art. 49 DSGVO greift.

8.2 Standardvertragsklauseln. Werden SCCs als Übermittlungsmechanismus eingesetzt, so gilt: (a) INTECH Automation & Intelligence schließt mit den jeweiligen Unterauftragsverarbeitern das einschlägige Modul der SCCs nach dem Durchführungsbeschluss (EU) 2021/914 ab; (b) sofern der Verantwortliche der UK-DSGVO unterliegt, schließt INTECH Automation & Intelligence das UK International Data Transfer Agreement (IDTA) oder den Addendum zu den EU-SCCs ab, je nach Anwendbarkeit; und (c) Kopien der abgeschlossenen SCCs werden dem Verantwortlichen auf schriftliches Verlangen zur Verfügung gestellt.

## 9. Datenschutz-Folgenabschätzung und vorherige Konsultation

9.1 Unterstützung bei der DSFA. Unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen leistet INTECH Automation & Intelligence dem Verantwortlichen angemessene Unterstützung bei der Durchführung einer nach Art. 35 DSGVO erforderlichen Datenschutz-Folgenabschätzung.

9.2 Vorherige Konsultation. INTECH Automation & Intelligence unterstützt den Verantwortlichen bei der Durchführung einer nach Art. 36 DSGVO erforderlichen vorherigen Konsultation einer Aufsichtsbehörde.

## 10. Überprüfungen und Inspektionen

10.1 Auditrechte. INTECH Automation & Intelligence stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung ihrer Pflichten nach Art. 28 DSGVO erforderlich sind, und

ermöglicht Überprüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder einem von ihm beauftragten externen Prüfer durchgeführt werden, und trägt zu diesen bei.

10.2 Häufigkeit und Ankündigung von Überprüfungen. Überprüfungen werden höchstens einmal pro Kalenderjahr durchgeführt, es sei denn: (a) eine Verletzung des Schutzes personenbezogener Daten ist eingetreten; (b) eine Aufsichtsbehörde hat eine Untersuchung eingeleitet; oder (c) der Verantwortliche hat begründete, dokumentierte Anhaltspunkte für eine Nichteinhaltung. Der Verantwortliche teilt INTECH Automation & Intelligence eine Vor-Ort-Überprüfung mindestens 30 Werkzeuge im Voraus schriftlich an.

10.4 Zertifizierungen durch Dritte. INTECH Automation & Intelligence stellt dem Verantwortlichen jährlich sowie auf angemessene Anfrage aktuelle Kopien ihrer einschlägigen Sicherheitszertifikate und Auditberichte zur Verfügung, einschließlich des ISO-27001-Zertifikats, des SOC-2-Typ-II-Berichts sowie etwaiger DSGVO-Compliance-Bewertungen. Die Bereitstellung solcher Berichte erfüllt – sofern keine konkreten Bedenken bestehen – das Auditrecht des Verantwortlichen hinsichtlich der darin behandelten Aspekte.

## 11. Aufbewahrung und Löschung personenbezogener Daten

11.1 Aufbewahrungsrichtlinie. INTECH Automation & Intelligence bewahrt personenbezogene Daten nur so lange auf, wie dies zur Erbringung der Dienste oder nach geltendem Recht erforderlich ist. INTECH Automation & Intelligence bewahrt personenbezogene Daten ohne schriftliche Zustimmung des Verantwortlichen nicht über die Beendigung der jeweiligen Dienste hinaus auf, es sei denn, dies ist nach Unions- oder Mitgliedstaatenrecht erforderlich.

11.2 Rückgabe oder Löschung. Innerhalb von 30 Kalendertagen nach Beendigung oder Auslaufen des MSA (oder der jeweiligen Dienste) oder bei vorheriger schriftlicher Aufforderung des Verantwortlichen wird INTECH Automation & Intelligence nach Wahl des Verantwortlichen:

- dem Verantwortlichen sämtliche personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format (z. B. JSON oder CSV) zurückgeben; und/oder
- sämtliche personenbezogene Daten (sowie alle Kopien davon) in ihrem Besitz oder unter ihrer Kontrolle dauerhaft löschen oder vernichten, einschließlich der bei Unterauftragsverarbeitern verarbeiteten Daten.

11.3 Löschungsnachweis. Innerhalb von 14 Kalendertagen nach Abschluss der Löschung stellt INTECH Automation & Intelligence dem Verantwortlichen einen schriftlichen Löschungsnachweis zur Verfügung, in dem die angewandten Methoden konkret beschrieben werden und bestätigt wird, dass sämtliche personenbezogenen Daten – soweit technisch durchführbar – aus den Produktionssystemen, den Datensicherungen sowie den Systemen der Unterauftragsverarbeiter gelöscht wurden.

## 12. Haftung und Freistellung

12.1 Haftung des Verantwortlichen. Der Verantwortliche stellt INTECH Automation & Intelligence von sämtlichen Ansprüchen, Verbindlichkeiten, Bußgeldern, Sanktionen, Kosten und Aufwendungen frei, die entstehen aus: (a) einem Verstoß des Verantwortlichen gegen diesen AVV oder gegen anwendbares Datenschutzrecht; (b) rechtswidrigen Weisungen des Verantwortlichen; oder (c) der Nichterfüllung seiner Pflichten als Verantwortlicher nach der DSGVO.

12.2 Haftung des Auftragsverarbeiters. INTECH Automation & Intelligence haftet für Schäden, die durch eine Verarbeitung verursacht werden, mit der den speziell an Auftragsverarbeiter gerichteten Pflichten der DSGVO nicht nachgekommen wurde oder bei der außerhalb oder entgegen rechtmäßiger Weisungen des Verantwortlichen gehandelt wurde, jeweils gemäß Art. 82 DSGVO.

12.3 Haftungsbeschränkung. Vorbehaltlich des anwendbaren Rechts ist die Gesamthaftung von INTECH Automation & Intelligence aus diesem AVV (gleich ob aus Vertrag, unerlaubter Handlung oder anderweitig) auf

die Beträge begrenzt, die der Verantwortliche an INTECH Automation & Intelligence in den zwölf (12) Monaten vor dem Anspruch gezahlt hat, es sei denn, der Schaden beruht auf grober Fahrlässigkeit oder Vorsatz von INTECH Automation & Intelligence.

## 13. Laufzeit und Beendigung

13.1 Laufzeit. Dieser AVV tritt am Inkrafttretensdatum in Kraft und bleibt für die Dauer des MSA in Kraft, sofern er nicht zuvor nach diesem Abschnitt 13 gekündigt wird.

13.4 Fortgeltung. Folgende Pflichten gelten nach Beendigung dieses AVV fort: Vertraulichkeitspflichten (Abschnitt 3.4); Rückgabe- und Löschungspflichten (Abschnitt 11); Auditrechte hinsichtlich des Verarbeitungszeitraums (Abschnitt 10); Haftungsregelungen (Abschnitt 12); Verbot des KI-Trainings (Abschnitt 17); sowie das Verbot des Zugriffs außerhalb der EU/des EWR ohne Schutzmaßnahmen (Abschnitt 16.4) – jeweils für einen Zeitraum von drei (3) Jahren nach Beendigung, es sei denn, das anwendbare Recht erfordert einen längeren Zeitraum.

---

## 14. Anwendbares Recht und Gerichtsstand

14.1 Anwendbares Recht. Dieser AVV unterliegt dem Recht der Bundesrepublik Deutschland und ist nach diesem auszulegen; das internationale Privatrecht findet keine Anwendung.

14.2 Gerichtsstand. Die Parteien unterwerfen sich unwiderruflich der ausschließlichen Zuständigkeit der Gerichte in München, Deutschland, für die Beilegung sämtlicher Streitigkeiten, die sich aus oder im Zusammenhang mit diesem AVV ergeben. Unbeschadet des Vorstehenden kann jede Partei vor jedem zuständigen Gericht einstweiligen oder sonstigen Eilrechtsschutz beantragen.

14.3 DSGVO-Aufsichtsbehörde. Die nach Art. 56 DSGVO federführende Aufsichtsbehörde für INTECH Automation & Intelligence ist [das Bayerische Landesamt für Datenschutzaufsicht (BayLDA)]. Der Verantwortliche kann darüber hinaus Beschwerden bei seiner zuständigen örtlichen Aufsichtsbehörde einreichen.

---

## 15. Sonstige Bestimmungen

15.1 Gesamte Vereinbarung. Dieser AVV (zusammen mit den Anlagen und dem MSA) bildet die gesamte Vereinbarung zwischen den Parteien hinsichtlich der Verarbeitung personenbezogener Daten und ersetzt sämtliche vorherigen Absprachen, Erklärungen oder Vereinbarungen zu diesem Gegenstand.

15.2 Änderungen. Änderungen dieses AVV sind nur wirksam, wenn sie schriftlich erfolgen und von ordnungsgemäß bevollmächtigten Vertretern beider Parteien unterzeichnet werden. INTECH Automation & Intelligence kann diesen AVV einseitig aktualisieren, um Änderungen des anwendbaren Datenschutzrechts oder aufsichtsrechtlicher Leitlinien Rechnung zu tragen, sofern INTECH Automation & Intelligence dem Verantwortlichen mindestens 30 Kalendertage zuvor schriftlich Mitteilung macht und der Verantwortliche innerhalb dieses Zeitraums keinen Widerspruch erhebt.

15.3 Salvatorische Klausel. Sollte eine Bestimmung dieses AVV unwirksam, rechtswidrig oder nicht durchsetzbar sein, so bleiben die übrigen Bestimmungen in vollem Umfang wirksam. Die Parteien verhandeln in gutem Glauben über eine Ersetzung der unwirksamen Bestimmung durch eine wirksame Bestimmung, die wirtschaftlich und rechtlich der unwirksamen Bestimmung möglichst nahekommt.

15.5 Mitteilungen. Mitteilungen nach diesem AVV erfolgen schriftlich (einschließlich per E-Mail) an die in Anlage I genannten Ansprechpartner. Datenschutzbezogene Mitteilungen an INTECH Automation & Intelligence sind an [privacy@empowergpt.ai](mailto:privacy@empowergpt.ai) zu richten.

15.7 Sprache. Dieser AVV ist in deutscher Sprache abgefasst. Im Falle eines Widerspruchs zwischen einer Übersetzung und dem deutschen Text hat der deutsche Text Vorrang.

---

## 16. Protokolle, Zugriffskontrolle und Datentrennung

16.1 Protokollminimierung. INTECH Automation & Intelligence wendet den Grundsatz der Protokollminimierung an und erhebt und speichert ausschließlich diejenigen Protokolle, die für Sicherheitsüberwachung, Audit, Rechtspflichten und Dienstintegrität erforderlich sind. Protokolldaten werden nicht länger als erforderlich aufbewahrt und unterliegen definierten Aufbewahrungsplänen. Soweit technisch möglich, werden personenbezogene Daten in Protokollen pseudonymisiert oder anonymisiert.

16.3 Zugriffskontrollen auf Protokolle und Produktionsdaten. Der Zugriff auf Protokolle und Produktionsdaten, die personenbezogene Daten enthalten, wird:

- streng über die rollenbasierte Zugriffskontrolle (RBAC) nach dem Prinzip der geringsten Rechte beschränkt;
- ausschließlich Personal gewährt, das für legitime betriebliche, sicherheitsbezogene oder rechtliche Zwecke Zugriff benötigt;
- für sämtliche privilegierten Zugriffe der Mehrfaktor-Authentifizierung (MFA) unterworfen;
- über ein zentralisiertes SIEM-System protokolliert und überwacht, wobei auffällige Zugriffe automatisierte Alarmer auslösen;
- mindestens vierteljährlich überprüft, wobei Zugriffsrechte bei Rollenwechsel oder Ausscheiden unverzüglich entzogen werden.

16.4 Fern- und Zugriffe außerhalb der EU/des EWR. Der Zugriff auf personenbezogene Daten oder auf Systeme, die personenbezogene Daten verarbeiten, von außerhalb der EU/des EWR aus wird:

- streng begrenzt und ausschließlich dann gewährt, wenn er betrieblich erforderlich ist, sowie einer dokumentierten Begründung unterworfen;
- denselben oder gleichwertigen Schutzmaßnahmen wie der Zugriff innerhalb des EWR unterworfen, einschließlich Verschlüsselung, MFA und Auditprotokollierung;
- in einem Zugriffsprotokoll dokumentiert, das dem Verantwortlichen auf Anfrage zur Verfügung gestellt wird;
- soweit anwendbar als beschränkte Übermittlung behandelt und durch geeignete Übermittlungsmechanismen nach Abschnitt 8 dieses AVV geregelt.

16.5 Trennung der Mandantendaten. INTECH Automation & Intelligence implementiert eine strikte logische Trennung zwischen den personenbezogenen Daten verschiedener Kunden (Mandanten) durch Isolationsmaßnahmen auf Infrastruktur- und Anwendungsebene. Die personenbezogenen Daten des Verantwortlichen sind zu keinem Zeitpunkt anderen Kunden zugänglich oder mit deren Daten vermischt. Die Maßnahmen zur Datentrennung werden im Rahmen der jährlichen Sicherheitsbewertungen von INTECH Automation & Intelligence überprüft.

## 17. Verbot der Nutzung personenbezogener Daten für KI-Training und Modellverbesserung

17.1 **Absolutes Verbot.** INTECH Automation & Intelligence darf personenbezogene Daten, die im Auftrag des Verantwortlichen verarbeitet werden, unter keinen Umständen verwenden für:

- das Training, Fine-Tuning oder die anderweitige Verbesserung von künstlicher Intelligenz, Maschinellern Lernen oder Large Language Models (LLM), unabhängig davon, ob diese von INTECH Automation & Intelligence oder einem Dritten betrieben werden;
- die Erstellung, Entwicklung oder Verbesserung von Datensätzen, die für die KI- oder Modellentwicklung verwendet werden;
- das Benchmarking, die Evaluierung oder das Testen von KI-Modellen unter Verwendung identifizierbarer personenbezogener Daten;
- jeden anderen Zweck, der über die strikte Erbringung der in Anlage I und im MSA beschriebenen Dienste hinausgeht.

17.2 **Reichweite – Unterauftragsverarbeiter und LLM-Anbieter.** Das Verbot in Ziffer 17.1 gilt entsprechend für sämtliche Unterauftragsverarbeiter, einschließlich der LLM-API-Anbieter. INTECH Automation & Intelligence verpflichtet sämtliche Unterauftragsverarbeiter, einschließlich der LLM-Anbieter wie OpenAI und Anthropic, vertraglich zur Einhaltung desselben Verbots. INTECH Automation & Intelligence verifiziert bei Aufnahme der Beauftragung sowie mindestens jährlich, dass entsprechende vertragliche Verbote vorhanden und wirksam sind.

17.4 **Zustimmungsausnahme.** Ungeachtet der Ziffer 17.1 darf INTECH Automation & Intelligence personenbezogene Daten zur Verbesserung von KI-Modellen ausschließlich dann verwenden, wenn der Verantwortliche zuvor ausdrücklich, konkret und dokumentiert schriftlich zugestimmt hat, wobei der genaue Umfang, das Modell, der Zweck und die Dauer einer solchen Nutzung zu bestimmen sind. Eine solche Zustimmung kann der Verantwortliche jederzeit mit sofortiger Wirkung widerrufen.

## 18. Unterstützung bei der aufsichtsrechtlichen Compliance

18.1 **Allgemeine Unterstützungspflicht.** INTECH Automation & Intelligence leistet dem Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen sämtliche angemessene Unterstützung bei der Erfüllung seiner Pflichten nach anwendbarem Datenschutzrecht, die über die in den Abschnitten 4 (Rechte betroffener Personen), 6 (Meldung von Verletzungen) und 9 (DSFAs) dieses AVV behandelten konkreten Pflichten hinausgehen.

18.2 **Aufsichtsrechtliche Anfragen und Untersuchungen.** INTECH Automation & Intelligence unterrichtet den Verantwortlichen unverzüglich nach Erhalt einer Anfrage, eines Auskunftersuchens, einer Inspektion oder einer Untersuchung durch eine Datenschutz-Aufsichtsbehörde, die sich auf nach diesem AVV verarbeitete personenbezogene Daten bezieht. INTECH Automation & Intelligence wird:

- den Verantwortlichen innerhalb von drei (3) Werktagen nach Erhalt einer solchen Mitteilung unterrichten;
- mit dem Verantwortlichen bei der Vorbereitung einer abgestimmten Antwort zusammenarbeiten;
- ohne vorherige schriftliche Zustimmung des Verantwortlichen nicht eigenständig gegenüber einer Aufsichtsbehörde in Angelegenheiten antworten, die personenbezogene Daten des Verantwortlichen betreffen, es sei denn, dies ist gesetzlich vorgeschrieben;
- dem Verantwortlichen – soweit gesetzlich zulässig – Kopien sämtlicher Korrespondenz mit Aufsichtsbehörden zur Verfügung stellen, die personenbezogene Daten des Verantwortlichen betreffen.

## Ausfertigung / Unterschriften

ZUM ZEUGNIS DESSEN haben die bevollmächtigten Vertreter der Parteien diesen Auftragsverarbeitungsvertrag zum Inkrafttretensdatum unterzeichnet.

FÜR UND IM NAMEN VON	FÜR UND IM NAMEN VON
<b>INTECH Automation &amp; Intelligence GmbH (Auftragsverarbeiter)</b>	<b>[Name des Kundenunternehmens] (Verantwortlicher)</b>
Unterschrift: _____	Unterschrift: _____
Name: _____	Name: _____
Funktion: _____	Funktion: _____
Datum: _____	Datum: _____

## ANLAGE I – Einzelheiten der Verarbeitungstätigkeiten

Diese Anlage ist Bestandteil des AVV und unterliegt diesem. Sie beschreibt den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Arten personenbezogener Daten sowie die Kategorien betroffener Personen, wie dies Art. 28 Abs. 3 DSGVO erfordert.

Parameter	Details
Verantwortlicher (Kunde)	[Name des Kundenunternehmens], [Eingetragene Anschrift], [Land]
Auftragsverarbeiter (INTECH Automation & Intelligence)	INTECH Automation & Intelligence GmbH, [Eingetragene Anschrift], Deutschland
Ansprechpartner / DSB (Verantwortlicher)	[Name, E-Mail, Telefon]
Ansprechpartner / DSB (Auftragsverarbeiter)	privacy@empowergpt.ai
Zweck der Verarbeitung	Bereitstellung KI-gestützter Wissensmanagement- und Produktivitätsdienste für Unternehmen, einschließlich: (1) Unternehmensweite Dokumentensuche und -wiedergewinnung; (2) KI-gestützte Beantwortung von Anfragen und Wissensextraktion; (3) KI-Assistent / Chat-Schnittstelle für autorisierte Nutzer; (4) Dokumentenerfassung, -indexierung und semantische Suche; (5) Integration mit internen Systemen des Verantwortlichen (z. B. SharePoint, Google Drive, Confluence, CRM); (6) Verarbeitung von Nutzereingaben und Erzeugung von KI-Antworten; (7) Nutzungsanalytik und Zugriffsprotokollierung zur Gewährleistung der Dienstintegrität und -sicherheit. Der genaue Umfang der aktiven Anwendungsfälle ist im MSA oder in einer gesonderten Leistungsbeschreibung zu vereinbaren.
Rechtsgrundlage (Verantwortlicher)	Art. 6 Abs. 1 Buchst. b DSGVO (Vertragserfüllung); Art. 6 Abs. 1 Buchst. c DSGVO (rechtliche Verpflichtung); Art. 6 Abs. 1 Buchst. f DSGVO (berechtigte Interessen) – jeweils nach Festlegung durch den Verantwortlichen
Kategorien betroffener Personen	Mitarbeitende, Auftragnehmer und autorisierte Nutzer der Plattform von INTECH Automation & Intelligence beim Verantwortlichen; Personen, auf die innerhalb von Dokumenten, Mitteilungen oder sonstigen Inhalten Bezug genommen wird, die vom Verantwortlichen oder seinen autorisierten Nutzern hochgeladen werden

Kategorien personenbezogener Daten	Identitätsdaten (Name, Benutzername, Personalnummer); Kontaktdaten (geschäftliche E-Mail, Telefon); Nutzungs- und Interaktionsdaten (Eingabeaufforderungen, Anfragen, KI-Antworten, von Nutzern hochgeladene Dokumenteninhalte); Metadaten (Dateinamen, Zeitstempel, Zugriffsmuster, Dokumenteigenschaften, Aktivitätsprotokolle der Nutzer); technische Daten (IP-Adresse, Geräte-Kennungen, Sitzungsprotokolle, Browsertyp); gegebenenfalls besondere Kategorien personenbezogener Daten, jedoch nur, sofern diese vom Verantwortlichen ausdrücklich in hochgeladenen Inhalten verarbeitet werden
Besondere Datenkategorien	Nicht vorgesehen; der Verantwortliche ist dafür verantwortlich, keine besonderen Kategorien personenbezogener Daten hochzuladen, sofern keine gesonderte schriftliche Vereinbarung getroffen wurde
Art der Verarbeitung	Erhebung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Abruf, Verwendung, Übermittlung und Löschung personenbezogener Daten über cloudbasierte KI-Dienste; KI-gestützte Analyse und Antwortgenerierung; Integration mit vom Verantwortlichen festgelegten Drittsystemen
Dauer der Verarbeitung	Für die Laufzeit des Master Services Agreement zuzüglich etwaig anwendbarer gesetzlicher Aufbewahrungsfristen; nach Vertragsbeendigung gemäß Abschnitt 11 dieses AVV
Genehmigte Unterauftragsverarbeiter	Wie in Anlage III aufgeführt; der Verantwortliche hat eine allgemeine Genehmigung erteilt, vorbehaltlich des Widerspruchsverfahrens in Abschnitt 7

## ANLAGE II — Technische und organisatorische Maßnahmen (TOMs)

Diese Anlage führt die von INTECH Automation & Intelligence gemäß Art. 32 und Art. 28 Abs. 3 Buchst. c DSGVO ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen auf. Diese Maßnahmen stellen einen Mindeststandard dar; INTECH Automation & Intelligence kann von Zeit zu Zeit zusätzliche Maßnahmen umsetzen.

Kontrollbereich	Maßnahme	Norm / Referenz
Zugriffskontrolle	Rollenbasierte Zugriffskontrolle (RBAC) nach dem Prinzip der geringsten Rechte; verpflichtende Mehrfaktor-Authentifizierung (MFA) für sämtliche privilegierten Konten; vierteljährliche Überprüfung der privilegierten Zugriffe Identität und Authentifizierung werden über Keycloak unter Verwendung von OpenID Connect (OIDC) verwaltet; Unternehmensnutzer können sich über externe Identitätsanbieter (z. B. Azure AD) authentifizieren; drei Anwendungsrollen (Organisationsadministrator, Workspace-Administrator, regulärer Nutzer) sowie drei Inhaltsrollen (Betrachter, Mitwirkender, Verantwortlicher) mit Unterstützung benutzerdefinierter Rollen; RBAC integriert mit Azure AD für den Zugriff auf Kubernetes und Datenbanken	ISO 27001 A.9; NIST AC
Verschlüsselung im Ruhezustand	AES-256-Verschlüsselung für sämtliche gespeicherten personenbezogenen Daten; Schlüsselverwaltung über HSM (FIPS 140-2 Level 3) Anwendungsgeheimnisse, API-Schlüssel und Verschlüsselungsschlüssel werden in Azure Key Vault	ISO 27001 A.10; SOC 2 CC6

	gespeichert und verwaltet; Geheimnisse werden über External Secrets in Kubernetes-Pods eingebracht (niemals in Umgebungsvariablen oder Quellcode gespeichert); Azure AD wird anstelle statischer Anmeldedaten zur Authentifizierung gegenüber PostgreSQL und Azure-Diensten verwendet; sämtliche Schlüssel werden in verschlüsseltem Speicher abgelegt	
Verschlüsselung bei der Übertragung	TLS 1.3 für sämtliche Daten während der Übertragung verpflichtend; HSTS erzwungen; zusätzlich AES-256-Verschlüsselung auf Anwendungsebene für sämtliche API-Anfrage- und -Antwortparameter mittels kurzlebiger ephemeraler Sitzungsschlüssel (außerhalb des Kanals vereinbart, niemals über die Leitung übermittelt); HTTP-Only-, SameSite- und Secure-Cookie-Attribute erzwungen mit serverseitiger Cookie-Verschlüsselung; CORS auf vertrauenswürdige Domänen beschränkt; NGINX-Ingress mit von Cert Manager verwalteten TLS-Zertifikaten	OWASP TLS; NIST SP 800-52
Netzwerksicherheit	Segmentierte VPC-Architektur; WAF und DDoS-Schutz; Intrusion Detection/Prevention (IDS/IPS); regelmäßige Schwachstellenscans Private Azure-Endpunkte für Speicherkonten und Datenbanken (keine öffentliche Internetexposition); Firewall-Regeln zur Beschränkung des Zugriffs auf bestimmte IP-Bereiche und vertrauenswürdige Azure-Dienste; Dienst-zu-Dienst-Authentifizierung; Infrastructure as Code (IaC) mit verpflichtenden Peer-Review-Pull-Requests	ISO 27001 A.13; CIS Controls
Protokollierung und Überwachung	Zentralisiertes SIEM; Auditprotokolle werden mindestens 12 Monate aufbewahrt; automatisierte Alarmierung bei auffälligen Zugriffsmustern; manipulationssichere Protokollspeicherung	ISO 27001 A.12; SOC 2 CC7
Reaktion auf Sicherheitsvorfälle	Dokumentierter Incident-Response-Plan; 24/7-SOC; SLA zur Meldung von Verletzungen an den Verantwortlichen binnen 72 Stunden; jährliche IR-Simulationen	ISO 27001 A.16; Art. 33 DSGVO
Schwachstellenmanagement	Monatliche automatisierte Scans; jährliche externe Penetrationstests; kritische/hohe Patches innerhalb von 30 Tagen; SLA-gestützte Behebung Statische Code-Analyse in die CI/CD-Pipeline für sämtliche Codeänderungen vor der Bereitstellung integriert; regelmäßige Sicherheitsaudits und Penetrationstests durch externe Cybersicherheitsspezialisten; Datei-Uploads werden strengen Dateityp-Prüfungen und einem Virenskan unterzogen; durchgängige Verwendung parametrisierter SQL-Abfragen zur Eliminierung des SQL-Injection-Risikos; CSRF-Token eingebettet in sämtliche Formulare; generische Fehlermeldungen zur Verhinderung von Informationslecks	NIST SP 800-115; ISO 27001
Physische Sicherheit	Tier-III+-Rechenzentren; biometrischer Zugang und Ausweiszugang; CCTV-Überwachung; Co-Location-Anbieter sind nach ISO 27001 zertifiziert	ISO 27001 A.11; SOC 2 A1

Geschäftskontinuität	RTO ≤ 4 Stunden; RPO ≤ 1 Stunde; geo-redundante Datensicherungen; jährliche BCP-/DR-Tests mit dokumentierten Ergebnissen Automatisierte tägliche Datensicherungen mit einer Aufbewahrungsfrist von 30 Tagen; Sicherungen sind im Ruhezustand verschlüsselt (AES-256) und unterliegen Zugriffskontrollen, die denen der Produktionssysteme entsprechen; Zugriffsprotokolle zu Datensicherungen werden dem Verantwortlichen auf Anfrage zur Verfügung gestellt	ISO 22301; SOC 2 A1
Mitarbeitersicherheit	Hintergrundprüfungen vor Beschäftigungsaufnahme; jährliche Schulungen zu DSGVO und Sicherheit; Vertraulichkeitsvereinbarungen für sämtliche Mitarbeitende mit Datenzugriff; Disziplinarverfahren	ISO 27001 A.7; Art. 28 Abs. 3 Buchst. b DSGVO
KI-Modell-Governance	Kein Training von LLMs auf personenbezogenen Daten des Verantwortlichen ohne ausdrückliche schriftliche Zustimmung; Datenisolation zwischen Mandanten; Filterung der Modellausgaben	NIST AI RMF; Erwägungen zum EU-KI-Gesetz
Datenminimierung	Verarbeitung auf das für die Erbringung der Dienste erforderliche Maß beschränkt; Pseudonymisierung wird umgesetzt, wo dies praktikabel ist; Aufbewahrungsrichtlinien werden automatisiert durchgesetzt	Art. 5 Abs. 1 Buchst. c und e DSGVO
Steuerung der Unterauftragsverarbeiter	Vertraglicher AVV mit sämtlichen Unterauftragsverarbeitern; jährliche Compliance-Überprüfungen; technische und organisatorische Maßnahmen der Unterauftragsverarbeiter werden bei Aufnahme der Beauftragung überprüft	Art. 28 Abs. 4 DSGVO
Pseudonymisierung	Nutzer-Identifikatoren werden in Analyse- und Protokollierungssystemen pseudonymisiert; Re-Identifizierungskontrollen sind implementiert	Art. 4 Nr. 5; Art. 32 Abs. 1 Buchst. a DSGVO

INTECH Automation & Intelligence überprüft und aktualisiert diese Maßnahmen mindestens jährlich sowie nach jeder wesentlichen Änderung der Verarbeitungstätigkeiten, nach Sicherheitsvorfällen oder bei Veränderungen der Bedrohungslage. Aktuelle Einzelheiten werden unter [trust.empowergpt.ai](https://trust.empowergpt.ai) veröffentlicht.

## ANLAGE III — Genehmigte Unterauftragsverarbeiter

Die folgenden Unterauftragsverarbeiter sind vom Verantwortlichen gemäß Abschnitt 7 dieses AVV genehmigt. INTECH Automation & Intelligence führt eine aktuelle Version dieses Registers unter [trust.empowergpt.ai/sub-processors](https://trust.empowergpt.ai/sub-processors). Wesentliche Änderungen (Hinzufügungen oder Ersetzungen) unterliegen dem in den Ziffern 7.3 bis 7.4 vorgesehenen Mitteilungs- und Widerspruchsverfahren mit einer Frist von 30 Tagen. Jeder Unterauftragsverarbeiter wurde hinsichtlich der DSGVO-Konformität bewertet und ist durch einen schriftlichen AVV mit INTECH Automation & Intelligence gebunden.

Unterauftragsverarbeiter	Eingetragene Anschrift	Leistung / Zweck	Standort	Übermittlungsgrundlage
--------------------------	------------------------	------------------	----------	------------------------

Microsoft Azure	Microsoft Ireland Operations Ltd, One Microsoft Place, Dublin, Irland	Kerninfrastruktur, Rechenleistung, Speicher, Netzwerk. Azure OpenAI Service (LLM-Inferenz und Embeddings); Azure Speech Service (Sprache-zu-Text-Transkription)	Germany West Central	EU-Angemessenheit; Art. 45 DSGVO
Google Cloud AI (über GCP)	Google Cloud EMEA Ltd, 70 Sir John Rogerson's Quay, Dublin 2, Irland	LLM-Inferenz: Gemini-Modelle (Google) und Claude-Modelle (Anthropic, über GCP-Integration); Eingabeaufforderungen, Antworten, Kontextdaten (vom Verantwortlichen ausdrücklich zu aktivieren)	Ausschließlich EU-Region (GCP-EU-Bereitstellung)	EU-Angemessenheit; Art. 45 DSGVO; keine regionsübergreifende Übertragung
E2B	E2B, Inc. (vom Anbieter verwaltete Infrastruktur)	Sichere, in einer Sandbox isolierte Code-Ausführungsumgebung (Code-Interpreter); von Nutzern übermittelter Code, Ausführungsergebnisse, temporäre Laufzeitdaten	Vom Anbieter verwaltet	Standardvertragliche Schutzmaßnahmen; isolierte, kurzlebige Ausführung
Cloudflare	Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA (EU-Edge-Standorte)	DNS, CDN, WAF, DDoS-Schutz; ausschließlich IP-Adresse und Anfrage-Metadaten	Globales Edge-Netzwerk	EU-SCCs (Art. 46 DSGVO); Cloudflare-AVV
PostHog	PostHog, Inc. (EU-Region-Bereitstellung)	Produkt- und Nutzungsanalytik; Ereignisdaten und Nutzungs-Metadaten; keine Erfassung von KI-Eingabeaufforderungen oder sensiblen Inhalten	EU (konfigurierte Bereitstellung)	EU-Angemessenheit; DSGVO-konforme Konfiguration

Hinweise: (1) KI-/LLM-Unterauftragsverarbeiter (Google Cloud AI) sind standardmäßig deaktiviert und verarbeiten personenbezogene Daten des Verantwortlichen erst dann, wenn der Verantwortliche das jeweilige Modell ausdrücklich über die Plattformeinstellungen oder durch schriftliche Vereinbarung aktiviert (gemäß Ziffer 7.6). (2) Die folgenden Komponenten werden innerhalb der Azure-Umgebung von INTECH Automation & Intelligence's selbst gehostet und sind keine Unterauftragsverarbeiter: Keycloak, Grafana, Prometheus, Grafana Loki. (3) Die primäre Infrastrukturregion ist Germany West Central (Azure). KI-Verarbeitungsregionen: Azure OpenAI → EU-Datenzone; Google Cloud AI (Gemini / Claude) → EU-Region; Azure Speech → EU-Region; PostHog → EU-Region. (4) Datenaufbewahrung: Blob Storage Soft-Delete 95 Tage (Versionierung aktiviert); PostgreSQL-Sicherungen 35 Tage; Protokolle 90 Tage; Metriken 10 Tage. (5) Diese Liste wird vor der Aufnahme jedes neuen Unterauftragsverarbeiters überprüft und aktualisiert. Die aktuelle Version wird unter

trust.empowergpt.ai/sub-processors veröffentlicht und ersetzt nach Unterzeichnung dieses Dokument. (6) Die eingetragenen Anschriften werden zu Informationszwecken angegeben; Änderungen der Rechtsform oder der Anschrift werden dem Verantwortlichen mitgeteilt. (7) Zertifizierungen und Auditberichte zu zentralen Unterauftragsverarbeitern sind auf schriftliche Anfrage an [privacy@empowergpt.ai](mailto:privacy@empowergpt.ai) erhältlich.

---

## **ANLAGE IV — Standardvertragsklauseln und Übermittlungsmechanismen**

### **A. EU-Standardvertragsklauseln**

Übermittelt INTECH Automation & Intelligence oder ein Unterauftragsverarbeiter personenbezogene Daten in ein Drittland ohne Angemessenheitsbeschluss der EU, so unterliegt die Übermittlung den durch den Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 verabschiedeten Standardvertragsklauseln (die „EU-SCCs“).

Für Übermittlungen vom Verantwortlichen (als Datenexporteur) an INTECH Automation & Intelligence (als Datenimporteur) außerhalb des EWR gelten die SCCs nach Modul Zwei (Verantwortlicher an Auftragsverarbeiter), mit folgenden Festlegungen: