Vereinbarung über die Auftragsverarbeitung (AVV)

Standardvertragsklauseln der EU-Kommission gemäß Art. 28 Abs. 7 DSGVO (Durchführungsbeschluss (EU) 2021/915) mit Floriti-Anhängen

Floriti · Version 1.2 · Stand: 23. Oktober 2026

Diese Vereinbarung wird mit Unterzeichnung von Anhang I Bestandteil des Hauptvertrags. Bitte Anhang I ausfüllen, unterzeichnen und an info@floriti-register.com senden; Sie erhalten ein gegengezeichnetes Exemplar zurück.

Vorbemerkung und Aufbau

Zwischen dem in Anhang I genannten Kunden (**„Verantwortlicher“**) und der Tasker & Fox GmbH, Hohenlohestraße 17, 80637 München (**„Auftragsverarbeiter“**) besteht ein Vertrag über die Nutzung der Software-Plattform „Floriti“ als Software-as-a-Service (**„Hauptvertrag“**). Zur Erfüllung von Art. 28 Abs. 3 und 4 DSGVO vereinbaren die Parteien Folgendes:

- **Teil A:** die von der Europäischen Kommission erlassenen **Standardvertragsklauseln** nach Art. 28 Abs. 7 DSGVO (Durchführungsbeschluss (EU) 2021/915 vom 4. Juni 2021) im **unveränderten amtlichen Wortlaut**. Gewählt sind jeweils die Optionen für die DSGVO sowie in Klausel 7.7 die Option 2 (allgemeine schriftliche Genehmigung). Die fakultative Klausel 5 (Kopplungsklausel) wird nicht vereinbart;
- **Teil B:** die **Anhänge I bis IV** mit den Angaben zu Parteien, Verarbeitung, technischen und organisatorischen Maßnahmen sowie Unterauftragsverarbeitern;
- **Teil C: ergänzende Vereinbarungen** gemäß Klausel 2 Buchstabe b, die die Klauseln für die Floriti-Plattform konkretisieren. Sie stehen weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln; im Zweifel gehen die Klauseln vor (Klausel 4).

Teil A – Standardvertragsklauseln

Abschnitt I

Klausel 1 – Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 – Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 – Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 – Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Abschnitt II – Pflichten der Parteien

Klausel 6 – Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 – Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche

Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 30 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und

den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 – Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

   2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

   3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

   4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 – Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

   Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Abschnitt III – Schlussbestimmungen

Klausel 10 – Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Teil B – Anhänge

Anhang I – Liste der Parteien

Verantwortlicher

Angabe	Eintrag
Name	[Name / Firma des Kunden]
Anschrift	[Anschrift]
Kontaktperson (Name, Funktion, Kontaktdaten)	[Name, Funktion, E-Mail, Telefon]
Datenschutzbeauftragter (falls bestellt)	[Name, Kontaktdaten]
Unterschrift und Beitrittsdatum	Ort, Datum, Unterschrift

Auftragsverarbeiter

Angabe	Eintrag
Name	Tasker & Fox GmbH (Amtsgericht München, HRB 315350)
Anschrift	Hohenlohestraße 17, 80637 München, Deutschland
Kontaktperson (Name, Funktion, Kontaktdaten)	Oliver Fuchs, Geschäftsführer, info@floriti-register.com
Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist nicht bestellt; hierzu besteht keine Pflicht (Art. 37 DSGVO, § 38 BDSG). Den Datenschutz verantwortet der Geschäftsführer Oliver Fuchs persönlich – TÜV-zertifizierter Datenschutzbeauftragter und Datenschutzauditor sowie Certified Information Privacy Professional/Europe (CIPP/E).
Unterschrift und Beitrittsdatum	Ort, Datum, Unterschrift

Anhang II – Beschreibung der Verarbeitung

Merkmal	Beschreibung
Kategorien betroffener Personen	• Personen, deren Daten der Verantwortliche in seinen Registern und Fragebögen erfasst, insbesondere Beschäftigte, Kunden, Interessenten, Lieferanten, Geschäftspartner und deren Ansprechpartner sowie sonstige Kontaktpersonen; • Benutzer der Plattform (Beschäftigte und Beauftragte des Verantwortlichen); • Empfänger von Benachrichtigungen und Einladungen aus der Plattform.

Merkmal	Beschreibung
Kategorien personenbezogener Daten	• Registerinhalte: Der Verantwortliche legt die Struktur seiner Register selbst fest und bestimmt damit die Datenarten; typischerweise Stamm- und Kontaktdaten, Vertrags-, Vorgangs- und Organisationsdaten, Bewertungen und Freigaben; • hochgeladene Dokumente und Datei-Anhänge; • Benutzerdaten: Name, Benutzername, E-Mail-Adresse, Rollen, Gruppen- und Bereichszuordnungen, Passwort-Hash bzw. SSO-Kennung, Spracheinstellung; • Protokolldaten: Aktivitätsprotokoll (Benutzer, Zeitpunkt, geänderte Felder), technische Server-Protokolle einschließlich IP-Adressen; • Kommunikationsdaten im Rahmen des Supports (Support-Tickets, E-Mails).
Sensible Daten (Art. 9, 10 DSGVO) und Garantien	Die Verarbeitung sensibler Daten ist nicht vorgesehen. Sie ist nur nach vorheriger Abstimmung in Textform zulässig. In diesem Fall gelten zusätzlich: Beschränkung des Zugriffs über Rollen, Bereiche und Nur-Genehmiger-Felder auf berechtigte Personen, Protokollierung aller Änderungen im Aktivitätsprotokoll, keine Übermittlung an KI-Dienste ohne gesonderte Freigabe durch den Verantwortlichen sowie gegebenenfalls weitere im Einzelfall vereinbarte Maßnahmen.
Art der Verarbeitung	Hosting und Speicherung, Erfassen, Organisieren, Ordnen, Auslesen, Abfragen, Auswerten (Berichte, Kennzahlen), Versand von Benachrichtigungen, Übermittlung über Export, API, Webhooks und Datenbank-Synchronisation auf Veranlassung des Verantwortlichen, Datensicherung, Löschung; Zugriff im Einzelfall für Support und Fehlerbehebung; optional KI-gestützte Analyse.
Zwecke der Verarbeitung	Bereitstellung und Betrieb der Floriti-Plattform in einer dedizierten Kundeninstanz gemäß Hauptvertrag und Leistungsbeschreibung, einschließlich Support, Datensicherung, Überwachung der Verfügbarkeit und Sicherheit sowie – nur nach Freischaltung durch den Verantwortlichen – KI-Funktionen.
Dauer der Verarbeitung	Für die Laufzeit des Hauptvertrags und darüber hinaus bis zur Löschung bzw. Rückgabe der Daten nach Klausel 10 Buchstabe d und Teil C Ziffer 7.
Verarbeitung durch Unterauftragsverarbeiter	Gegenstand, Art und Dauer der Verarbeitung durch Unterauftragsverarbeiter ergeben sich aus Anhang IV.

Anhang III – Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters sind im beigefügten Dokument „Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO“ in der jeweils aktuellen Fassung konkret beschrieben; es ist Bestandteil dieses Anhangs. Die folgende Übersicht ordnet die Maßnahmen den Kategorien des Musters zu:

Maßnahmenkategorie	Umsetzung (Fundstelle in der TOM)
Pseudonymisierung und Verschlüsselung	TLS-Verschlüsselung aller Verbindungen inkl. Reporting-Zugang; Passwörter nur als bcrypt-Hash; ausgelagerte Sicherungskopien asymmetrisch verschlüsselt, privater Schlüssel offline verwahrt (TOM 1.2, 2.1, 3)
Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit	Mandantentrennung durch eigene Instanz und Datenbank je Kunde, Ressourcenlimits, automatischer Neustart (TOM 1.4, 3)

Maßnahmenkategorie	Umsetzung (Fundstelle in der TOM)
Rasche Wiederherstellung	Tägliche Sicherung aller Datenbanken und der Konfiguration, 14 Tage Aufbewahrung; zusätzlich tägliche verschlüsselte Sicherungskopie (Datenbanken, Datei-Anhänge, Konfiguration) an zwei voneinander unabhängigen Standorten in der EU mit Löschschutz, ebenfalls 14 Tage Aufbewahrung; Alarmierung bei fehlgeschlagener oder ausbleibender Sicherung und wöchentlicher automatischer Wiederherstellungstest; Wiederherstellung einzelner Instanzen (TOM 3)
Regelmäßige Überprüfung	Sicherheitsaktualisierungen, protokollierte Provisionierung, Uptime-Überwachung (TOM 5)
Identifizierung und Autorisierung	Persönliche Konten, rollen- und bereichsbasiertes Berechtigungskonzept, optional Single Sign-on (TOM 1.2, 1.3)
Schutz bei Übermittlung und Speicherung	HTTPS-Zwang, SSH-only-Administration, getrennte Container-Netzwerke (TOM 1.2, 1.4, 2.1)
Physische Sicherheit	ISO/IEC 27001-zertifizierte Rechenzentren der Hetzner Online GmbH in Falkenstein; verschlüsselte Sicherungskopien zusätzlich in Helsinki, Finnland (Hetzner Online GmbH) und Paris, Frankreich (Scaleway SAS) (TOM 1.1, 3)
Protokollierung	Lückenloses Aktivitätsprotokoll mit konfigurierbarer Aufbewahrungsdauer (TOM 2.2)
Datenminimierung, begrenzte Speicherung	Aufbewahrungsfristen für Protokolle, Rotation der Sicherungen nach 14 Tagen, Löschung bei Vertragsende (TOM 3, 7)
Datenübertragbarkeit und Löschung	Vollständiger Selbstexport (Excel/CSV/ZIP inkl. Anhängen), Löschung von Instanz, Datenbank und Dateien (TOM 7)

Spezifische Maßnahmen zur Unterstützung des Verantwortlichen (Klauseln 8 und 9)

- **Betroffenenrechte:** Auskunft, Berichtigung, Löschung und Datenübertragbarkeit kann der Verantwortliche selbst über die Plattformfunktionen (Bearbeitung, Löschung, Export, Aktivitätsprotokoll) umsetzen. Darüber hinausgehende Unterstützung leistet der Auftragsverarbeiter auf Anfrage.
- **Verletzungen des Schutzes personenbezogener Daten:** Meldung an die Kontaktperson des Verantwortlichen (Anhang I) per E-Mail, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, mit den Angaben nach Klausel 9.2; auf Anfrage Bereitstellung relevanter Protokollauszüge.
- **Datenschutz-Folgenabschätzung und Konsultation:** Bereitstellung der TOM, einer Beschreibung der Systemarchitektur und der Angaben zu Unterauftragsverarbeitern.
- **Unterauftragsverarbeiter:** Die Unterauftragsverarbeiter sind über Auftragsverarbeitungsverträge an technische und organisatorische Maßnahmen gebunden, die dem Schutzniveau dieses Anhangs entsprechen.

Anhang IV – Liste der Unterauftragsverarbeiter

Die folgende Liste ist die vereinbarte Liste im Sinne von Klausel 7.7 Buchstabe a (Option 2):

Unterauftragsverarbeiter	Gegenstand und Art der Verarbeitung	Ort der Verarbeitung / Übermittlungsgrundlage
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen	Hosting: Server, Speicher, Netzwerk und Datensicherung der Kundeninstanz sowie Speicherung verschlüsselter Sicherungskopien (Storage Box); für die Laufzeit des Hauptvertrags	Deutschland, Rechenzentrum Falkenstein/Sachsen; verschlüsselte Sicherungskopien (Storage Box): Finnland, Rechenzentrum Helsinki (EU); keine Drittlandübermittlung
Scaleway SAS 8 rue de la Ville-l'Évêque, 75008 Paris, Frankreich	Object Storage (Region Paris, Frankreich) – Speicherung verschlüsselter Datensicherungen; der Anbieter hat keinen Zugriff auf den Schlüssel	EU (Frankreich), Region Paris; keine Drittlandübermittlung
Heinlein Hosting GmbH (mailbox.org) Schwedter Straße 9a, 10119 Berlin	E-Mail-Postfächer des Auftragsverarbeiters (Support- und Kontaktkommunikation, inkl. darin übermittelter Daten)	Deutschland; keine Drittlandübermittlung
Sendinblue SAS (Brevo) rue Salneuve 9-17, 75017 Paris, Frankreich	Versand von Transaktions-E-Mails aus der Plattform (Benachrichtigungen, Einladungen, Passwort-Links)	EU (Frankreich); etwaige Übermittlungen durch Unter-Dienstleister von Brevo auf Grundlage von Standardvertragsklauseln bzw. EU-US Data Privacy Framework gemäß Brevo-AVV
Anthropic PBC San Francisco, USA	KI-gestützte Analyse übermittelter Texte – **ausschließlich**, wenn der Verantwortliche die KI-Funktionen für seine Instanz freischaltet und Anthropic als KI-Anbieter gewählt hat (für die Instanz oder einzelne Register)	USA; Übermittlung auf Grundlage der Standardvertragsklauseln (EU) 2021/914, Modul 3, gemäß Anthropic-DPA
Mistral AI SAS 15 rue des Halles, 75001 Paris, Frankreich	KI-gestützte Analyse übermittelter Texte – **ausschließlich**, wenn der Verantwortliche die KI-Funktionen für seine Instanz freischaltet und Mistral AI als KI-Anbieter gewählt hat (für die Instanz oder einzelne Register)	EU (Frankreich); etwaige Übermittlungen durch Unter-Dienstleister von Mistral AI auf Grundlage eines Angemessenheitsbeschlusses oder von Standardvertragsklauseln gemäß Mistral-DPA

Keine Unterauftragsverarbeiter des Auftragsverarbeiters sind Dienste, die der Verantwortliche selbst anbindet und beauftragt, insbesondere ein eigener KI-Endpunkt oder eigener KI-Schlüssel, ein eigener Identitätsanbieter (SSO), externe Datenbanken, API-Clients und Webhook-Empfänger. Die semantische Indexierung der KI-Wissensbasis erfolgt auf den Servern des Auftragsverarbeiters in Deutschland.

Teil C – Ergänzende Vereinbarungen

Die folgenden Vereinbarungen ergänzen die Klauseln im Sinne von Klausel 2 Buchstabe b. Bei Widersprüchen gehen die Klauseln vor (Klausel 4).

1. Verhältnis zum Hauptvertrag

(1) Diese Vereinbarung gilt für die Laufzeit des Hauptvertrags und darüber hinaus, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet.

(2) Vergütung und Haftung richten sich nach dem Hauptvertrag, soweit die Klauseln oder zwingendes Recht (insbesondere Art. 82 DSGVO) nichts anderes bestimmen.

2. Weisungen (Klausel 7.1)

(1) Weisungen erteilt der Verantwortliche in der Regel durch die Konfiguration und Nutzung der Plattform, etwa durch das Anlegen von Registern, Rechten und Workflows, durch Exporte, Schnittstellen und das Ein- oder Ausschalten von Funktionen. Diese Vorgänge sind in der Plattform dokumentiert und gelten als dokumentierte Weisungen.

(2) Darüber hinausgehende Weisungen erteilen die in Anhang I benannte Kontaktperson oder die Administratoren der Kundeninstanz in Textform. Weisungen, die über den im Hauptvertrag vereinbarten Leistungsumfang hinausgehen, werden als Änderungswunsch behandelt; ihre Umsetzung kann gesondert vergütet werden.

3. KI-Funktionen und Drittlandübermittlung (Klausel 7.8)

(1) Die Übermittlung von Daten an einen KI-Unterauftragsverarbeiter nach Anhang IV erfolgt nur, wenn ein Administrator des Verantwortlichen die KI-Funktionen für die Instanz freischaltet, und nur an den vom Verantwortlichen gewählten KI-Anbieter (Anthropic PBC oder Mistral AI SAS; Wahl je Instanz, abweichend je Register möglich). Die Freischaltung und die Anbieter-Wahl gelten als dokumentierte Weisung im Sinne von Klausel 7.8 Buchstabe a; sie werden protokolliert und können jederzeit geändert oder widerrufen werden.

(2) Nutzt der Verantwortliche einen eigenen KI-Endpunkt oder einen eigenen KI-Schlüssel, erfolgt die Verarbeitung durch diesen Anbieter im Auftrag des Verantwortlichen und nicht als Unterauftragsverarbeitung des Auftragsverarbeiters.

(3) Ist für ein Register Mistral AI SAS als KI-Anbieter gewählt, werden Inhalte dieses Registers nicht an Anthropic PBC übermittelt; Analysen, an denen ein solches Register beteiligt ist, erfolgen insgesamt über Mistral AI SAS. Steht der gewählte KI-Anbieter nicht zur Verfügung, wird die KI-Funktion nicht ausgeführt; der Auftragsverarbeiter weicht nicht auf einen anderen KI-Anbieter aus.

4. Nachweise und Prüfungen (Klausel 7.6)

(1) Den Nachweis erbringt der Auftragsverarbeiter vorrangig durch die TOM, Selbstauskünfte, die Beantwortung von Sicherheitsfragebögen sowie Zertifikate und Prüfberichte der Unterauftragsverarbeiter.

(2) Prüfungen vor Ort kündigt der Verantwortliche mit einer Frist von mindestens 14 Tagen in Textform an, es sei denn, es bestehen Anzeichen für eine Nichteinhaltung oder eine Verletzung des Schutzes personenbezogener Daten. Sie finden während der üblichen Geschäftszeiten und ohne vermeidbare Störung des Betriebs statt. Beauftragte Prüfer müssen zur Verschwiegenheit verpflichtet sein und dürfen nicht im Wettbewerb mit dem Auftragsverarbeiter stehen.

(3) Für die Rechenzentren gilt: Der Betreiber lässt Prüfungen durch Kunden seiner Kunden nicht zu; der Nachweis erfolgt durch dessen ISO/IEC 27001-Zertifizierung.

(4) Jede Partei trägt ihre eigenen Kosten. Für mehr als eine Prüfung vor Ort pro Kalenderjahr ohne Anlass nach Absatz 2 kann der Auftragsverarbeiter eine angemessene Vergütung seines Aufwands verlangen.

5. Unterauftragsverarbeiter (Klausel 7.7)

(1) Die Unterrichtung über beabsichtigte Änderungen erfolgt per E-Mail an die Kontaktperson nach Anhang I. Einwände erhebt der Verantwortliche innerhalb der Frist nach Klausel 7.7 Buchstabe a in Textform unter Angabe der Gründe.

(2) Können sich die Parteien nicht einigen, ist der Verantwortliche berechtigt, den Hauptvertrag zum Zeitpunkt des Wirksamwerdens der Änderung außerordentlich zu kündigen; im Voraus gezahlte Entgelte für die Zeit danach werden anteilig erstattet.

6. Meldung von Verletzungen (Klausel 9.2)

Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten spätestens innerhalb von 48 Stunden nach Kenntniserlangung. Anlaufstelle nach Klausel 9.2 Buchstabe b ist die Kontaktperson des Auftragsverarbeiters nach Anhang I.

7. Rückgabe und Löschung (Klausel 10 Buchstabe d)

(1) Die Rückgabe der Daten erfolgt durch Selbstexport des Verantwortlichen (Excel/CSV/ZIP inklusive Datei-Anhängen), der während der Laufzeit jederzeit und bis 30 Tage nach Vertragsende möglich ist. Auf Wunsch unterstützt der Auftragsverarbeiter den Export.

(2) Der Verantwortliche teilt seine Wahl nach Klausel 10 Buchstabe d in Textform mit. Äußert er sich bis zum Ablauf der Frist nach Absatz 1 nicht, löscht der Auftragsverarbeiter die Daten (Instanz, Datenbank, Datei-Anhänge) und bestätigt die Löschung in Textform.

(3) Datensicherungen werden nicht einzeln bereinigt, sondern rotieren binnen 14 Tagen nach der Löschung automatisch aus; bis dahin werden sie nicht verarbeitet und bleiben durch die Maßnahmen nach Anhang III geschützt.

8. Zugriffe für Support und Betrieb; Verschwiegenheit (Klausel 7.4)

(1) Der Auftragsverarbeiter greift auf Inhalte der Kundeninstanz nur zu, soweit dies für Support-Anfragen, Störungsbeseitigung, Sicherheit oder Wiederherstellung erforderlich ist.

(2) Ist der Verantwortliche Berufsgeheimnisträger, verpflichtet der Auftragsverarbeiter die mitwirkenden Personen gemäß § 203 Abs. 4 Satz 2 Nr. 1 StGB zur Geheimhaltung.

9. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Aktualisierungen von Anhang IV erfolgen nach dem Verfahren der Klausel 7.7 und Teil C Ziffer 5.

(2) Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, München.

(3) Sollten einzelne ergänzende Vereinbarungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen und der Klauseln unberührt.