AUFTRAGSVERARBEITUNGSVERTRAG INSIGN 365

Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR

Stand 12.09.2023
Version 2.0.2

Auftragsverarbeitungsvertrag

(nachfolgend und in Anhängen **Auftragsverarbeitungsvertrag**)

zwischen dem

Lizenznehmer des Onlinedienstes inSign 365

(nachfolgend und in Anhängen **Verantwortlicher**)

und

inSign GmbH
Am Bäckeranger 2
85417 Marzling
Deutschland

(nachfolgend und in Anhängen **Auftragsverarbeiter**)

(nachfolgend und in Anhängen gemeinsam die **Parteien,** einzeln jeweils eine **Partei**)

Präambel

Bei den folgenden Klauseln handelt es sich um die Standardvertragsklauseln (Vertrag über die Verarbeitung personenbezogener Daten gem. Art. 28 Abs. 3 DSGVO), welche die EU-Kommission am 4. Juni 2021 verabschiedet hat. Diese entsprechen den Anforderungen des Artikels 28 Absatz 3 DSGVO.

inSign GmbH ist eine Unternehmung mit Sitz in Deutschland. inSign verwendet zum Zweck der Regelung von Auftragsverarbeitungsverhältnissen die Standardklauseln für Verantwortliche und Auftragnehmer in der EU / im EWR. Der Originaltext der Standardvertragsklauseln inklusive der vorgegebenen Optionen kann hier aufgerufen werden: https://ec.europa.eu/info/law/law-topic/data-protection_de.

Die Standardvertragsklauseln sehen in gewissen Klauseln Optionen vor, bei denen inSign als Auftragsverarbeiter bereits eine Auswahl getroffen hat. Die ausgewählten Optionen sind im Vertragstext zur besseren Lesbarkeit bereits umgesetzt. Entfallene Optionen sind im Anhang VI zum Zweck der Transparenz aufgeführt. Im Übrigen wurden die Standardvertragsklauseln in unveränderter Form übernommen und lediglich um einzelne Bestimmungen ergänzt. Solche Ergänzungen sind ausschließlich in Anhang V aufgenommen.

Abschnitt 1

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 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.

Klausel 5 (fakultativ) – Kopplungsklausel

Bleibt frei.

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 20 Arbeitstage 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 Verletzung 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 Vertrages

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.

Anhang I – Liste der Parteien

Verantwortliche(r):

Lizenznehmer des Onlinedienstes inSign 365

Auftragsverarbeiter:

inSign GmbH
Am Bäckeranger 2
85417 Marzling

Anhang II – Beschreibung der Verarbeitung

Hinsichtlich des Gegenstandes und der Dauer der Verarbeitung wird vollinhaltlich auf die Regelungen des Hauptvertrags, nachfolgend **Dienstleistungsvertrag**, Bezug genommen.

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Auftraggebers und der Interessenten und Kunden des Auftragsgebers.

Kategorien personenbezogener Daten, die verarbeitet werden

Der Auftragsverarbeiter verarbeitet personenbezogene Daten aller Kategorien.

Verarbeitete sensible Daten (falls zutreffend)

Der Auftragsverarbeiter verarbeitet sensible personenbezogene Daten (Art. 9 DSGVO).

Art der Verarbeitung

Zur Art der Verarbeitung wird auf den Dienstleistungsvertrag verwiesen.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Elektronische Vertragsschlüsse mit elektronischer Unterschrift.

Dauer der Verarbeitung

Hinsichtlich des Gegenstandes und der Dauer der Verarbeitung wird vollinhaltlich auf die Regelungen des Dienstleistungsvertrags Bezug genommen.

Staaten der Verarbeitung

☒ Deutschland/EU

☒ Schweiz

☐ Andere:

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben:

Siehe Anlage IV

Anhang III – Technisch organisatorische Maßnahmen, einschließlich zur Gewährleistung der Datensicherheit

Einleitung

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar. Die jeweils für Ihren Anwendungsfall erforderlichen technischen-organisatorischen Maßnahmen eingesetzter Unterauftragnehmer sind in diesem Dokument nicht mit aufgenommen und werden gesondert zur Verfügung gestellt. Unterauftragnehmer werden nach Art. 28 DSGVO sorgfältig ausgewählt und laufend überprüft.

Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Diese Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Für eine automatisierte Verarbeitung (also vor allem per Hard- und Software) nennen die Gesetze verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

(1) Vertraulichkeit
(2) Integrität
(3) Verfügbarkeit und Belastbarkeit
(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
(5) Pseudonymisierung und Verschlüsselung

Für nicht-automatisierte Verarbeitungen von personenbezogenen Daten sind die oben genannten Kontrollbereiche nach dem Gesetzeswortlaut nicht direkt anwendbar. Es wird jedoch empfohlen, für einen bestmöglichen Schutz auch in diesen Fällen die Datensicherheit in Anlehnung an die Kontrollbereiche zu organisieren. Diese Maßnahmen stellen wir in der Folge vor, um unseren Informationspflichten aus Art. 32 Abs. 3 lit. C nachzukommen.

Organisatorisches

Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. B, 29, 32 Abs. 4 DSGVO verpflichtet. Die bei der Datenverarbeitung eingesetzten Systemadministratoren sind auf ihre Geheimhaltungspflichten gemäß §203 StGB verpflichtet.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlich werden.

Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der inSign GmbH betrieben werden:

Kontrollziel	Maßnahmen
VERTRAULICHKEIT	
1. Zutrittskontrolle Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren	Elektronische Zutrittskontrolle zum Firmengebäude und den zentralen Datenverarbeitungsanlagen (Serverraum) Elektronische Protokollierung aller Schließvorgänge (Schlüsselnummer und Zeitstempel) Zentrale Vergabe und Dokumentation der Vergabe der Schließberechtigungen Meldeverpflichtung und Sperre der Zutrittsberechtigung bei Verlust Zugang zu Serverräumen nur für autorisiertes Personal nach ausdrücklicher Genehmigung durch die Geschäftsleitung Autorisiertes Wachpersonal für Notfälle 24/7 verfügbar und zutrittsberechtigt Aufenthalt von nicht autorisierten Personen in Sicherheitsbereichen nur unter Aufsicht Sorgfältige Auswahl des Reinigungspersonals Aktive Netzwerkkomponenten außerhalb des Serverraums befinden sich nur in verschlossenen Sicherheitsschränken
2. Zugangskontrolle Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Schutz aller Datenverarbeitungsanlagen mindestens durch die Kombination aus Benutzerkennung und Passwort Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten Mindestanforderungen an Passwortkomplexität durch Kennwortrichtlinie Einsatz von Multi-Faktor-Authentifizierung (MFA) Kennwörter müssen geändert werden, wenn der Verdacht auf Kompromittierung des Kennworts (z.B. durch Offenlegung, Hackerangriff, etc.) besteht. Falscheingabe des Passworts wird elektronisch protokolliert und führt im Wiederholungsfall zu einer zeitlich begrenzten Deaktivierung des Benutzerkontos Verschlüsselte Speicherung von Kennwörtern Datenverarbeitungsanlagen sperren die Benutzereingabe, sofern über einen bestimmten Zeitraum keine Interaktion erfolgt Netzwerksegmentierung, Verwendung einer Demilitarisierten Zone (DMZ) Zugangsbeschränkung für bestimmte IP-Adressbereiche

	Externer Zugang nur über sichere Verbindungen (VPN oder TLS-Verschlüsselung) Durchführung regelmäßiger Softwareupdates Automatisierte Schwachstellen-Scans Protokollierung administrativer Systemzugriffe Dokumentation von Konfigurationsänderungen Regelmäßige Überprüfung der Zugangsberechtigungen Betrieb eines separaten Gast-Netzwerks (Gast-WLAN) Einsatz server- und clientseitiger Spamfilter und Antimalwareprogramme (inkl. automatischer Updates) Funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe). Automatisches Netzwerkmonitoring mit Alarmierung. Abschaltung/Sperrung nicht benötigter Dienste und Netzwerkports.
3. Zugriffskontrolle Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Automatische Prüfung der Zugriffsberechtigung mittels Passwort Ausschließliche Menüsteuerung je nach Berechtigung Aufgaben- und Rollenbasiertes Berechtigungskonzept Trennung von Anwendungs- und Administrationszugängen Externer administrativer Zugriff nur im Ausnahmefall und unter Aufsicht von berechtigtem Personal Durchführung regelmäßiger Softwareupdates Protokollierung administrativer Systemzugriffe Dokumentation von Konfigurationsänderungen Personenbezogene Daten, die im Auftrag verarbeitet werden, werden mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik verschlüsselt gespeichert Zugriff auf Backups nur für Administratoren möglich Backups werden mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik verschlüsselt Löschung und Vernichtung von Datenträgern gemäß BSI-Empfehlungen
4. Trennungsgebot Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können	Zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden voneinander getrennt verarbeitet Trennung von Test- und Produktionsumgebungen Trennung Managementnetz von Produktionsnetz Daten, die im Auftrag verarbeitet werden, werden für jeden Auftraggeber separat auf eigenständigen, getrennten Systemen verarbeitet

INTEGRITÄT

1. Weitergabekontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Übermittlung personenbezogener Daten mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik (Kryptokonzept) Verschlüsselung von mobilen Endgeräten mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik Löschung und Vernichtung von Datenträgern gemäß BSI-Empfehlungen
2. Eingabekontrolle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	Protokollierung zur nachträglichen Überprüfung der Datenverarbeitung(ssysteme) von: - erfolgreiche und gescheiterte An- und Abmeldevorgänge - Firewall-Protokollierung (TCP/IP) - Protokollierung administrative Tätigkeiten über Ticketsystem Aufbewahrungsfristen für Backups sind festgelegt
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO) Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können	Alle Datenverarbeitungsanlagen, auf denen personenbezogene Daten gespeichert werden, befinden sich in ISO/IEC 27001:2013-zertifizierten Rechenzentren ausschließlich in Deutschland. Personenbezogene Daten werden mithilfe automatischer Wiederherstellungs- und Failover-Mechanismen in drei Verfügbarkeitszonen innerhalb eines Rechenzentrums repliziert. Automatisierte Überwachung der gesamten Anlage auf Verfügbarkeit und ordnungsgemäßen Betrieb Protokollierung und Meldung abnormer Ereignisse an zuständige Mitarbeiter Sicherung personenbezogener Daten erfolgt mindestens täglich auf ein eigenständiges, unabhängiges Backupsystem gemäß eines Datensicherungskonzeptes Automatische Funktionsüberwachung der Datensicherung Regelmäßige, stichprobenartige Prüfung der Wiederherstellbarkeit der Daten Antimalwareprogramme sind vorhanden und werden immer auf dem aktuellen Stand gehalten

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

1. Datenschutz-Management

Ein Datenschutzmanagementsystem ist umgesetzt. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen.

2. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können.

3. Auftragskontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Alle inSign-Mitarbeiter sind hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert. Sollte inSign bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden technisch-organisatorische Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO und Art 32 Abs. 1 DSGVO sichergestellt. Voraussetzungen für das Eingehen eines Unterauftragsverhältnisses: - Vertrag zur Auftragsverarbeitung nach Vorgabe Art. 28 Abs. 3 DSGVO - Datenverarbeitung erfolgt ausschließlich innerhalb der EU, bevorzugt in Deutschland - Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse Wenn möglich Zertifizierung der Dienstleister nach ISO27001:2013 Prüfungen und Audits der mit dem Dienstleister vereinbarten Maßnahmen Auf technische Umgebungen von Dienstleistern werden Zugriffsberechtigungen für inSign Mitarbeiter restriktiv vergeben. Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG (Art. 32 Abs. 1 lit. a DSGVO)

Einsatz geeigneter Kryptographieverfahren zur Verschlüsselung von Kommunikationsverbindungen (encryption in transit) und Daten in Ruhe (encryption at rest) anhand eines Kryptokonzepts.

Anhang IV – Liste der Unterauftragsverarbeiter

Der Verantwortliche stimmt der Beauftragung folgender Unterauftragnehmer durch den Auftragsverarbeiter zu.

Service-Provider	Zweck	Art der verarbeiteten Daten
BSI Business Systems Integration Deutschland GmbH Rheinstraße 97 64295 Darmstadt Deutschland	Umsetzungspartner für den SaaS-Betrieb	Alle Informationen, die zur Erfüllung der Dienstleistung notwendig sind.
Plusserver GmbH Venloer Str. 47 50672 Köln Deutschland	Bereitstellung von Cloud- Rechenzentrumsdienstleistungen (insbesondere Netzwerk, Computing, Storage, Backup)	Hostname und IP-Adresse von Kundenservern, verschlüsselte Kundendaten.
gridscale GmbH Oskar-Jäger-Straße 173 50825 Köln Deutschland	Managed Service/ PaaS & IaaS Cloud Hosting	Hostname und IP-Adresse von Kundenservern. Es findet keine originäre Nutzung oder Verarbeitung von Kundendaten durch den Subunternehmer statt.
IONOS SE Elgendorfer Str. 57 56410 Montabaur Deutschland	Bereitstellung von Cloud- Rechenzentrumsdienstleistungen (insbesondere Netzwerk, Computing, Storage, Backup)	Hostname und IP-Adresse von Kundenservern. Es findet keine originäre Nutzung oder Verarbeitung von Kundendaten durch den Subunternehmer statt.
rapidmail GmbH Augustinerplatz 2 79098 Freiburg i.Br. Deutschland	Bereitstellung von E-Mail-Diensten	Alle Informationen, die für die E-Mail-Kommunikation benötigt werden.
CM.com Germany GmbH Dr. Eugen Schön Straße 35 97332 Volkach Deutschland	Bereitstellung von SMS-Diensten	Alle Informationen, die für die SMS-Kommunikation benötigt werden.
D-Trust GmbH Kommandantenstraße 18 10969 Berlin	Bereitstellung von Diensten für qualifizierte elektronische Signaturen (nur wenn vom Auftraggeber als Option beauftragt)	Alle Informationen, die zum Erstellen von, und Signieren mit, qualifizierten Zertifikaten benötigt werden.

Swisscom Trust Services GmbH Konradstraße 12 8005 Zürich Schweiz	Bereitstellung von Diensten für qualifizierte elektronische Signaturen (nur wenn vom Auftraggeber als Option beauftragt)	Alle Informationen, die zum Erstellen von, und Signieren mit, qualifizierten Zertifikaten benötigt werden.
A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH Landstraßer Hauptstraße 1b, E02 1030 Wien Österreich	Bereitstellung von Diensten für qualifizierte elektronische Signaturen (nur wenn vom Auftraggeber als Option beauftragt)	Alle Informationen, die zum Erstellen von, und Signieren mit, qualifizierten Zertifikaten benötigt werden.
die Bayerische IT GmbH Thomas-Dehler-Str. 25 81737 München Deutschland	Bereitstellung von Cloud- Rechenzentrumsdienstleistungen zur Langzeitarchivierung von Dokumenten	Informationen, die für die verschlüsselte Verarbeitung von Dokumenten benötigt werden. Es findet keine originäre Nutzung oder Verarbeitung von Kundendaten durch den Subunternehmer statt.

Anhang V – Weitere Regelungen

Kosten bei Prüfungen und Unterstützungsleistungen

Der Auftragsverarbeiter führt auf eigene Kosten regelmäßig Kontrollen und Prüfungen gemäß seines Auditprogramms nach anerkannten Standards durch und stellt dem Kunden den Revisionsbericht dieses Audits, zur Zeit des Vertragsabschlusses ISAE 3402 Typ II, nach Anfrage zur Verfügung.

In Ergänzung zum Prüfungsrecht gemäß Klausel 7.6 lit. c) kann der Verantwortliche die Überprüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten anlassbezogen durchführen. Ein Anlass stellt beispielsweise ein wesentlicher Sicherheitsvorfall auf Seiten des Auftragsverarbeiters dar. Die jeweiligen Verdachtsmomente sind vom Verantwortlichen mit der Ankündigung der Überprüfung/Inspektion vorzutragen. Für derartige anlassbezogene Überprüfungen, Inspektionen oder Unterstützungsleistungen kann der Auftragsverarbeiter weder Aufwände noch eine sonstige Vergütung geltend machen, sofern der Anlass vom Auftragsverarbeiter allein verschuldet wurde.

Im Falle sonstiger bzw. anlassloser Überprüfungen, Inspektionen oder für Unterstützungsleistungen kann der Auftragsverarbeiter vom Verantwortlichen eine angemessene Aufwandsentschädigung beanspruchen, sofern dazu personelle Ressourcen des Auftragsverarbeiters gebunden wurden.

Weisungen, Benachrichtigungen oder Meldungen

Sofern die Parteien nach diesen Klauseln verpflichtet sind, sich schriftlich Informationen, Benachrichtigungen oder Meldungen zukommen zu lassen, hat dies mindestens in Textform (z.B. E-Mail) zu erfolgen. Hierbei sind die in Anhang I genannten Kontaktdaten des Verantwortlichen bzw. des Auftragsverarbeiters oder andere zwischen den Parteien vereinbarte Kommunikationswege zu nutzen.

Weisungsbefugte(r) des Verantwortlichen im Sinne Artikel 28 Absatz 3 DSGVO

Weisungsbefugt ist der Lizenznehmer des Onlinedienstes inSign 365.

Änderungen des/der Weisungsbefugte(n) bedürfen der Schriftform oder der Textform in Verbindung mit einer elektronischen Signatur gemäß Art. 26 eIDASVO.

Datenschutzbeauftragter des Verantwortlichen für Meldungen im Sinne Artikel 28 Absatz 3 DSGVO

Meldungen im Sinne Artikel 28 Absatz 3 DSGVO werden an den Weisungsbefugten übermittelt.

Datenschutzbeauftragter des Auftragsverarbeiters

Herr Rechtsanwalt Sascha Weller
IDR – Institut für Datenschutzrecht
Ziegelbräustraße 7
85049 Ingolstadt, Deutschland
datenschutz@bsi-software.com

Verpflichtung zum Geheimnisschutz

Der Auftragsverarbeiter verarbeitet im Rahmen seines Auftrages u.a. Daten, die in den Anwendungsbereich von § 203 Strafgesetzbuch (StGB) fallen (im Folgenden „Geheimnisschutzdaten“) und wirkt insoweit an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mit. Der Auftragsverarbeiter verpflichtet sich, über Geheimnisschutzdaten Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihr zugewiesenen Aufgaben unbedingt erforderlich ist.

Der Verantwortliche hat den Auftragsverarbeiter darauf hingewiesen, dass Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken, sich nach § 203 Abs. 4 S. 1 StGB strafbar machen, wenn sie unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

Der Auftragsverarbeiter wird diejenigen von ihm beschäftigten Personen oder Unterauftragsverarbeiter, die bestimmungsgemäß mit Geheimnisschutzdaten des Berufsgeheimnisträgers in Berührung kommen oder bei denen dies nicht auszuschließen ist, zur Vertraulichkeit hinsichtlich der Geheimnisschutzdaten verpflichten und über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehren.

Anhang VI – Entfallene Optionen

Klausel 1 a

[OPTION 2: Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG]

Klausel 7.7 a

OPTION 1: VORHERIGE GESONDERTE GENEHMIGUNG: Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens [ZEITRAUM ANGEBEN] vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.

Klausel 8 c 4

[OPTION 2: Artikel 33 und Artikel 36 bis 38 der Verordnung (EU) 2018/1725]

Klausel 9.1 b

[OPTION 2: Artikel 34 Absatz 3 der Verordnung (EU) 2018/1725]

Klausel 9.1 c

[OPTION 2: Artikel 35 der Verordnung (EU) 2018/1725]

Klausel 9.2

[OPTION 2: Artikel 34 und 35 der Verordnung (EU) 2018/1725]