Vertrag über die Auftragsverarbeitung personenbezogener Daten

Version 3.2, Stand 02.01.2025

SoSafe SE | Lichtstr. 25a | 50825 Cologne | sosafe.de

1. Standardvertragsklauseln

Die Parteien stimmen dem Text des Durchführungsbeschlusses (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates zu.

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.

Klausel 5

Kopplungsklausel

(a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

(b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

(c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

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 Verfügun.

7.7. **Einsatz von Unterauftragsverarbeitern**

(a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: 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 14 Kalendertage 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.

Anhang I – Liste der Parteien

Verantwortlicher

Die Kontaktperson, die der Kunde nach Unterzeichnung des Hauptvertrags im SoSafe Manager benannt hat, ist der primäre Empfänger von Mitteilungen.
Bis zur Benennung dieser Person werden Mitteilungen an den spätestens zu Beginn der Implementierung der Awareness-Building-Leistungen im SoSafe-Manager hinterlegten Administrator des Kunden weitergeleitet.

Auftragsverarbeiter

SoSafe SE
Lichtstr. 25a
50825 Köln

Datenschutzbeauftragter

Herr Sebastian Herting
Herting Oberbeck Datenschutz GmbH
Hallerstraße 76
20146 Hamburg
E-Mail: dpo@sosafe.de

Hinweis: Bitte übermitteln Sie eine Kopie sämtlicher Mitteilungen an privacy@sosafe.de

Anhang II – Beschreibung der Verarbeitung

1. Gegenstand

Die Leistungen des Auftragsverarbeiters, die die Grundlage für die Verarbeitungstätigkeiten des Auftragsverarbeiters gemäß diesem Auftragsverarbeitungsvertrag bilden, sind im Hauptvertrag detailliert festgelegt. Die Verarbeitung personenbezogener Daten auf Weisung des Verantwortlichen im Rahmen dieses Auftragsverarbeitungsvertrags bezieht sich insbesondere auf Folgendes:

Bereitstellung einer Software-as-a-Service-Plattform für Human Risk Management, Schulungen und Nutzertests. Gemäß der vom Verantwortlichen getroffenen Auswahl der jeweiligen Awareness-Building-Leistungen erhalten die Nutzer des Verantwortlichen oder seiner verbundenen Unternehmen im Rahmen des Hauptvertrags Zugang zu Social-Engineering-Simulationen (z. B. Phishing, Smishing, Vishing), Fragebögen, Tests, optionalen KI-gestützten Chatbots und Tools sowie anderen nutzerzentrierten Mechanismen zur Erstellung von Risikoprofilen. Schulungen zum Sicherheitsbewusstsein, Analysen, Feedback-Mechanismen sowie technische und verfahrenstechnische Eingriffe können automatisch oder manuell ausgelöst werden, je nach Konfiguration des Verantwortlichen, oder anderweitig als Ergebnis der Nutzerinteraktion mit der Plattform oder der von der Plattform aufgenommenen Daten über technische Integrationen mit anderen Geschäftssystemen des Verantwortlichen, wie vom Verantwortlichen implementiert oder anderweitig spezifiziert.

Die Plattform kann ein personalisiertes Profil des jeweiligen Nutzers erstellen und automatisierte Maßnahmen ergreifen, um das sichere Verhalten des Nutzers zu melden oder zu verbessern, vorbehaltlich der vom für die Verarbeitung Verantwortlichen gewählten Anonymisierungseinstellungen.

2. Dauer

Die Dauer der Verarbeitung durch den Auftragsverarbeiter hängt grundsätzlich von der Dauer des Hauptvertrags ab. Die Verarbeitung und dieser Vertrag über die Auftragsverarbeitung enden daher jedenfalls mit der Beendigung des Hauptvertrags (zuzüglich der jeweils anwendbaren Aufbewahrungsdauer nach Vertragsende gemäß dem Löschungskonzept), sofern sich aus den Bestimmungen dieses Auftragsverarbeitungsvertrags keine fortgeltenden Verpflichtungen ergeben bzw. keine vorzeitige Kündigung dieses Auftragsverarbeitungsvertrags erfolgt.

3. Zweck der Verarbeitung

Die Verarbeitung dient dem folgenden Zweck: Es soll dem Auftragsverarbeiter ermöglicht werden, gegenüber den Nutzern die vom Verantwortlichen erworbenen Awareness-Building-Leistungen zu erbringen.

4. Art der Daten

Die folgenden Arten von personenbezogenen Daten, die sich alle auf Nutzer beziehen, werden vom Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Erbringung der Awareness-Building-Leistungen verarbeitet, so wie im Hauptvertrag näher ausgeführt.

(1) Registrierungs- und Account Management-Daten

Alle Awareness-Building-Leistungen verarbeiten bestimmte Datenarten, die von Nutzern zur Registrierung für die Awareness-Building-Leistungen und für ihre Verwaltung im Auftrag des Verantwortlichen benötigt werden ("**Registrierungs- und Account Management-Daten**"). Zu diesen gehören insbesondere:

- Vor- und Nachname
- Geschäftliche E-Mail-Adresse
- Zugewiesene Benutzergruppen (z. B. Organisationseinheit, Standort, Rolle), Zugriffsberechtigungen
- *Optionale* weitere Nutzerpräferenzen, wie z.B. Sprache und Anredeform

(2) Nutzungsdaten

Zusätzlich zu den Registrierungs- und Account Management-Daten können je nach gewählter Awareness-Building-Leistung weitere Datenarten in Bezug auf Nutzer verarbeitet werden, um die Awareness-Building-Leistungen zu betreiben und zur Verrfügiung zu stellen, wie im Hauptvertrag näher spezifiziert. Dies schließt insbesondere ein:

- Nutzer-Scoping und Anpassung von Informationen wie Rolle, Abteilung, anfänglicher Wissensstand und Antworten auf einführende Fragebögen;
- Nutzeraktivitäten auf der Plattform, wie z. B. Beginn und Abschluss von Schulungen, Testergebnisse und Interaktion mit Tests;
- Informationen zur Stellung des Nutzers innerhalb der Organisation des Verantwortlichen (z.B. Information zu Vorgesetzten).
- Optionale KI-Module: Interaktion mit KI-gestützten Chatbots und Tools, soweit sie personenbezogene Daten enthalten, basierend auf den Eingaben, die der Auftragsverarbeiter vom Benutzer des KI-Moduls des Verantwortlichen erhalten hat.
- Optionales PhishFeedback-Modul: Einstellungen für Benutzerregionen (z. B. Sprache, Zeitzone) und gemeldete E-Mails, die jeweils personenbezogene Daten enthalten können.

(3) Technische Daten

Daten in Bezug auf Nutzer, die erforderlich sind für den Betrieb der Anwendung und der Infrastruktur und für die Erfüllung der Verpflichtungen der technischen und organisatorische Maßnahmen. Hierzu zählen insbesondere Folgende personenbezogene Daten:

- Nutzerbezogene Systeminformationen, die von der Anwendung benötigt werden, wie z. B. Browserversion und -plattform, Informationen zum User-Agent;
- Netzwerkdaten wie IP-Adresse, Zeitstempel, URL und API-Endpunkte, auf die zugegriffen wird;
- Mail-Daten wie Absender- und Empfängeradressen, Routing-Informationen und Zeitstempel; und
- Daten, die von Integrationen gesammelt werden, die vom Verantwortlichen angefordert oder implementiert werden, einschließlich Organisations- oder Nutzerdaten, wie z. B. Warnungen von DLP-Tools (Data Loss Prevention), Endpunkterkennungs- und Response Agenten.

5. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind, sofern im Hauptvertrag nicht anderweitig bestimmt, sämtliche vom Verantwortlichen zur Teilnahme bestimmten Nutzer. Dem Verantwortlichen ist es freigestellt, einzelnen Nutzern per „Opt-Out“-Verfahren eine Nicht-Teilnahme zu ermöglichen.

Anhang III – Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragsverarbeiter mindestens einzurichten und laufend aufrechtzuerhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Konfigurierbare Anonymisierung und zweckbezogener Zugriff auf Daten

Alle Leistungen des Auftragsverarbeiters können so konfiguriert werden, dass Kundenadministratoren standardmäßig nur anonymisierten, aggregierten Zugriff auf Nutzerdaten erhalten. Der Zugang für bestimmte Mitarbeiter des Verantwortlichen auf individueller Ebene kann konfiguriert werden, wenn der für die Verarbeitung Verantwortliche dies klar und ausdrücklich anfordert.

2. Verschlüsselung

2.1 Data in Transfer

Sämtliche Datenübertragungen (sowohl zwischen dem Verantwortlichen und dem Auftragsverarbeiter als auch zwischen Mitarbeitern des Auftragsverarbeiters) sind stark verschlüsselt in Übereinstimmung mit anerkannten Verfahren der Branche, wie z. B. ECC mit Curve25519, RSA mit einem Schlüssel von 2048 Bit oder länger, und werden entsprechend des fortschreitenden Stands der Technik aktualisiert. Der interne Netzwerk- und Verwaltungszugriff des Auftragsverarbeiters ist stark verschlüsselt. Die Kommunikation mit Service-Endpunkten erfordert eine sichere Verbindung .

2.2 Data at Rest

Sämtliche personenbezogenen Verantwortlichen- und Nutzerdaten werden von der Plattform auf Speicherebene unter Verwendung von branchenweit anerkannten Algorithmen und Implementierungen, wie z. B. AES-256-GCM oder höher, angemessen verschlüsselt.

2.3 Data in Use

Bei der Lösung des Auftragsverarbeiters handelt es sich um eine reine Cloud-Anwendung, bei der das Frontend auf dem Computer des Endnutzers betrieben wird. Hier besteht keine Möglichkeit der Verschlüsselung.

3 Vertraulichkeit

3.1 Physische Zugangskontrolle

Die Räumlichkeiten der Büros des Auftragsverarbeiters sind jeweils nur mit Schlüsseln bzw. Transpondern mit passenden Sicherheitsschlössern zugänglich. Die Ausgabe der Schlüssel und Transponder wird von der Geschäftsführung des Auftragsverarbeiters protokolliert und gegengezeichnet. Geeignete Einbruchmeldeanlagen, CCTV-Abdeckung und Reaktionsverfahren sind vorhanden. Büros des Auftragsverarbeiters bieten keine speziellen Netzwerkzugriffsrechte, die über den Zugriff auf das Internet hinausgehen.

Die SoSafe-Plattform wird von branchenführenden Hyperscale-Cloud-Service-Providern gehostet. Diese Anbieter arbeiten von Rechenzentren aus und implementieren angemessene physische und umgebungsbezogene Sicherheitskontrollen, wie z. B.:

- Verfolgung und Überwachung aller Besucherzugänge und Personalbewegungen
- CCTV-Überwachung mit 90 Tagen Aufbewahrungsfrist
- Starke Zugangskontrolle zu allen Datenhosting-, Netzwerk-, Maschinen- und Umgebungsräumen
- Mindestens N+1-Redundanz von Strom-, Netz- und Umweltdiensten

Cloud Service Provider müssen über eine ISO 27001- und/oder SOC2-Akkreditierung oder ähnliches verfügen. Der Auftragsverarbeiter bewertet ihre physische Sicherheit durch die Überprüfung von Audit- und Akkreditierungsmaterialien.

3.2 Logische Zugangskontrolle

Für alle logischen Zugriffe ist eine authentifizierte VPN-Verbindung mit Multi-Faktor erforderlich. Die Büronetzwerke gewähren keine besonderen Netzwerkprivilegien, die über den Zugriff auf das Internet hinausgehen. Die Authentifizierung bei Geschäftssystemen des Auftragsverarbeiters erfolgt über SSO und erfordert eine Multi-Faktor-Authentifizierung und starke, richtliniendefinierte Passwörter gemäß den anerkannten Verfahren der Branche. Der gesamte Systemzugriff, einschließlich des Zugriffs auf Kundendaten, wird nur auf einer überprüfbaren, bereichsbezogenen und need-to-know-Basis bereitgestellt. Die internen Zugriffsrechte der Nutzer werden regelmäßig überprüft.

3.3 Endpunkt-Sicherheit

Alle Endnutzergeräte werden sicher von Mobile Device Management konfiguriert, um alle Kontrollen durchzusetzen und Endpoint Detection and Response-Agenten zu verwenden. Eine vollständige Festplattenverschlüsselung ist vorhanden. Bei Endnutzergeräten tritt nach höchstens fünf (5) Minuten Inaktivität eine Zeitüberschreitung auf. Alle Endgeräte verfügen über eine individuelle Antiviren- und Firewall-Software mit automatischer Update-Funktion. Aktualisierungen der Endnutzergeräte, des Betriebssystems und der wichtigsten Softwarepaketversionen werden ordnungsgemäß verwaltet.

3.4 Weitergabekontrolle

Der Datenverkehr mit personenbezogenen Daten wird minimiert und auf das zur Erbringung der Leistungen erforderliche Maß beschränkt. Auf der Seite des Auftragsverarbeiters haben nur die relevanten und notwendigen Mitarbeiter Zugriff auf personenbezogene Daten (auf einer Need-to-know-Basis).

Es besteht eine Richtlinie für die Fernarbeit und geeignete Kontrollen. Die Speicherung personenbezogener Daten auf Endgeräten der Nutzer ist nicht gestattet. Alle Mitarbeiter sind vertraglich zur Verschwiegenheit und zum Schutz von Geschäftsgeheimnissen verpflichtet.

Eine Bring Your Own Device (BYOD)-Risikobewertung wurde gemäß ISO 27001 durchgeführt, und es gibt eine entsprechende Richtlinie, um die Verwendung und die von BYOD ausgehenden Risiken zu begrenzen. Entsprechende zentral verwaltete Kontrollen sind vorhanden.

3.5 Löschung von Daten

Die seitens des Auftragsverarbeiters eingesetzten Cloud-Service-Provider stellen die logische Datenvernichtung gemäß anerkannten Verfahren der Branche bereit.

Systemprotokolle und Sicherheitsdaten können bis zu 12 Monate ab dem Zeitpunkt der Erstellung aufbewahrt werden, um eine angemessene Reaktion auf Sicherheitsvorfälle und Forensik zu ermöglichen. Systemsicherungen sind angemessen geschützt, und alle darin enthaltenen Nutzerdaten werden innerhalb von 12 Monaten nach der Erstellung gemäß den Sicherungsrichtlinien des Auftragsverarbeiters gelöscht.

3.6 Trennungskontrolle

Es besteht eine Trennung von Produktiv-, Test-/Entwicklungs- und Verwaltungssystemen. Datenbankrechte wurden festgelegt und es erfolgt eine softwareseitige, logische Mandantentrennung, die durch Datenbanklogik durchgesetzt wird.

4 Integrität

Zugriffe auf die Datenbanken der Produktivsysteme werden protokolliert und zwölf (12) Monate gespeichert. Geeignete Sicherungs- und Wiederherstellungsverfahren sind vorhanden, um die Datenintegrität zu schützen. Der Zugriff auf Datenbanken ist rollenbasiert eingeschränkt.

5 Verfügbarkeit

5.1 Business Continuity

Die Produktivsysteme und Server werden durch den Auftragsverarbeiter kontinuierlich überwacht, um eine ständige Verfügbarkeit zu gewährleisten. Der Auftragsverarbeiter betreibt eine angemessene Architektur und ein Business-Continuity-System im Rahmen des ISO 27001-Audits und der Akkreditierung, die geeignet sind, die im Hauptvertrag definierten SLAs zu erfüllen. Die Server und produktiven Systeme werden jeden Tag kontinuierlich durch ein vollständiges Back-up sichergestellt. Backups werden verschlüsselt und auf separaten Serversystemen des Auftragsverarbeiters gespeichert. Zugriff wird nur den Administratoren des Auftragsverarbeiters gewährt.

5.2 Security Awareness und Training

Sämtliche Mitarbeiter des Auftragsverarbeiters werden laufend und umfassend (Seminare, eigenes E-Learning sowie interaktive Formate wie Quizze) zu den Datenschutzvorgaben sowie zu grundlegenden Themen der Informationssicherheit geschult.

6 Incident Management

Der Auftragsverarbeiter betreibt angemessene Maßnahmen zur Sicherheitsüberwachung, Erkennung von Vorfällen und Reaktion, einschließlich technischer Protokollierung und automatisierter Auditkontrollen, eines Security Operations-Teams und -Funktionen sowie unternehmensweiter Incident-Response-Prozesse. Alle signifikanten Sicherheitsvorfälle, einschließlich Beinaheunfälle, lösen ein eine formelle Retrospektive und Ursachenanalyse aus.

7 Informationssicherheits-Managementsystem

Der Auftragsverarbeiter betreibt ein formelles Informationssicherheitsmanagementsystem (ISMS) gemäß den Anforderungen der ISO 27001, das extern geprüft und akkreditiert ist. Darüber hinaus holt der Auftragsverarbeiter bei Bedarf weitere Industrieakkreditierungen wie TISAX ein. Die formellen Richtlinien und Verfahren für die Risikobewertung und das Risikomanagement werden von der Sicherheitsorganisation durchgeführt, wobei der Sicherheitsausschuss (Security Committee) regelmäßig Beiträge leistet und dem Sicherheitsausschuss Bericht erstattet, der sich aus den relevanten Mitgliedern des Sicherheits- und Führungsteams zusammensetzt. Das ISMS wird formal von der Geschäftsleitung und dem CEO unterstützt.

Das ISMS und alle Sicherheitsfunktionen werden von einer angemessen ausgestatteten Sicherheitsorganisation unter der Leitung eines Chief Information Security Officers betrieben.

8 Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen

Alle relevanten Sicherheits-, Datenschutz- und Betriebsprozesse werden jährlich von qualifizierten, fachkundigen Auditoren intern geprüft, und an das ISMS und den Sicherheitsausschuss berichtet. Das ISMS des Auftragsverarbeiters wird mindestens einmal im Jahr von einem anerkannten Fachunternehmen formell extern geprüft.

Annex IV – Liste der Unterauftragsverarbeiter

Bitte besuchen Sie https://sosafe-awareness.com/de/legal/sub-processors/ um eine aktuelle Liste der Unterauftragsverarbeiter, Verarbeitungsaktivitäten und Schutzmaßnahmen zu erhalten.

SoSafe SE | Lichtstr. 25a | 50825 Cologne | Geschäftsführer: Dr. Niklas Hellemann, Felix Fichtl | HRB121629 | Amtsgericht Köln | VAT ID: DE322382415 |
Visitor address and parking: Lichtstr. 25a | 50825 Köln | Tel: +49 (0) 221 6508 3800 |
Email: info@sosafe.de | Web: sosafe.de