Vertrag über die Auftragsverarbeitung personenbezogener Daten

Version 3.0, updated 13.12.2023

SoSafe GmbH | 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

[Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen]

Name: Geben Sie hier den Namen des Verantwortlichen an

Anschrift: Geben Sie hier die Anschrift des Verantwortlichen an

Name, Funktion und Kontaktdaten der Kontaktperson: Unterschrift und Beitrittsdatum:

Geben Sie hier den Namen, die Funktion und die Kontaktdaten der Kontaktperson an

Auftragsverarbeiter

SoSafe GmbH
Lichtstr. 25a
50825 Köln

Datenschutzbeauftragter

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

Felix Schürholz, Geschäftsführer Unterschrift und Beitrittsdatum:

22 April 2024 | 08:37 PDT DocuSigned by: Felix Schürholz 6459695B96B249C...

DS sosaf SoSafe GmbH straße 25a, 50825 de | +49 (0) 221

Anhang II – Beschreibung der Verarbeitung

1. Gegenstand

Der Auftragnehmer übernimmt im Rahmen seiner Leistungserbringung insbesondere – eine abschließende Aufzählung ergibt sich aus dem Hauptvertrag – folgende Tätigkeiten, bei denen personenbezogene Daten verarbeitet werden:

(1) Durchführung anonymer Phishing-Simulationen

Versand von Phishing-Mails:

- Auf Basis der vom Auftraggeber zur Verfügung gestellten Arbeitnehmer-E-Mail-Adressen und Namen von Arbeitnehmern (im Folgenden: „**Nutzer**“) versendet der Auftragnehmer eine definierte Anzahl an E-Mail-Templates über einen definierten Zeitraum.
- Die E-Mail-Templates sind dabei personalisiert, d.h. sie enthalten eine persönliche Ansprache mit dem jeweiligen Namen des Nutzers, um einen realistischen Phishing-Angriff zu simulieren.
- Falls vom Auftraggeber gewünscht, erfolgt eine differenzierte Ausspielung nach zusätzlichen Ordnungskriterien (z. B. Organisationseinheit, Standort, Zugehörigkeit zum Management). Die Gruppierungen von Empfängern/Nutzern, die sich aus diesen Ordnungskriterien ergeben, müssen aber stets mindestens fünf (5) Personen beinhalten.
- Jede einzelne E-Mail enthält zudem einen identischen Link zu einer unsichtbaren Bilddatei („Tracking Pixel“), die beim Öffnen der E-Mail heruntergeladen wird.

Rückmeldung an die Nutzer im Rahmen von Lernseiten im Browser:

- Die E-Mail-Templates enthalten jeweils einen eigenen Template-spezifischen, aber für alle Nutzer des Auftraggebers identischen Link, der auf eine Lernseite führt, welche auf einem Webserver des Auftragnehmers gehostet wird.
- Beim Klick auf den Link werden die Nutzer auf die Lernseite geführt und werden hier anhand der konkreten E-Mail (jedoch mit nicht-personalisierter Ansprache) darüber aufgeklärt, wie sie die Mail als Phishing-Mail hätten erkennen können.

Nutzung des Phishing-Melde-Buttons:

- Optional kann ein Add-In für verschiedene Mailprogramme (u.a. Microsoft Outlook) installiert werden, über welches Nutzer verdächtige E-Mails melden können. Stammt die entsprechende Mail aus der Simulation, fließt der Klick in die sog. Melderate in der Auswertung ein. Die aufgezeichneten Daten werden anonymisiert und nur anonymisierte Daten werden an den Kunden gesendet. Entstammt die Mail nicht der Simulation, wird sie an eine vom Auftraggeber definierte E-Mail-Adresse weitergeleitet. In diesem Fall erfolgt keine Rückmeldung bzw. kein Datenfluss an den Auftragnehmer.

(2) Bereitstellung einer E-Learning-Plattform:

- Nutzer können sich mit ihrer beruflichen E-Mail-Adresse unter https://elearning.sosafe.de/registration auf der Plattform des Auftragnehmers für das E-Learning-Portal registrieren und haben Zugriff auf alle für sie freigeschalteten bzw. vom Auftraggeber

bestellten E-Learning-Module. Pro Modul kann zum Abschluss ein kurzes Quiz beantwortet werden. Basierend auf den Antworten wird ein Ergebniswert berechnet (auf Basis der Anzahl an richtigen Antworten). Dieses Quiz kann beliebig oft wiederholt werden.

- Alternativ können die E-Learning-Module als SCORM-Datei dem Auftraggeber zur Verfügung gestellt werden, um in ein bereits bestehendes Learning Management System integriert zu werden.

(3) Bereitstellung einer Auswertung (Reporting-Dashboard):

- Auf Basis der Gesamtanzahl der versendeten E-Mails kann auf die Öffnungs-, Antwort-, Eingabe- und Klickraten (gesamthaft und pro etwaig definierter Gruppierung nach Ordnungskriterien, vgl. Ziffer 1.1 (1)) rückgeschlossen werden. Diese Informationen werden dem Auftraggeber auf einem Auswertungsportal zur Verfügung gestellt – ein personenbezogenes Tracking ist jedoch nicht möglich, da jede Organisationseinheit mindestens fünf (5) Personen enthalten muss.
- Wird für das E-Learning die Plattform des Auftragnehmers genutzt, so werden Registrierungsraten, Fortschritt in den Modulen und Ergebnisse der E-Learning-Quizze für die einzelnen Nutzer erfasst und (sofern nicht anders vereinbart) an den Auftraggeber zurückgemeldet.
- Bei Nutzung des Phishing-Melde-Buttons wird die Melderate (d.h. wie viele Mails aus der Simulation durch die Nutzer als Phishing-Versuch erkannt wurden) ebenfalls gesamthaft und pro etwaig definierter Gruppierung erfasst und an den Auftraggeber zurückgemeldet.

2. Dauer

Die Dauer der Verarbeitung durch den Auftragnehmer hängt grundsätzlich von der Dauer des Hauptvertrags ab. Die Verarbeitung und dieser Vertrag über die Auftragsverarbeitung enden daher jedenfalls mit der Beendigung des Hauptvertrags, sofern sich aus den Bestimmungen dieses Vertrags über die Auftragsverarbeitung keine fortgeltenden Verpflichtungen ergeben bzw. keine vorzeitige Kündigung dieses Vertrags über die Auftragsverarbeitung erfolgt. Eine Geltung der Verpflichtungen aus diesem Vertrag über die Auftragsverarbeitung findet bereits für den Zeitraum Anwendung, wenn ein „alter“ Hauptvertrag durch einen zu diesem Vertrag über die Auftragsverarbeitung gehörenden „neuen“ Hauptvertrag mit vergleichbaren datenschutzrechtlichen Anforderungen abgelöst bzw. angepasst wird und daher übergangsweise eine Verarbeitung von personenbezogenen Daten ohne Hauptvertrag erfolgt. Es wird insoweit eine ununterbrochene Verarbeitung im Auftrag durch den Auftragnehmer vereinbart, es sei denn die Parteien regeln in dem „ablösenden“ bzw. „angepassten“ Hauptvertrag etwas Abweichendes. Die Dauer der Verarbeitung richtet sich dann nach dem „ablösenden“ bzw. „angepassten“ Hauptvertrag.

3. Zweck der Verarbeitung

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

4. Art der Daten

Es werden folgende personenbezogene Daten erhoben und verarbeitet (entsprechend der im Hauptvertrag definierten Leistung):

(1) Versand der Phishing-E-Mails
- Vor- und Nachname der Nutzer
- Akademischer Grad (optional)
- Berufliche E-Mail-Adresse der Nutzer
- Geschlecht der Nutzer (optional)
- Zugehörige Nutzergruppen (z. B. Organisationseinheit, Standort, Funktion) des Auftraggebers
- Weitere Ordnungskriterien, falls erforderlich (s. Ziffer 1.1)
- Sprache der Nutzer
- Browser/Browserversion und Plattform der Nutzer
- Teilnahme am Awareness-Building (= kein Opt-Out gemäß Ziffer 5)

Diese Daten werden in einer gesicherten Datenbank (s. Anlage III) zum Zweck des individualisierten Versands gespeichert. Nach Beendigung der Leistungen des Hauptvertrags werden sie unwiderruflich gelöscht.

(2) Rückmeldung an die Nutzer im Rahmen von Internet-Lernseiten
- Aufruf der Lernseiten an sich (ohne weitere Datenpunkte wie IP-Adressen oder Geo-Location-Daten – diese werden entweder nicht erhoben oder von einem regelmäßigen Mechanismus aus den Server-Log-Daten gelöscht)
- Anzahl der aufgerufenen Tooltipps/Hinweistexte
- Optionale Feedback-Bewertung bzw. Feedback-Freitext

(3) E-Learning-Plattform

Bei der Registrierung auf der E-Learning-Plattform sowie bei deren weiterführender Nutzung:

- Vor- und Nachname des Nutzers
- Berufliche E-Mail-Adresse des Nutzers
- Sprache des Nutzers
- Geschlecht des Nutzers
- Bearbeitungsstatus der einzelnen E-Learning-Module je Nutzer
- Ergebnisse der die Module abschließenden Quizze je Nutzer

Im Rahmen der Rückmeldung an den Auftraggeber:

- Namen der angemeldeten Nutzer
- Bearbeitungsstatus aller Module (aggregiert)
- Durchschnittlicher Quiz-Wert bzw. prozentuale Richtigkeit der Antworten der abschließenden Quizze (aggregiert)
- Bearbeitungsstatus aller Module pro Nutzer
- Quiz-Wert bzw. prozentuale Richtigkeit der Antworten der abschließenden Quizze pro Nutzer (optional)

(4) Escalation Manager

Wenn der Auftraggeber die Funktion Escalation Manager gebucht hat, werden die folgenden personenbezogenen Daten erhoben und verarbeitet. Zu Eskalationszwecken werden sie auch an den Auftraggeber übermittelt:

- Vor- und Nachname, berufliche E-Mail-Adresse und zugehörige Nutzergruppen der Nutzer des Auftraggebers
- Individueller Fertigstellungsstatus aller Module
- Deadline der Kampagne
- Information, ob der Nutzer einen Account erstellt hat oder nicht (ja/nein)
- Information, ob der Nutzer neu im E-Learning ist (Nutzer hat sich in den letzten 90 Tagen registriert: ja/nein

(5) Server-Logs

Die folgenden technischen Informationen werden für zwölf (12) Wochen bis maximal 6 Monate in serverseitigen Logs gespeichert:

- IP-Adressen
- User-Agent
- URL, auf die zugegriffen wurde
- Zeit

(6) Mail-Logs

Die folgenden technischen Informationen werden für zwölf (12) Wochen in serverseitigen Logs gespeichert:

- E-Mail-Adresse
- Versender
- Annehmender E-Mail-Server
- Zeit

5. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind, sofern im Hauptvertrag nicht anderweitig bestimmt, sämtliche vom Auftraggeber zur Teilnahme bestimmten Nutzer. Dem Auftraggeber 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 Auftragnehmer mindestens einzurichten und laufend aufrechtzuerhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Anonymisierung

Personenbezogene Daten werden im Rahmen der Durchführung und Verarbeitung der Phishing-Simulation nicht erhoben. Sämtliche Verhaltensdaten (z. B. Klicks auf Links in den simulierten Phishing-Mails) werden nicht personenbezogenen Daten, sondern zufällig generierten Codes zugeordnet und gemeinsam mit diesen gespeichert. Dieser Vorgang der Anonymisierung wird durch das System automatisch durchgeführt (Privacy-by-Design-Ansatz).

2. Verschlüsselung

2.1 Data in Transfer

Sämtliche Datenübertragungen (sowohl zwischen dem Auftraggeber und dem Auftragnehmer als auch zwischen Mitarbeitern des Auftragnehmers) sind gemäß den Empfehlungen des BSI zur Verschlüsselung verschlüsselt. Mit der Integration von AWS werden wir die empfohlene ELBSecurityPolicy-2016-08 aus den vordefinierten SSL-Sicherheitsrichtlinien von AWS anwenden. Dies beinhaltet TLS 1.2 mit SHA 256, ECDHE-Schlüsselaustausch und ECDSA zur Authentifizierung mit AES 128 zur Verschlüsselung als Mindestanforderung. Der Netzwerkzugang erfordert eine VPN-Verbindung. Die Kommunikation mit Service-Endpunkten erfordert eine sichere Verbindung
.

2.2 Data at Rest

Sämtliche personenbezogenen Auftraggeber- und Nutzerdaten (z. B. die Mail-Adressen der Nutzer) werden in geschützten Datenbanken (Berechtigungssystem, Passwort-Policy mit den u. g. Attributen, SSH-Zertifikat, Zugriff nur aus dem internen IP-Bereich möglich) verschlüsselt gesichert. Die Blockspeicherverschlüsselung wird für Daten im Ruhezustand unter Verwendung der AWS SYMMETRIC_DEFAULT_Policy verwendet. Dies entspricht dem symmetrischen Algorithmus AES-256-GCM, einem Industriestandard für sichere Verschlüsselung. Mit AES-256-GCM verschlüsselte Daten sind jetzt und in Zukunft geschützt, da er als quantenresistent gilt.

2.3 Data in Use

Bei der Lösung des Auftragnehmers 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 Zutrittskontrolle

Die Räumlichkeiten der Büros des Auftragnehmers sind jeweils nur mit Schlüsseln bzw. Transpondern mit passenden Sicherheitsschlössern zugänglich. Die Ausgabe der Schlüssel und Transponder wird von der Geschäftsführung des Auftragnehmers protokolliert und gegengezeichnet. Darüber hinaus besteht in den Räumlichkeiten eine Rezeption bzw. permanent anwesende Mitarbeiter, die eine weitere Zugangskontrolle sicherstellen. Zusätzlich existiert eine Videoüberwachung aller Zugänge.

3.2 Zugangskontrolle

Es bestehen dedizierte Vorgaben für die Vergabe von Passwörtern (zufallsgeneriert, mindestens zwölf (12) (in der Regel länger, wenn wir Passwort-Manager verwenden) Zeichen lang, Groß-/Kleinschreibung, Ziffern und Sonderzeichen) für sämtliche Systeme, in denen personenbezogene Daten verarbeitet werden. Passwörter sind in periodischen Abständen zu ändern. Diese Anforderungen sind über technische Maßnahmen unmittelbar in den Systemen umgesetzt wenn möglich. Es ist sichergestellt, dass alle befugten Personen informiert sind, dass Passwörter sicher zu verwahren sind und nicht weitergegeben werden. Die beauftragten Personen sind informiert, nur einzigartige Passwörter zu verwenden, d.h. Passwörter, die vom Nutzer bei keinen anderen (insbesondere privaten) Systemen verwendet werden. Alle Clients werden nach spätestens fünf (5) Minuten der Inaktivität gesperrt. Sämtliche Clients besitzen eine individuelle Antivirus- und Firewall-Software, die über eine automatisierte Update-Funktionalität verfügt.

Zur Sicherstellung des Zugriffs auf Server-Systeme, die personenbezogene Daten verarbeiten, durch die richtigen Personen wird eine 2-Faktor-Authentifizierung genutzt. Auch wird eine Hardware- und Software-Firewall zur Absicherung des Unternehmensnetzwerks des Auftragnehmers eingesetzt und der Auftragnehmer verfügt über ein Netzwerk- und Netzwerkzonenkonzept. Es wird eine Software für das Mobile Device Management genutzt und VPN-Technologie für den externen Zugang zum Unternehmensnetzwerk des Auftragnehmers eingesetzt.

3.3 Zugriffskontrolle

Der Zugang sowohl zu den Datenbank-Systemen als auch dem Application-Management-System erfolgt nach dem need-to-know-Prinzip, d.h. der IT-Administrator vergibt die Benutzerrechte im Rahmen des Notwendigen nur für Mitarbeiter, die mit dem Administrieren von Kampagnen betraut sind. Sämtliche internen Zugriffe auf die Datenbank-Systeme werden protokolliert und regelmäßig durch den IT-Administrator geprüft. Die Protokolle werden revisionssicher gespeichert. Die Protokolle umfassen die Dokumentation der Berechtigungsvergaben. Die Berechtigungen für Produktiv-, Test-, Entwicklungs- und Verwaltungssysteme werden getrennt vergeben.

3.4 Weitergabekontrolle

Datenverkehr mit personenbezogenen Daten wird grundsätzlich minimiert und auf das nötige Maß zur Erbringung der Leistung beschränkt. Auf der Seite des Auftragnehmers haben nur die verantwortlichen Projektmanager und die IT-Administratoren Zugriff auf die personenbezogenen Daten.

Es existiert eine Home-Office-Regelung. Die Verarbeitung personenbezogener Daten erfolgt im Frontend der SoSafe Management Software. Sämtliche Datenübertragungen (sowohl zwischen dem Auftraggeber und dem Auftragnehmer als auch zwischen Mitarbeitern des Auftragnehmers) auf die SoSafe Management Software sind gemäß unserer Data-in-Transit-Definition https-verschlüsselt per AES 256bit. Der Zugriff auf die Datenbanken

wird protokolliert und regelmäßig durch den IT-Administrator geprüft. Unmittelbarer Datenbankzugriff ist nur im lokalen Unternehmensnetzwerk des Auftragnehmers möglich oder im Home-Office via VPN. Sämtliche WLAN-Netzwerke sind mit WPA2 verschlüsselt. Es werden keinerlei physische, externe Datenträger im Geschäftsbetrieb verwendet.

Die Mitarbeiter des Auftragnehmers verpflichten sich auf das Verbot des Verrats von Geschäfts- und Betriebsgeheimnissen gemäß dem Geschäftsgeheimnisgesetz sowie auf Zweckbindung und Geheimhaltungspflicht gemäß den anwendbaren Gesetzen.

Es existiert eine Bring-Your-Own-Device-Regelung (BYOD). Die im Rahmen dieses Vertrags betroffenen, personenbezogenen Daten des Auftraggebers werden jedoch nicht auf privaten Geräten von Mitarbeitern des Auftragnehmers verarbeitet. Die privaten Geräte (Smartphones) dienen lediglich der internen und externen Kommunikation per E-Mail und Kollaborations-Tool (Microsoft Teams). Die Verarbeitung der hier betroffenen personenbezogenen Daten erfolgt ausschließlich über firmeneigene Geräte (Laptops und Server), für die die hier dargestellten technischen und organisatorischen Maßnahmen zum Schutz der Daten gelten.

3.5 Löschung von Daten

Es besteht ein Standard-Prozess für die Löschung personenbezogener Daten, dessen Einhaltung sowohl durch den IT-Administrator als auch den verantwortlichen Key-Account-Mitarbeiter geprüft wird. Für die Vernichtung physischer Daten gilt Sicherheitsstufe P4 gemäß DIN 66399.

3.6 Trennungskontrolle

Es besteht eine Trennung von Produktiv-, Test-/Entwicklungs- und Verwaltungssystemen. Datenbankrechte wurden festgelegt und es erfolgt eine softwareseitige, logische Mandantentrennung. Darüber hinaus sind alle Konten nach ihrer Arbeitslast getrennt. Speicher, Rechenleistung und Netzwerk werden für jedes Konto unabhängig voneinander verwaltet.

4. Integrität

Die Zugriffe auf die Datenbanken der Produktivsysteme werden protokolliert und zwölf (12) Monate gespeichert.

5. Verfügbarkeit

5.1 Sicherstellen der Verfügbarkeit

Es liegt ein Desaster-Recovery-Konzept vor. Wir verfügen über eine Business Continuity Management Plan. Dieser ist in einer Business Continuity Management Policy beschrieben, welche auf der "ISO 22301:2019 Business Continuity Management" basiert und die Aufrechterhaltung der Geschäftsprozesse basierend auf Minimum Business Continuity Output (MBCO) zum Ziel hat. Darüber hinaus verwenden wir innerhalb unserer Cloud-Architektur mehrere Verfügbarkeitszonen, die die Betriebszeit auch bei einem Ausfall eines kompletten Rechenzentrums gewährleisten. Die Daten werden täglich gesichert. Alle Anwendungen sind containerisiert und können bei Bedarf neu erstellt und bereitgestellt werden.

5.2 Zweckbindung

Mit allen beauftragten Dienstleistern bestehen Verträge zur Auftragsdatenverarbeitung. Sämtliche Mitarbeiter des Auftragnehmers werden zudem laufend und umfassend (Seminare, eigenes E-Learning sowie interaktive Formate wie Quizze) zu den Datenschutzvorgaben sowie zu grundlegenden Themen der Informationssicherheit geschult.

6. Belastbarkeit der Systeme

Die Produktivsysteme und Server werden laufend durch den Dienstleister überwacht, um eine laufende Verfügbarkeit sicherzustellen.

7. Wiederherstellung nach Zwischenfall

Die Server und Produktivsysteme werden laufend, d.h. jeden Tag automatisch durch ein Voll-Backup gesichert. Die Backups werden verschlüsselt auf separaten Server-Systemen beim Dienstleister gespeichert. Es besteht Zugriff für die Administratoren des Auftragnehmers. Die Backups werden jeweils 30 Tage gespeichert.

8. Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen

Für das Incident-Response-Management ist ein dedizierter Mitarbeiter des Auftragnehmers verantwortlich. Im Rahmen der kontinuierlichen Verbesserung der Informationssicherheit des Auftragnehmers werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit laufend durch die Geschäftsführung des Auftragnehmers überwacht, überprüft und verbessert.

Annex IV – Liste der Unterauftragsverarbeiter

- Amazon Web Services EMEA SARL (Amazon Web Services, Inc. als Vertragspartnerin der EU Standardvertragsklauseln)

38 avenue John F. Kennedy, L-1855, Luxemburg

Hosting aller aktuell und zukünftigen Komponenten, die zur Leistungserbringung erforderlich sind, inkl. API-Schnittstelle, Datenbank-System sowie Mailserver für die Phishing-Simulation. Wir haben die folgenden Maßnahmen zum Schutz der Daten getroffen:

- Speicherung und Verarbeitung aller Daten in zertifizierten Rechenzentren in Deutschland (Frankfurt a.M.).
- Verschlüsselung aller Kundendaten durch einen vom Auftragnehmer generierten Masterschlüssel, damit weder AWS noch sonstige Drittparteien Zugriff auf Kundendaten erhalten, weder innerhalb noch außerhalb der EU / des EWR.
- Abschluss eines Auftragsverarbeitungsvertrag sowie den Abschluss der EU-Standardvertragsklauseln ((EU) 2021/915, 4.6.2021, Modul 2 und 3), inkl. zahlreicher Verpflichtungen der AWS zum Umgang und der Transparenz bei etwaigen Behördenanfragen.
- Durch einen externen Datenschutzexperten durchgeführtes Transfer Impact Assessment (TIA).
- Datenschutzrechtliche Expertenmeinung zum Einsatz von AWS beim Auftragnehmer, das auf Wunsch übermittelt werden kann.

- Hetzner Online GmbH

Industriestr. 25, 91710 Gunzenhausen

Nutzung von Mailservern für die Phishing-Simulation der SoSafe GmbH. Sofern explizit individuell mit dem Auftraggeber vereinbart: Zurverfügungstellung der API-Schnittstelle.

ISO27001-Zertifikat für die Rechenzentren: https://www.hetzner.de/pdf/FOX_Zertifikat.pdf

- salesforce.com Germany GmbH

Postanschrift: Salesforce.com Sarl, Route de la Longeraie 9, Morges, 1110, Switzerland, attn: Director, EMEA Sales Operations, Rechtsabteilung: Erika-Mann-Strasse 31-37, 80636, München, Germany

Zurverfügungstellung einer Support-Software (Customer Service Cloud) für den Kundendienst (Supportformular oder E-Mail an support@sosafe.de). Dieser Anbieter ist für den Auftraggeber nur relevant, sofern der Auftraggeber den SoSafe Kundensupport nutzt.

Nähere Informationen: https://trust.salesforce.com/

ISO27001-Zertifikat kann hier abgerufen werden: https://compliance.salesforce.com/en/iso-27017. Im Übrigen wurden folgende Maßnahmen getroffen:

- Speicherung und Verarbeitung aller Daten in zertifizierten Rechenzentren in Deutschland (Frankfurt a.M.)

- Verschlüsselung aller Daten mit branchenüblichen Verschlüsselungsprodukten während der Übertragungen sowie im Ruhezustand.
- Abschluss eines Auftragsverarbeitungsvertrags unter Einbindung der durch Salesforce für seine Konzerngesellschaften und Unterauftragnehmer abgeschlossenen und genehmigten Binding Corporate Rules (BCR) sowie den 2021er Standardvertragsklauseln mit zahlreichen Verpflichtungen gegenüber der zuständigen Aufsichtsbehörde sowie weiteren Selbstverpflichtungen.
- Durch einen externen Datenschutzexperten durchgeführtes Transfer Impact Assessment (TIA).

- Microsoft Ireland Operations Ltd

One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521

Zurverfügungstellung einer E-Mail-Server-Infrastruktur zur Kundenkommunikation über die Support-Software im Supportfall (Supportformular oder E-Mail an support@sosafe.de). Dieser Anbieter ist für den Auftraggeber nur relevant, sofern der Auftraggeber den SoSafe Kundensupport nutzt. Es wurden folgende Maßnahmen getroffen:

- Alle Daten werde im Rahmen der Azure EU-Cloud ausschließlich innerhalb der Europäischen Union verarbeitet und gespeichert.
- Alle Rechenzentren sind ISO27001- und ISO27018-zertifiziert: https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure.
- Verschlüsselung aller Daten mit branchenüblichen Verschlüsselungsprodukten während der Übertragungen sowie im Ruhezustand.
- Implementierung der Customer Lockbox, die sicherstellt, dass Microsoft nicht ohne explizite Einwilligung des Auftragnehmers auf Inhalte zugreifen kann.
- Abschluss eines Auftragsverarbeitungsvertrags sowie Abschluss der EU-Standardvertragsklauseln ((EU) 2021/915, 4.6.2021, Modul 2 und 3).
- Durch einen externen Datenschutzexperten durchgeführtes Transfer Impact Assessment (TIA).

- Kombo Technologies GmbH (Optional)

Lohmühlenstraße 65, 12435 Berlin, Deutschland

Integration des Active Directory des Auftraggebers. Dieser Anbieter ist nur insoweit erforderlich, als der Kunde eine Active Directory-Integration für das automatische Hochladen und die regelmäßige Aktualisierung von Nutzerdaten auf der Plattform des Auftragnehmers verlangt. Die folgenden Maßnahmen wurden ergriffen:

- Alle Daten werden ausschließlich innerhalb der Europäischen Union verarbeitet und gespeichert. Server-Hosting-Anbieter: Google Cloud EMEA Limited.
- Die Kombo Technologies GmbH ist ISO27001 zertifiziert. Der Zugang zum Zertifikat kann hier beantragt werden: https://security.kombo.dev/?itemUid=1fed9faa-4a87-427c-9a95-96b4d6bf66b7&source=click/. Weitere Informationen zu den technischen und organisatorischen Sicherheitsmaßnahmen der Kombo Technologies GmbH finden Sie unter security.kombo.dev.
- Verschlüsselung:

  - Alle Kundendaten werden im Ruhezustand (*data at rest*) mit symmetrischer AES-256-Verschlüsselung verschlüsselt, einschließlich der Sicherungskopien.
  - *Data in transit*: Der gesamte ausgehende Datenverkehr (zu Integrations-APIs) verwendet die höchste TLS-Version, die von der API der jeweiligen Integration zur Verfügung gestellt wird (z. B. Google Workspace). Der gesamte eingehende Datenverkehr über die Kombo-API verwendet zwingend TLS 1.3. Verbindungen von den Anwendungs-Workloads von Kombo zur Datenbank von Kombo verwenden ebenfalls TLS 1.3 mit einer AES-256-Verschlüsselung.

- Abschluss eines Auftragsverarbeitungsvertrags.

SoSafe GmbH | Lichtstr. 25a | 50825 Cologne | Geschäftsführer: Dr. Niklas Hellemann,
Lukas Schaefer, Felix Schürholz, Felix Fichtl | HRB96220 | 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