Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

SoSafe GmbH

Lichtstr. 25a

und

50825 Köln

im Folgenden: **Auftraggeber**

im Folgenden: **Auftragnehmer**

Version 2.6, Stand 14.11.2023

1. Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag über die Auftragsverarbeitung personenbezogener Daten (im Folgenden: „**Vertrag**“) regelt die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.
(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung (im Folgenden: „**DS-GVO**“) zu verstehen.
(4) Die konkrete Leistungserbringung (sowie die dafür notwendige Erhebung, Verarbeitung und Nutzung personenbezogener Daten) beruht auf dem zwischen den Parteien bestehenden Vertrag über die Erbringung von Awareness-Building-Leistungen (im Folgenden: „**Hauptvertrag**“).

2. Gegenstand und Dauer der Verarbeitung

2.1 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 – diese wird vom Auftragnehmer ohne eine Erhebung personenbezogener Daten ermittelt. 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 2.1 (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.

2.2 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. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

3.1 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.

3.2 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 2.1)
- Sprache der Nutzer
- Browser/Browserversion und Plattform der Nutzer
- Teilnahme am Awareness-Building (= kein Opt-Out gemäß Ziffer 3.3)

Diese Daten werden in einer gesicherten Datenbank (s. Anlage 1) zum Zweck des individualisierten Versands gespeichert. Nach Beendigung der Leistungen des Hauptvertrags werden sie unwiderruflich gelöscht (gemäß Ziffer 6 sowie Anlage 1).

(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

3.3 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.

4. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich im Sinne des Art. 28 Abs. 3 a) DS-GVO zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten nicht für andere, sondern nur für die vertraglich vereinbarten Zwecke.
(2) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.

(4) Der Auftragnehmer sorgt dafür, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht gestaltet wird und bei ihm zur Verarbeitung eingesetzte Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(5) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung im notwendigen Umfang zu unterstützen, insbesondere alle erforderlichen Angaben und Dokumentationen vorzuhalten und dem Auftraggeber auf Anforderung so schnell wie in einem zumutbaren Rahmen möglich zuzuleiten.

(6) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(7) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten. Anfragen von Aufsichtsbehörden muss der Auftragnehmer direkt und unmittelbar beantworten. Er setzt den Auftraggeber hiervon jedoch unverzüglich in Kenntnis, soweit die Verarbeitung von personenbezogenen Daten im Auftrag des Auftraggebers hiervon betroffen ist.

(8) Die Kontaktdaten des bestellten Datenschutzbeauftragten sind jederzeit aktuell in der Datenschutzerklärung auf der Website des Auftragnehmers hinterlegt unter https://www.sosafe.de/datenschutz.

(9) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der DS-GVO enthaltenen Bedingungen sowie unter Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5. Technische und organisatorische Maßnahmen

(1) Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, wozu auch herstellerseitige Softwareupdates zählen, solange das hier vereinbarte Sicherheitsniveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
(4) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
(5) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6. Regelung zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete personenbezogene Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren, soweit dies vom Weisungsrahmen umfasst ist. Der Kunde ist über die Admin-Oberfläche in der Lage, die Daten der Endnutzer selbst zu modifizieren oder zu löschen. Der Auftragnehmer ist im Hinblick auf die Berichtigung, Löschung oder Sperrung über die Admin-Oberfläche nur sekundär zur Unterstützung verpflichtet.
(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.
(3) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder datenschutzkonform zu vernichten oder an den Auftraggeber zurückzugeben. Ebenfalls zu vernichten sind sämtliche vorhandenen Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.
(4) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
(5) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen. Beim Löschen sämtlicher Daten des Auftraggebers (Mandantenlöschung aus der SoSafe Management Software) wird ein Löschbericht erzeugt, der den Zeitpunkt und Umfang der Löschung dokumentiert. Dieser Löschbericht wird dem Auftraggeber auf Verlangen unverzüglich vorgelegt.
(6) Ein Zurückbehaltungsrecht des Auftragnehmers an Materialien und Arbeitsergebnissen ist ausgeschlossen.
(7) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

7. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragsverarbeitern (im Folgenden: „**Subunternehmer**“) durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers zulässig. Diese gilt für die in Anlage 2 aufgeführten Subunternehmer als erteilt. Die Beauftragung oder Änderung eines weiteren Subunternehmers durch den Auftragnehmer ist dem Auftraggeber schriftlich oder in Textform vor einer Umstellung anzuzeigen. Der Auftraggeber erhält dann beginnend mit Vorlage der zur Prüfung erforderlichen Unterlagen des Subunternehmers für 14 Kalendertage die Gelegenheit, aus einem wichtigen Grund Einspruch gegen die Umstellung auf diesen weiteren Subunternehmer zu erheben. Ein wichtiger Grund liegt insbesondere dann vor, wenn tatsächliche Anhaltspunkte bestehen, dass der weitere Subunternehmer nicht in der Lage ist, die datenschutzrechtlichen und vertraglichen Anforderungen zu erfüllen. Im Falle eines berechtigten Einspruchs kann der Auftragnehmer entscheiden, den weiteren Subunternehmer nicht einzusetzen. Entscheidet sich der Auftragnehmer dafür, den Subunternehmer trotz des berechtigten Einspruchs des Auftraggebers einzusetzen, steht dem Auftraggeber nach Mitteilung dieses Umstands (Einsatz des Subunternehmers trotz Einspruch) für sieben (7) Kalendertage ein fristloses Sonderkündigungsrecht im Hinblick auf diese Vereinbarung zu. Nach Ablauf der 14 Kalendertage ohne Einspruch gilt die Zustimmung als erteilt.

(2) Der Einsatz von Subunternehmern als weitere (Unter-)Auftragsverarbeiter zur Erfüllung der Leistungen des Auftragnehmers ist nur möglich, wenn dem Subunternehmer vertraglich mindestens solche Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten Bestimmungen vergleichbar sind und das Datenschutzniveau nicht unterschritten wird. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Vertragsteile zwischen Auftragnehmer und Subunternehmer.

(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(5) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(6) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Ziffer 4 (9) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(7) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig und angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

(8) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

(9) Mit Abschluss dieses Vertrags sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(10) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Telekommunikationsdienstleistungen oder Reinigungsleistungen und Bewachungsdienste (soweit nicht nach dem Hauptvertrag geschuldet), sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung und die Wahrung der Rechte von Betroffenen, soweit sie den Verantwortlichen betreffen, allein verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen sowie Änderungen, Ergänzungen oder Ersetzungen dieser in schriftlicher Form oder in einem elektronischen Format (Textform). In Eilfällen können Weisungen mündlich erteilt werden. Mündliche Weisungen sind vom Auftraggeber unverzüglich schriftlich oder in Textform zu bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder bezüglich der datenschutzrechtlichen Bestimmungen feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Soweit ein Dritter die Prüfung vornimmt, muss dieser Dritte zu einem Daten- und ein Geheimnisschutz wie in Ziffer 7 der SoSafe-AGB verpflichtet werden.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle zwölf (12) Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken. Sollte der

durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

9. Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
   a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
   c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 32-36 DS-GVO im erforderlichen Umfang zu unterstützen.

10. Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer hat den Auftraggeber darauf aufmerksam zu machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit einer Forderung hinsichtlich der Betroffenenrechte gemäß Art. 12 ff. DS-GVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen Rahmen auf Weisung sowie wie vereinbart.

12. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrags erfolgt nicht.

13. Haftung

Es gelten die Bestimmungen der DS-GVO, insbesondere Art. 82 DS-GVO sowie im Falle des Einsatzes eines Subunternehmers Art. 28 Abs. 4 Satz 2 DS-GVO.

14. Sonderkündigungsrecht

(1) Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften vorliegt oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen nicht erfüllt oder in erheblichem Maße nicht erfüllt hat.
(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

15. Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrags vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungsplicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch

sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer wird alle in diesem Zusammenhang stehenden Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DS-GVO liegen.

(3) Für Änderungen dieses Vertrags, bei Nebenabreden und bei in diesem Vertrag genannten Erklärungen ist die Schriftform im Sinne des § 126 BGB erforderlich, wobei auch E-Mails dieses Erfordernis erfüllen.

(4) Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(6) Es gilt deutsches Recht.

Unterschriften

Ort, Datum:

Köln, den

F. Schürholz

Auftraggeber	Auftragnehmer

Anlage 1 – technische und organisatorische Maßnahmen

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 § 78 Abs. 1 SGB X.

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 (s. Anlage 2) 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.

Anlage 2 – Zugelassene Subdienstleister

- 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.

Anlage 3 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt.

SEITENS DES AUFTRAGGEBERS:	**SEITENS DES AUFTRAGNEHMERS:**
Vorstand bzw. Geschäftsführung	Felix Schürholz, Geschäftsführer
Sonstige seitens des Auftraggebers explizit benannte Personen (z. B. Datenschutzbeauftragte)	Lukas Schaefer, Geschäftsführer
	Dr. Niklas Hellemann, Geschäftsführer
	Felix Fichtl, Geschäftsführer

SoSafe GmbH | Lichstr. 25a | 50825 Köln | Geschäftsführer: Dr. Niklas Hellemann,
Lukas Schaefer, Felix Schürholz, Felix Fichtl | HRB96220 | Amtsgericht Köln | USt-IdNr: DE322382415 |
Besucheradresse und Parkplatz: Lichstr. 25a | 50825 Köln | Tel: +49 (0) 221 6508 3800 |
E-Mail: info@sosafe.de | Web: sosafe.de