AGB SoSafe GmbH

Stand 18.08.2021

Teil A -- Allgemeine Bestimmungen

1. Vertragsgegenstand und Geltungsbereich

1.1. Die SoSafe GmbH, Ehrenfeldgürtel 76, 50823 Köln (im Folgenden „SoSafe"), bietet für Unternehmen, Behörden und sonstige Organisationen (im Folgenden „Kunden") die Durchführung eines umfangreichen Awareness-Buildings im Bereich Cybersicherheit an (im Folgenden „Awareness-Building").

1.2. Diese Allgemeinen Geschäftsbedingungen (im Folgenden „AGB") sowie das Service Level Agreement („SLA"), beigefügt als Anlage 1, sind Bestandteil des Vertrags über das Awareness-Building zwischen SoSafe und dem Kunden und gelten für alle Kunden. Ergänzend zu den Bestimmungen in diesem Teil A der AGB gelten für die Nutzung von webbasierten Leistungen die Bestimmungen in Teil B dieser AGB. Soweit nachfolgend auf Ziffern dieser AGB ohne besondere Nennung von Teil A oder B verwiesen wird, sind die Ziffern desselben Teils gemeint, aus dem der Verweis erfolgt.

1.3. Das Awareness-Building setzt sich aus vier verschiedenen Bausteinen zusammen (im Folgenden „Leistungsbausteine"), die teilweise durch weitere Dienstleistungen und Software-Tools ergänzt werden. Hierzu zählen (i) Phishing-Simulationen, die Bereitstellung von darauf aufbauenden (ii) E-Learning-Modulen, ein (iii) Phishing-Melde-Button und der (iv) SoSafe Manager. Teilweise werden die Leistungsbausteine webbasiert über die Plattform von SoSafe (im Folgenden „Plattform") unter https://elearning.sosafe.de (für den Zugriff auf die E-Learning-Module) bzw. unter https://manager.sosafe.de (für den Zugriff auf das Admin- und Reporting-Dashboard) zur Verfügung gestellt.

1.4. SoSafe bietet die Leistungsbausteine in den Leistungspaketen gemäß des SLA (im Folgenden „Leistungspaket") an. Je nach Leistungspaket werden die Leistungsbausteine dem Kunden in unterschiedlichem Ausmaß (Anzahl der der Nutzer, Anzahl der zugänglichen Module usw.) und mit unterschiedlichen Zusatzleistungen bereitgestellt. Bei einem Vertragsschluss über die von SoSafe betriebene Website (https://app.sosafe.de/) kann der Kunde nur das Leistungspaket „Starter" bestellen.

1.5. Maßgebend ist die jeweils bei Abschluss des Vertrags über das Awareness-Building gültige Fassung dieser AGB.

1.6. Die Geltung allgemeiner Vertrags- oder Geschäftsbedingungen des Kunden wird ausdrücklich ausgeschlossen. Dies gilt auch dann, wenn SoSafe den Bedingungen des Kunden nicht ausdrücklich widersprochen hat. Gesonderte, bilateral vereinbarte Verabredungen bleiben hiervon unberührt.

1.7. Die AGB von SoSafe gelten nur gegenüber Unternehmern im Sinne von § 14 BGB, juristischen Personen des öffentlichen Rechts und öffentlich-rechtlichen Sondervermögen.

2. Vertragsschluss und Leistungsumfang

2.1. Der Vertrag über das Awareness-Building kann, soweit dies angeboten wird, entweder über die von SoSafe betriebene Website https://app.sosafe.de/ oder offline durch die Annahme eines Angebots des Kunden abgeschlossen werden.

2.2. Soweit der Vertrag über das Awareness-Building offline abgeschlossen wird, kommt er zustande, wenn SoSafe die Bestellung oder den Auftrag des Kunden (Angebot des Kunden), innerhalb von 7 Kalendertagen nach Zugang annimmt. Die Annahme, unterschriebene Kopie der Bestellung/des Auftrags, kann entweder postalisch oder in elektronischer Form erfolgen.

2.3. Alle an den Kunden übermittelten Unterlagen über mögliche Leistungen und Preise von SoSafe im Hinblick auf den in Aussicht genommenen Vertrag über das Awareness-Building sind freibleibend und unverbindlich, sofern sie nicht ausdrücklich als verbindliches Angebot gekennzeichnet sind oder eine bestimmte Annahmefrist enthalten.

2.4. Soweit der Vertrag über das Awareness-Building über die von SoSafe betriebene Website abgeschlossen wird, kann der Vertrag über das Awareness-Building in deutscher Sprache abgeschlossen werden und kommt über die folgenden technischen Schritte zustande:

- Die auf der Website von SoSafe angebotenen Awareness-Building-Leistungen stellen kein bindendes Angebot zum Abschluss eines Vertrags dar. Es handelt sich vielmehr um eine Aufforderung zur Abgabe eines bindenden Angebots durch den Kunden.
- Durch Klicken des Bestell-Buttons, der mit „Jahreslizenzen kaufen" bezeichnet ist, übermittelt der Kunde seine bindende Angebotserklärung.
- SoSafe bestätigt dem Kunden den Zugang von dessen Angebotserklärung auf elektronischem Wege an die vom Kunden angegebene E-Mail-Adresse unmittelbar nach deren Abgabe. Diese Zugangserklärung stellt noch keine Annahme des Angebots des Kunden dar.
- Die verbindliche Annahme des Angebots des Kunden durch SoSafe erfolgt durch die Versendung einer gesonderten ausdrücklichen Annahmeerklärung per E-Mail.
- Während der Laufzeit des Vertrags über die Awareness-Building-Leistungen kann der Kunde jederzeit die Details zu seinem Vertrag mit SoSafe über seinen Account einsehen.

3. Vertragslaufzeit und Kündigung

3.1. Der diesen AGB zugrundeliegende Vertrag über das Awareness-Building wird für den vereinbarten Zeitraum geschlossen. Die Laufzeit der vertraglich vereinbarten Awareness-Building-Leistungen beginnt mit dem Zeitpunkt der Leistungserbringung an den Kunden, spätestens jedoch 30 Tage nach Vertragsschluss. Nach Ablauf des vereinbarten Zeitraums oder bei Vertragsende nach einer Kündigung werden die Awareness-Building-Leistungen nicht mehr erbracht und die Zugangsberechtigungen des Kunden zu der Plattform gesperrt.

3.2. Sowohl der Kunde als auch SoSafe hat das Recht, den Vertrag über das Awareness-Building aus wichtigem Grund – ohne Einhaltung einer Kündigungsfrist – zu kündigen. Ein wichtiger Grund ist für SoSafe insbesondere:

- ein schwerwiegender Verstoß des jeweiligen Kunden gegen die Bestimmungen dieser AGB, einschließlich des SLAs, oder
- die Eröffnung des Insolvenzverfahrens über das Vermögen eines Kunden oder die Abweisung des entsprechenden Eröffnungsantrages mangels Masse.

3.3. Jede Kündigung muss in Schriftform erfolgen. Eine Kündigung per E-Mail ist ebenfalls zulässig.

3.4. Der Vertrag über das Awareness-Building verlängert sich jeweils um ein (1) weiteres Jahr, wenn der Vertrag über das Awareness-Building nicht einen (1) Monat vor Ende der jeweiligen Vertragslaufzeit durch eine der beiden Parteien gekündigt wird.

4. Zahlungsbedingungen

4.1. Die Vergütung richtet sich nach dem individuellen Vertrag mit dem Kunden. Etwas anders gilt nur, wenn der Vertragsschluss, wie in Ziffer 2.4. beschrieben, über die von SoSafe betriebene Website erfolgt ist. Hier wird die zu zahlende Vergütung vor Absenden der Angebotserklärung, abhängig von der Anzahl der bestellten Lizenzen, angezeigt. Sämtliche in dem Vertrag über das Awareness-Building vereinbarten Vergütungen sind Nettobeträge und verstehen sich zuzüglich der Umsatzsteuer in der gesetzlichen Höhe.

4.2. Sofern nicht anderweitig vereinbart, erfolgt die Rechnungsstellung durch SoSafe umgehend nach Vertragsschluss für die gesamte vereinbarte Vertragslaufzeit. Dies gilt auch für Mehrjahreslizenzen. Hier werden die Leistungen für den gesamten Leistungszeitraum bei Vertragsschluss in Rechnung gestellt, sofern nicht anderweitig vereinbart. Bei einer Vertragsverlängerung erfolgt die Rechnungsstellung vollständig zu Beginn des jeweiligen Verlängerungszeitraums. Alle Rechnungen von SoSafe sind innerhalb von 14 Kalendertagen fällig und ohne Abzug zahlbar.

4.3. Tritt nach Vertragsabschluss eine wesentliche Verschlechterung in den Vermögensverhältnissen des Kunden ein, so kann SoSafe Vorauszahlungen oder Sicherheit binnen angemessener Frist fordern und die Leistung bis zur Erfüllung des Vertrages verweigern. Bei Weigerung des Kunden oder fruchtlosem Fristablauf ist SoSafe berechtigt, vom Vertrag zurückzutreten oder Schadensersatz wegen Nichterfüllung zu verlangen.

4.4. Eine Zahlung gilt erst dann als erfolgt, wenn SoSafe über den vollständigen Betrag verfügen kann. Im Falle von Schecks, Überweisungen oder Kartenzahlungen gilt die Zahlung erst als erfolgt, wenn der Betrag auf dem Konto von SoSafe endgültig gutgeschrieben wurde.

5. Weiterentwicklung unserer Leistungen, Übergabe

5.1. SoSafe behält sich das Recht vor, einzeln angebotene Leistungen jederzeit zu erweitern, zu ergänzen oder zu verändern, sofern dies zu einer Verbesserung der Leistung für den Kunden führt bzw. keine oder keine wesentliche Beeinträchtigung dieser beinhaltet.

5.2. SoSafe stellt die Plattform, einschließlich der hierüber zu erbringenden Leistungen, auf Servern zur Nutzung am Zugangspunkt des Rechenzentrums von SoSafe zur Verfügung („Übergabepunkt der Leistung"). Zur Nutzung der Plattform ist es erforderlich, dass der Kunde über einen eigenen Zugang zum Internet verfügt und über diesen Zugang auf die Plattform am Übergabepunkt der Leistung zugreift.

6. Haftung, Haftungsbegrenzung

6.1. SoSafe haftet unbeschränkt für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer Pflichtverletzung von SoSafe, eines gesetzlichen Vertreters oder Erfüllungsgehilfen von SoSafe beruhen sowie für Schäden, die durch Fehlen einer von SoSafe garantierten Beschaffenheit hervorgerufen werden oder bei arglistigem Verhalten von SoSafe.

6.2. SoSafe haftet unbeschränkt für Schäden, die durch SoSafe oder einen gesetzlichen Vertreter oder Erfüllungsgehilfen von SoSafe vorsätzlich oder durch grobe Fahrlässigkeit verursacht wurden.

6.3. Bei der leicht fahrlässig verursachten Verletzung wesentlicher Vertragspflichten haftet SoSafe außer in den Fällen der Ziffer 6.1. oder der Ziffer 6.2. der Höhe nach begrenzt auf den vertragstypisch vorhersehbaren Schaden. Wesentliche Vertragspflichten sind abstrakt solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung eines Vertrags überhaupt erst ermöglicht und auf deren Einhaltung die Vertragsparteien regelmäßig vertrauen dürfen.

6.4. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

6.5. Im Übrigen ist eine Haftung von SoSafe ausgeschlossen.

6.6. Die Verjährungsfrist für Schadensersatzansprüche des Kunden gegen SoSafe beträgt ein (1) Jahr, außer in den Fällen der Ziffern 6.1., 6.2. oder 6.4.

7. Daten- und Geheimnisschutz

7.1. „Vertrauliche Informationen" bezeichnet hinsichtlich einer Partei („Offenlegende Partei") sämtliche nicht-öffentlichen vertraulichen Informationen im Zusammenhang mit dem Geschäft der Offenlegenden Partei. SoSafe und der Kunde werden beim Austausch Vertraulicher Informationen die Ziffern 7.1., 7.2., 7.3. und 7.4. einhalten. Vertrauliche Informationen werden bei der Offenlegung als vertraulich benannt und/oder gekennzeichnet, mit der Maßgabe, dass Informationen, von denen der diese Informationen empfangenden Partei („Empfängerpartei") bekannt war oder unter den gegebenen Umständen hätte bekannt sein müssen, dass sie von der Offenlegenden Partei als vertraulich oder geschützt betrachtet werden, auch dann als Vertrauliche Informationen gelten, wenn sie nicht als solche benannt oder gekennzeichnet wurden. Die Empfängerpartei hält die Vertraulichen Informationen geheim und behandelt sie mindestens mit dem gleichen Maß an Sorgfalt, das die Empfängerpartei zum Schutz ihrer eigenen vertraulichen Informationen anwendet, jedoch mindestens mit angemessener Sorgfalt. Die Empfängerpartei wird die Vertraulichen Informationen nur zur Ausübung von Rechten und Erfüllung von Pflichten gemäß dem jeweiligen Vertrag über das Awareness-Building verwenden. Vertrauliche Informationen werden nur denjenigen Mitarbeitern und Auftragnehmern der Empfängerpartei offengelegt, die diese Informationen kennen müssen. Im Hinblick auf SoSafe sind vertrauliche Informationen insbesondere Auswertungen von Kundendaten, die genauen Abläufe und Konfigurationen des Awareness-Trainings (sofern nicht öffentlich verfügbar), die vereinbarten Preise und Rabatte sowie die Inhalte der Lernmodule und -seiten.

7.2. Zum Schutz der betroffenen Informationen werden den Umständen nach angemessene Geheimhaltungsmaßnahmen ergriffen. Hierzu zählen bei SoSafe insbesondere die physische Zugangsbeschränkung zu den Räumlichkeiten inkl. Videoüberwachung, die Beschränkung der Zugriffsrechte auf kundenspezifische Notizen, Vermerke etc. nur für einzelne Mitarbeiter und nur, falls diese davon für die Leistungserbringung Kenntnis erlangen müssen (Need-to-know-Prinzip), und eine umfassende Vertraulichkeitsvereinbarung, die von allen Mitarbeitern von SoSafe unterzeichnet wird.

7.3. Vertrauliche Informationen fallen nicht unter Ziffer 7.1., soweit (i) sie allgemein zugänglich werden und dies nicht auf einem Verstoß gegen Ziffer 7.1. oder 7.2. beruht; (ii) sie der Empfängerpartei vor dem Zeitpunkt des Erhalts bekannt waren und die Empfängerpartei die Vertraulichen Informationen frei und ohne Geheimhaltungspflicht benutzen durfte; (iii) die Empfängerpartei die Vertraulichen Informationen rechtmäßig durch einen Dritten erlangt hat, der weder bei der Offenlegenden Partei angestellt noch ihrem Unternehmen auf andere Art und Weise zugehörig ist und der diese Informationen der Empfängerpartei freiwillig und rechtmäßig zugeführt hat; (iv) die Empfängerpartei beweisen kann, dass diese Informationen durch Mitarbeiter oder Personal der Empfängerpartei, das auf die entsprechenden Vertraulichen Informationen keinen Zugriff hatte, selbständig erschlossen wurden und dass keine Vertraulichen Informationen verwendet wurden, um diese Informationen zu erschließen; und/oder (v) sie aufgrund eines Gesetzes oder einer gerichtlichen Entscheidung offengelegt werden müssen oder eine Offenlegung durch eine hierzu berechtigte Behörde angeordnet wird.

7.4. Die Verpflichtungen nach Ziffer 7.1. gelten für fünf (5) Jahre über das Ende des jeweiligen Vertrags über das Awareness-Building hinaus.

7.5. Der Kunde sichert zu, dass er berechtigt ist, die personenbezogenen Daten seiner Mitarbeiter im Rahmen der Nutzung der Plattform oder sonstiger Leistungen von SoSafe, die aufgrund eines Vertrags über das Awareness-Building erbracht werden, zu erheben, zu verarbeiten und zu nutzen. Ein Verstoß gegen die Pflichten des Kunden in dieser Ziffer 7.5 berechtigt SoSafe auch zur außerordentlichen fristlosen Kündigung sämtlicher zwischen dem Kunden und SoSafe bestehenden Verträge.

7.6. Die Parteien werden personenbezogene Daten nur im Einklang mit den anwendbaren Datenschutzvorschriften und dem als Anlage 2 beigefügten Vertrag zur Auftragsverarbeitung verarbeiten. Genauere Informationen zu den Daten, die während der simulierten Phishing-Kampagnen, beim E-Learning usw. verarbeitet werden, sind dem Vertrag zur Auftragsverarbeitung personenbezogener Daten zu entnehmen. Einzelheiten über die Verarbeitung von personenbezogenen Daten, die SoSafe als Verantwortlicher verarbeitet, sind in der Datenschutzerklärung, welche außervertraglich ist und von Zeit zu Zeit geändert werden kann, unter https://sosafe.de/datenschutz/ abrufbar.

7.7. Unternehmensbezogene Informationen des Kunden bleiben anonymisiert gespeichert, um bei einer etwaigen Wiederholung des Awareness-Buildings oder anderer Lösungen einen Vergleich der erzielten Ergebnisse zu ermöglichen.

8. Mitwirkungspflichten des Kunden

8.1. Alle benötigten oder angeforderten Unterlagen und Informationen zur möglichst reibungslosen Durchführung des Awareness-Buildings werden SoSafe vom Kunden vollständig unmittelbar nach Vertragsschluss zur Verfügung gestellt. Dies umfasst insbesondere die Übermittlung der Nutzerliste mit den Nutzern (siehe Definition Teil B Ziffer 1.2.), bei denen Phishing-Simulationen erfolgen sollen und die Zugriff auf das E-Learning haben sollen.

8.2. Der Kunde benennt einen für die Projektdurchführung zuständigen Ansprechpartner, der sämtliche Rückfragen beantworten und alle damit zusammenhängenden Entscheidungen treffen kann.

8.3. Der Kunde stellt im Rahmen seiner Möglichkeiten sicher, dass E-Mails von SoSafe nicht an der Zustellung gehindert werden; hierzu zählt insbesondere das sog. "Whitelisting" der von SoSafe betriebenen Domains und Server. SoSafe wird dem Kunden diesbezügliche Hinweise mitteilen, die nach Möglichkeit zu beachten sind.

9. Allgemeines

9.1. Der Kunde ist nur mit vorheriger schriftlicher Zustimmung von SoSafe berechtigt, Forderungen aus oder im Zusammenhang mit der Geschäftsbeziehung zu SoSafe abzutreten, § 354a HGB bleibt unberührt.

9.2. Erfüllungsort für alle sich aus dem Vertrag über das Awareness-Building ergebenden Verbindlichkeiten, einschließlich der Zahlungspflichten des Kunden, ist der Geschäftssitz von SoSafe.

9.3. SoSafe ist berechtigt, den Kunden als Referenzkunden zu nennen. Der Kunde gewährt SoSafe das unentgeltliche, räumlich und inhaltlich unbeschränkte, zeitlich auf die Dauer des Kundenverhältnisses begrenzte Recht an der Verwendung von Logo und Namen des Auftraggebers in elektronischer, gedruckter oder sonstiger Form zu internen oder externen Marketingaktivitäten. (Z. B. im Internet, in Broschüren, Angeboten, Präsentationen oder Pressemitteilungen.)

9.4. Ausschließlicher Gerichtsstand für alle sich aus oder im Zusammenhang mit dem Vertrag über das Awareness-Building ergebenden Streitigkeiten ist der Geschäftssitz von SoSafe. SoSafe ist jedoch berechtigt, den Kunden auch an dessen Geschäftssitz zu verklagen.

9.5. Das Vertragsverhältnis unterliegt allein dem Recht der Bundesrepublik Deutschland mit Ausnahme des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG). Bei dem Recht der Bundesrepublik Deutschland soll es - soweit rechtlich möglich - auch dann verbleiben, wenn nach deutschem Recht auf das Recht eines anderen Staates verwiesen wird (Ausschluss des Kollisionsrechts).

9.6. SoSafe behält sich vor, die angebotenen Awareness-Building-Leistungen sowie diese AGB zu ändern, soweit die jeweilige Änderung notwendig ist, um Veränderungen abzubilden, die bei Abschluss des jeweiligen Vertrags über das Awareness-Building nicht vorhersehbar waren und deren Nichtbeachtung das vertragliche Gleichgewicht zwischen SoSafe und dem Kunden beeinträchtigen würde, insbesondere soweit SoSafe (i) die Übereinstimmung der Awareness-Building-Leistungen mit dem darauf anwendbaren Recht herzustellen verpflichtet ist, insbesondere wenn sich die geltende Rechtslage ändert, (ii) damit einem gegen SoSafe gerichteten Gerichtsurteil oder einer Behördenentscheidung nachkommt und/oder (iii) die Awareness-Building-Leistungen aufgrund zwingender sicherheitsrelevanter Aspekte anpassen muss. Zu keinem Zeitpunkt wird durch die Leistungsänderung die Erfüllung der Hauptvertragspflichten durch SoSafe eingeschränkt.

9.7. In anderen Fällen als der Ziffer 9.6. teilt SoSafe dem Kunden vorab die Änderungen der AGB mit. Soweit der Kunde deren Geltung nicht innerhalb von vier (4) Wochen nach Mitteilung widerspricht, gelten die Änderungen mit Wirkung für die Zukunft als angenommen. Widerspricht der Kunde den Änderungen, wird das Vertragsverhältnis in der bisherigen Form fortgesetzt. Auf die Wirkung des Schweigens wird SoSafe in der Mitteilung hinweisen.

9.8. Änderungen und Ergänzungen des Vertrags über das Awareness-Building, einschließlich dieser AGB, bedürfen, vorbehaltlich von Ziffer 9.6. und 9.7., jeweils der Schriftform.

9.9. Bei Unwirksamkeit einer der Klauseln dieser AGB bleibt die Wirksamkeit der übrigen Klauseln davon unberührt.

Teil B -- Besondere Bestimmungen für webbasierte Leistungen (Plattform und über die Plattform erbrachte Leistungen)

1. Nutzungsberechtigung und Nutzungsvoraussetzungen

1.1. Sofern der Vertrag über das Awareness-Building nicht über die Website von SoSafe geschlossen wurde und damit nicht bereits ohnehin ein Account erstellt wurde, müssen Kunden einen Account (im Folgenden „Account") unter https://manager.sosafe.de anlegen, um über die Plattform auch auf die nur online zur Verfügung gestellten Awareness-Building-Leistungen zugreifen zu können. Bei der Erstellung des Accounts hat der Kunde zunächst seine berufliche E-Mail-Adresse sowie seinen Vor- und Nachnamen anzugeben. Zudem hat der Kunde ein Passwort zu erstellen. Die Registrierungsinformationen müssen korrekt, aktuell und vollständig sein. Alternativ kann SoSafe den Account auch für den Kunden anlegen und diesem dann das Passwort zusenden.

1.2. Neben dem Kunden dürfen nur die von ihm autorisierten Nutzer (im Folgenden „Nutzer") die Awareness-Building-Leistungen, die über die Plattform zur Verfügung gestellt werden, im durch Teil A Ziffer 2. und Teil B Ziffer 2. bestimmten Umfang benutzen. Hierfür müssen die Nutzer, wie in Ziffer 1.1. beschrieben, ebenfalls jeweils einen Account (im Folgenden „User Account") anlegen. Jeder Nutzer darf sich nur einmal registrieren und pro Nutzer ist ein (1) User Account anzulegen. Die Registrierung ist kostenlos. Ein User Account ist für einen bestimmten Nutzer anzulegen und ist nicht auf eine andere Person übertragbar.

1.3. Die Registrierung als Nutzer gemäß Ziffer 1.2. ist nur Personen erlaubt, für die dem Kunden eine Nutzungslizenz zur Nutzung der Awareness-Building-Leistungen erteilt wurde. Die zeitgleiche Nutzung desselben Accounts über mehrere Endgeräte ist nicht erlaubt. Sofern nicht ausdrücklich von SoSafe erlaubt, ist eine Registrierung der Nutzer mit privaten E-Mailadressen, insb. Freemailangeboten wie GMX, Web.de oder Google Mail nicht gestattet.

1.4. Der Kunde ist für die Einhaltung des Vertrags über das Awareness-Building und dieser AGB durch alle seine Nutzer verantwortlich, einschließlich dessen, wie Nutzer ihren User Account verwenden. Jegliche Nutzung der Awareness-Building-Leistungen muss ausschließlich zu eigenen betrieblichen Zwecken des Kunden und innerhalb des Nutzungsumfangs liegen.

1.5. Der Kunde und seine Nutzer sind verpflichtet, die Login-Daten, Passwörter etc. von den Accounts/User Accounts geheim zu halten und die Zugangsdaten nicht an unbefugte Dritte (oder andere Nutzer) weiterzugeben und sich nach jeder Anmeldung wieder abzumelden. Entsprechendes gilt bei einer Anmeldung via Single-Sign-On für die dort verwendeten Zugangsdaten, mit der Ausnahme, dass nicht nach jedem Zugang wieder eine manuelle Abmeldung erfolgen muss. Erklärungen und Handlungen, die nach einem Login über den Account /User Account mit dem Passwort und der E-Mail-Adresse des Kunden oder eines Nutzers abgegeben bzw. begangen werden, können dem Kunden auch dann zuzurechnen sein, wenn er hiervon keine Kenntnis hat. Eine Zurechnung erfolgt insbesondere dann, wenn der Kunde oder ein Nutzer Dritten (auch Familienangehörigen) vorsätzlich oder fahrlässig Zugang zum Passwort oder dem Account/User Account verschafft. Der Kunde hat den Anbieter unverzüglich zu informieren, sobald er Kenntnis davon erlangt, dass unbefugten Dritten Zugangsdaten zugänglich und bekannt sind.

1.6. Im Falle eines begründeten Verdachts, dass Zugangsdaten unbefugten Dritten bekannt wurden, ist SoSafe aus Sicherheitsgründen berechtigt, aber nicht verpflichtet, nach freiem Ermessen die Zugangsdaten des Kunden oder des betreffenden Nutzers ohne vorherige Ankündigung selbständig zu ändern bzw. die Nutzung des Accounts/User Accounts vorübergehend zu sperren. SoSafe informiert den Kunden bzw. Nutzer hierüber unverzüglich und teilt innerhalb angemessener Frist neue Zugangsdaten mit. Der Kunde bzw. Nutzer hat

keinen Anspruch darauf, dass die ursprünglichen Zugangsdaten wiederhergestellt werden. Im Falle der Anmeldung via Single-Sign-On wird lediglich der Zugang via dieses Single-Sign-On mit den bisherigen Zugangsdaten gesperrt und der Kunde bzw. Nutzer kann sich nur noch über die neuen Zugangsdaten anmelden. Diese neuen Zugangsdaten können wiederum in einen Single-Sign-On integriert werden.

1.7. Der Kunde verpflichtet sich dafür zu sorgen, dass die Nutzer es unterlassen:

- beleidigende, gewaltverherrlichende, diskriminierende, menschenverachtende oder verleumderische Inhalte auf der Plattform zu veröffentlichen oder zur Verfügung zu stellen;
- pornographische oder rassistische Inhalte auf der Plattform zu veröffentlichen oder zur Verfügung zu stellen;
- Inhalte auf der Plattform zu veröffentlichen oder zur Verfügung zu stellen, die gegen Jugendschutzgesetze oder Strafgesetze verstoßen;
- Handlungen durchzuführen, die das einwandfreie Funktionieren bzw. Erscheinungsbild der Plattform oder der Leistungsbausteine blockieren, überlasten oder beeinträchtigen könnten (z. B. Denial-of-Service-Attacken);
- unwahre oder unsachliche Inhalte auf der Plattform zu veröffentlichen oder zur Verfügung zu stellen;
- nicht von SoSafe vorab freigegebene kommerzielle Kommunikation (beispielsweise Spam) auf der Plattform zu veröffentlichen oder zur Verfügung zu stellen;
- mittels automatisierter Mechanismen (wie Bots, Roboter, Spider oder Scraper) Inhalte oder Informationen von anderen Nutzern zu erfassen oder auf andere Art auf die Plattform oder die Leistungsbausteine zuzugreifen, sofern nicht die ausdrückliche vorherige Erlaubnis von SoSafe eingeholt wurde;
- rechtswidrige Strukturvertriebe, wie beispielsweise Schneeballsysteme, auf der Plattform oder in den Leistungsbausteinen zu betreiben;
- Viren oder anderen bösartigen Code hochzuladen;
- Anmeldeinformationen einzuholen oder auf einen Account/User Account zuzugreifen, die/der einem anderen Nutzer gehören /gehört;
- gesetzlich geschützte Inhalte zu verwenden, ohne dazu berechtigt zu sein;
- Daten anderer Nutzer zu erheben, zu nutzen oder zu verarbeiten, ohne dazu berechtigt zu sein.

1.8. SoSafe ist berechtigt, Inhalte, die gegen Ziffer 1.7. verstoßen, unwiederbringlich zu löschen. Der Kunde und Nutzer haben insoweit keinen Anspruch auf Wiedereinstellung bereits gelöschter Inhalte.

1.9. Verstößt der Kunde oder einer seiner Nutzer gegen Ziffer 1.7. oder gesetzliche Vorschriften kann SoSafe

- Inhalte abändern oder löschen;
- den User Account zeitlich beschränken oder dauerhaft sperren;
- dem Nutzer ein Verbot erteilen, sich nach der Löschung seines User Accounts unter seinem oder einem anderen Namen wieder anzumelden.

Diese Sanktionen kann SoSafe ohne vorherige Ankündigung und ohne Rücksprache mit dem Kunden auch gegen dessen ausdrücklichen Willen bzw. gegen den Willen des Nutzers verhängen. SoSafe wird den Kunden und den Nutzer über die entsprechenden Sanktionen per E-Mail informieren.

2. Nutzungs- und Urheberrechte

2.1. SoSafe räumt dem Kunden das örtlich unbeschränkte, befristete, widerrufliche, nicht-ausschließliche, nicht-unterlizenzierbare und nicht übertragbare Recht ein, die Plattform und die hierüber zur Verfügung gestellten Leistungsbausteine und Zusatzleistungen für die eigenen betrieblichen Zwecke für die in dem Vertrag über das Awareness-Building bestimmte Anzahl an Nutzern und vereinbarten Umfang zu nutzen.

2.2. Der Kunde ist nicht berechtigt, (i) die Plattform oder den Zugang zu der Plattform zu vermieten, zu verleasen, zu verleihen, zu reproduzieren, weiterzuverkaufen oder in sonstiger Weise zu vertreiben oder weiterzugeben, auch nicht über das Internet oder ein nachgelagertes öffentliches oder privates Datennetzwerk; (ii) die Plattform zur Entwicklung anderer Leistungen zu nutzen; (iii) Bestandteile der Plattform, für die dem Kunden keine Nutzungsrechte eingeräumt wurden, zu aktivieren oder zu nutzen; (iv) die Nutzungsrechte an der Plattform an Dritte zu übertragen oder Dritten Zugriff auf die Plattform zu gewähren; (v) den Programmcode der Plattform zu ändern, zu übersetzen, zu vervielfältigen, zu dekompilieren, seine Funktionen zu untersuchen, außer soweit gesetzlich zwingend gemäß § 69d oder § 69e UrhG zulässig; sowie (vi) rechtliche Hinweise, insbesondere auf gewerbliche Schutzrechte von SoSafe, zu entfernen, zu verdecken oder zu ändern.

2.3. Sofern SoSafe es dem Kunden ermöglicht über die Plattform individuelle Materialien (Auswertungen des E-Learnings, Auswertungen der Phishing-Simulationen usw.) zu erstellen oder dem Kunden solche individuell für ihn erstellten Materialen zum Download oder Drucken zur Verfügung stellt, räumt SoSafe dem Kunden mit der vollständigen Zahlung der vereinbarten Vergütung die zeitlich und örtlich unbegrenzten, widerruflichen, nicht-ausschließlichen, nicht-unterlizenzierbaren und nicht-übertragbaren Nutzungsrechte an allen von SoSafe im Rahmen dieses Vertrages für den Kunden individuell erstellten Materialien ein, soweit die Übertragung nach deutschem Recht oder den tatsächlichen Verhältnissen möglich ist.

2.4. Die Nutzung der vorgenannten individuellen Materialien (ausgenommen aller fremden geschützten Marken oder Zeichen) und insbesondere der hierdurch gewonnenen Erkenntnisse zu eigenen Zwecken bleibt SoSafe vorbehalten.

3. Gewährleistung

3.1. Bezüglich der Nutzung der Plattform und der über die Plattform erbrachten Leistungsbausteine und Zusatzleistungen gelten bei Mängeln grundsätzlich die §§ 536 ff. BGB sowie die nachfolgenden Ziffern 3.2. bis 3.5.:

3.2. Die verschuldensunabhängige Haftung für anfängliche Mängel gemäß § 536a Abs. 1., 1. Var. BGB wird ausgeschlossen. Die verschuldensabhängige Haftung von SoSafe bleibt bestehen.

3.3. Die Behebung von Mängeln erfolgt nach Wahl von SoSafe entweder durch kostenfreie Nachbesserung oder Ersatzlieferung.

3.4. Eine Kündigung des Kunden gem. § 543 Abs. 2 S. 1 Nr. 1 BGB wegen Nichtgewährung des vertragsgemäßen Gebrauchs ist erst zulässig, wenn SoSafe ausreichende Gelegenheit zur Mängelbeseitigung gegeben wurde und diese fehlgeschlagen ist.

3.5. SoSafe übernimmt keine Gewährleistung für den Internet-Zugang des Kunden, insbesondere für die Verfügbarkeit und Dimensionierung des Internet-Zugangs. Der Kunde ist für seinen Internet-Zugang zum Übergabepunkt der Leistung selbst verantwortlich.

Anlage 1: Service Level Agreement (SLA) SoSafe GmbH

Stand 19.04.2022

Einleitung

Geltungsbereich

Das Service Level Agreement konkretisiert und spezifiziert die Qualität sowie den Umfang der Leistungen, die die SoSafe GmbH (nachfolgend „SoSafe") anbietet. Zwischen SoSafe und dem Kunden wird ein Vertrag zur Erbringung von Leistungen im Bereich Mitarbeiter-Training/Awareness-Building geschlossen (im Folgenden „Hauptvertrag"). Der Leistungserbringer SoSafe und der Leistungsempfänger (nachfolgend „Kunde") werden im Folgenden gemeinsam als „Parteien" bezeichnet.

Dieses Dokument enthält alle relevanten Bestimmungen und Regelungen, durch welche die Leistungsbeschreibung der Awareness-Building-Leistungen und die Mitwirkungspflichten im Hauptvertrag zwischen den Parteien konkretisiert werden.

Gültigkeit für verschiedene Awareness-Pakete

SoSafe bietet grundsätzlich vier verschiedene Awareness-Pakete an: Starter, Essential, Professional und Premium. Einzelne Abschnitte dieses Service Level Agreements beziehen sich teilweise nur auf einzelne Pakete. Dies ist bei den betroffenen Bestimmungen entsprechend gekennzeichnet durch die Überschrift der jeweiligen Abschnitte. Eine Konkretisierung des Leistungsumfangs der einzelnen Pakete folgt darunter. Außerdem ist es in einigen Paketen möglich, nur einzelne Bausteine daraus zu nutzen (z. B. nur das E-Learning aus dem Paket Essential) in diesem Falle gelten die entsprechenden Regelungen des jeweiligen Paketes analog für den einzelnen Baustein.

Darüber hinaus bietet SoSafe einzelne, zusätzliche Dienstleistungen/Features optional an. Diese sind gesondert gelistet.

Die in diesem SLA in Ziffer 3. und 5. beschriebenen Awareness-Building-Leistungen stehen dem Kunden nur im jeweils erworbenen Umfang zu.

Voraussetzungen und Mitwirkungspflichten für die Nutzung der Leistungen

Allgemeine Voraussetzungen und Mitwirkungspflichten

Für diverse Bestandteile der nachfolgenden Leistungsbausteine (Ziffer 3.) ist der Zugriff auf Webseiten von SoSafe mit einem Web-Browser erforderlich. Insoweit werden nur folgende Browser unterstützt und deren Verwendung bildet damit eine Voraussetzung für die Leistungserbringung: Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge und Microsoft Internet Explorer 11 in der jeweils aktuellen Version.

Spezielle Voraussetzungen und Mitwirkungspflichten

Die speziellen Voraussetzungen bzw. Mitwirkungspflichten für die Nutzung der Awareness-Building-Leistungen sind in Ziffer 3. bei den jeweiligen Leistungsbausteinen ausgeführt.

Leistungsbausteine

Die folgenden Abschnitte beschreiben die durch SoSafe angebotenen Leistungen und legen die Abläufe und organisatorischen Schnittstellen fest, die für eine Leistungserbringung erforderlich sind.

Phishing-Simulation

Der Leistungsbaustein Phishing-Simulation umfasst den Versand einer definierten Anzahl von (im Vorfeld abgestimmten) E-Mails an die Nutzer über den Leistungszeitraum. Diese E-Mails simulieren echte Phishing-Mails zur Steigerung der Awareness der Nutzer gegenüber IT-Sicherheitsrisiken durch Phishing-Angriffe. Beim Klick auf ein Phishing-Element (z. B. Bild, Link) in einer der simulierten Phishing-Mails wird eine Webseite aufgerufen (im Folgenden „Lernseite"), die den Nutzer über die Simulation aufklärt und konkrete Hinweise gibt, woran die jeweilige E-Mail als Phishing-Versuch hätte erkannt werden können.

Zur Sicherstellung der Zustellung aller simulierten Phishing-Mails an alle im Rahmen des Trainings zu schulenden Nutzer ist die Einrichtung eines Whitelistings durch den Kunden erforderlich. Es handelt sich hierbei um eine Mitwirkungspflicht des Kunden, ohne welche die Leistungserbringung durch SoSafe nicht gewährleistet werden kann. Der Kunde trägt somit an dieser Stelle die Verantwortung, dass die simulierten Phishing-Mails in vollständiger Form auch tatsächlich in den Postfächern der Nutzer ankommen und im Rahmen der Trainingsmaßnahme genutzt werden können. Kann der Kunde das Whitelisting selbst nicht beeinflussen (z. B. weil der Kunde einen IT-Dienstleister mit der Verwaltung seiner IT-Systeme beauftragt hat), so hat er dafür Sorge zu tragen, dass das Whitelisting dennoch erfolgt.

Für das Whitelisting müssen folgende Schritte unternommen werden:

- Die dedizierten Mail-Server von SoSafe müssen im empfangenden Mail-System auf eine Whitelist gesetzt werden, um das Abweisen der eingehenden E-Mails zu verhindern.
- Kundenseitig etwaig vorhandene Filtersysteme (z. B. Secure Mail-Gateway) sind entsprechend so zu konfigurieren, dass die simulierten Phishing-Mails nicht als „Junk" oder „Spam" markiert werden und die Zustellung an die Nutzer gewährleistet werden kann.
- Kundenseitig etwaig vorhandene Systeme zum Zugriffsschutz auf das Internet von den Endgeräten der Nutzer aus (z. B. Web-Gateways, Proxies, Sicherheitseinstellungen des Betriebssystems) sind so zu konfigurieren, dass die unverfälschte Anzeige der simulierten Phishing-Mails in den E-Mail-Programmen der Nutzer gewährleistet ist. Des Weiteren sind diese Systeme so zu konfigurieren, dass die Lernseiten über einen Web-Browser anzeigbar sind.

Zur Umsetzung dieser Schritte wird durch SoSafe eine Anleitung bereitgestellt. Die Anleitung beinhaltet auch alle benötigten technischen Informationen wie IP-Adressen und Servernamen der Mail-Server, freizugebende URLs für Filtersysteme und Systeme zum Zugriffsschutz.

Phishing-Melde-Button

Beim Leistungsbaustein Phishing-Melde-Button handelt es sich um eine Funktionalität, die es den Nutzern ermöglicht, E-Mails, die als potenzieller Phishing-Angriff eingeschätzt werden, zu melden. Die Meldung erfolgt an eine vom Kunden definierte E-Mail-Adresse in Form einer Weiterleitung der verdächtigen E-Mail. Simulierte Phishing-Mails von SoSafe werden nicht weitergeleitet, sondern an SoSafe gemeldet und gelöscht. Vom Kunden ist eine E-Mail-Adresse zu benennen, wohin die Weiterleitung erfolgen soll.

Die Funktionalität wird in Form eines Outlook-Add-Ins bereitgestellt. Damit das Outlook-Add-In ordnungsgemäß laden und funktionieren kann, müssen auf Server- und Clientseite verschiedene Anforderungen erfüllt sein.

Clientanforderungen

- Der Client muss eine der unterstützten Anwendungen für Outlook-Add-Ins sein. Die folgenden Clients unterstützen Add-Ins:
    - Outlook 2013 oder höher auf Windows
    - Outlook 2016 oder höher auf Mac
    - Outlook unter iOS
    - Outlook unter Android
    - Outlook im Web für Exchange 2016 oder höher und Office 365
    - Outlook.com
- Alternativ Google Workspace
- Der Client muss über eine direkte Verbindung mit einem Exchange-Server oder mit Office 365 verbunden sein. Bei der Konfiguration des Clients muss der Benutzer als Kontotyp „Exchange", „Office 365" oder „Outlook.com" auswählen. Wenn für den Client eine POP3- oder IMAP-Verbindung konfiguriert ist, werden Add-Ins nicht geladen.

Anforderungen an den E-Mail-Server

Wenn der Benutzer mit Google Workspace, Office 365 oder Outlook.com verbunden ist, sind damit bereits sämtliche Anforderungen an den E-Mail-Server erfüllt. Für Benutzer, die mit einer lokalen Exchange-Server-Installation verbunden sind, gelten jedoch die folgenden Anforderungen:

- Bei dem Server muss es sich um Exchange 2016 oder höher handeln.
- Die Exchange-Webdienste (EWS) müssen aktiviert und über das Internet erreichbar sein. Viele Add-Ins erfordern EWS, damit sie ordnungsgemäß funktionieren.
- Der Server muss ein gültiges Authentifizierungszertifikat besitzen, damit er gültige Identitätstoken ausstellen kann. In neuen Exchange Server-Installationen ist ein Standardauthentifizierungszertifikat enthalten.
- Die Clientzugriffsserver müssen mit AppSource kommunizieren können, um auf Add-Ins aus Microsoft AppSource zugreifen zu können.

Eine erfolgreiche Installation sowie ein reibungsloser Roll-Out des Add-Ins kann nur gewährleistet werden, sofern der Kunde die Standardeinstellungen des jeweiligen Programms nutzt und keine Drittanwendung im Betrieb hat, die die Funktionalität des Add-Ins beeinflusst. Ein individueller Support durch SoSafe bei dem Setup des Add-Ins in einer nicht-standardmäßigen Infrastruktur wird explizit ausgeschlossen. Als optionale Leistung können Ressourcen mit entsprechender Expertise vermittelt werden. Dies bedarf einer separaten und expliziten Vereinbarung zwischen den betroffenen Parteien.

Client-/Server-API-Kompatibilität

Das Outlook-Add-In nutzt die Exchange Web Services (EWS) oder die Outlook REST API, um Daten aus dem Outlook-Postfach des Benutzers abzurufen. Die folgenden Abschnitte geben die Verfügbarkeit von EWS und REST API für alle unterstützten Exchange-Server-/Outlook-Client-Kombinationen und deren Auswirkung auf die Weiterleitung an.

Exchange On-Premise

Für alle Exchange-On-Premise-Server (kein hybrides Deployment) können wir nur EWS unterstützen.

Exchange Online/Hybrid server deployments

Für Exchange Online und hybride Deployments von Exchange-Servern unterstützen wir die folgende EWS- und REST-API-Verfügbarkeit für die jeweiligen Client-/Server-Kombinationen:

REST: nur REST API
EWS: nur EWS
Beide: EWS und REST API

Windows

Windows		Windows Outlook Clients			
		MS 365[1]	Outlook 2019	Outlook 2016	Outlook 2013
Server	Exchange Online	Beide	Beide	EWS	EWS
	Exchange 2019[2]	Beide	Beide	EWS	EWS
	Exchange 2016[2]	Beide	Beide	EWS	EWS

macOS

macOS		macOS Outlook Clients		
		MS 365[1]	Outlook 2019	Outlook 2016
Server	Exchange Online	Beide	Beide	Beide
	Exchange 2019[2]	Beide	Beide	Beide
	Exchange 2016[2]	Beide	Beide	Beide

Other

		Outlook Clients			
		Android App	iOS App	Desktop Browser	Mobile Browser
Server	Exchange Online	REST	REST	Beide	nicht unterstützt
	Exchange 2019[2]	REST	REST	Beide	nicht unterstützt
	Exchange 2016[2]	REST	REST	Beide	nicht unterstützt

[1] Microsoft Office 365 Abonnement
[2] verbunden mit Exchange Online (hybrides Deployment)

Unterschiede bei der Weiterleitung

Die Weiterleitung kann im .eml- oder im Split-Modus erfolgen, was jeweils die folgenden Unterschiede mit sich bringt. Abhängig von der nutzbaren API und dem Weiterleitungs-Modus werden folgende Dateien an die vom Kunden definierte E-Mail-Adresse weitergeleitet:

	via REST	via EWS
.eml-Modus	• mail.eml	• mail.eml • Bei E-Mails größer als 500 kB wechselt das Add-in automatisch zum Split-Modus
Split-Modus	• body.html • headers.txt • Alle Anhänge als originale Dateien[3]	• body.html • headers.txt • attachments.txt [3] • Beinhaltet Informationen über Name, Größe, Typ, IsInline der Anhänge

[3] Wenn die E-Mail Anhänge enthält

E-Learning

Der Leistungsbaustein E-Learning umfasst die Zugriffsmöglichkeit für alle berechtigten Nutzer eines Kunden im Rahmen der Leistungserbringung auf die vereinbarte Anzahl Lernmodule. Die Lernmodule vermitteln Wissen im Bereich IT-Sicherheit, Arbeitssicherheit und Compliance und decken eine Bandbreite an Unterthemen ab. Die gebuchten Lernmodule können über die eigene Lernplattform von SoSafe abgerufen oder auch per SCORM-Streaming in ein kundenseitig bestehendes Learning Management System (LMS) integriert werden. Die Lernmodule unterteilen sich in Lernvideos und interaktive Lernmodule.

Die Lernvideos können mit und ohne akustische Ausgabe genutzt werden (dies kann lokal über das Betriebssystem bzw. den Browser des Nutzers gesteuert werden). Bei allen Sprachversionen (vgl. Multilinguales Paket) der Lernvideos ist eine Tonspur sowie Untertitel hinterlegt. Die interaktiven Lernmodule sind ohne Tonspur.

Zugriff über Lernplattform

Die proprietäre Lernplattform von SoSafe ist erreichbar unter https://elearning.sosafe.de. Hier können sich die Nutzer mit ihren beruflichen E-Mail-Adressen registrieren. Alternativ kann ein anonymer Zugangscode genutzt werden.

Zugriff über kundenseitiges LMS

Die Lernmodule werden im Standard SCORM 1.2 (kompatibel mit gängigen LMS wie zum Beispiel: SAP SuccessFactors Learning, Adobe Captive Prime LMS, ILIAS, Moodle, Totara Learning) als Container-Dateien zur Verfügung gestellt. Diese Container-Dateien können in das LMS integriert werden. Die Inhalte der Lernmodule werden dann zum Zugriffszeitpunkt von einem Streaming-Server von SoSafe bereitgestellt. Hierfür ist der Zugriff auf den Streaming-Server unter lms0.sosafe.de zu gewährleisten. Der Inhalt der Lernmodule wird von SoSafe stets auf aktuellem Stand gehalten, das bedeutet, es werden sowohl Fehlerkorrekturen als auch Aktualisierungen auf den neuesten Erkenntnisstand („State-of-the-Art") im Bereich IT-Sicherheit vorgenommen.

SoSafe Manager

Unter https://manager.sosafe.de ist der SoSafe Manager für den Kunden erreichbar. Der SoSafe Manager ist das Portal zur Administration der Awareness-Maßnahmen. Innerhalb des Reporting-Dashboards auf dem Portal kann der Kunde diverse Kennzahlen über die beauftragten Leistungsbestandteile einsehen, wie z. B. allgemeine Klickraten der simulierten Phishing-Mails, den Gesamtfortschritt im E-Learning oder – je nach Leistungsvereinbarung – auch individuelle E-Learning-Ergebnisse einzelner Mitarbeiter. Welche Daten genau einsehbar sind und verarbeitet werden, ist in einem separaten AV-Vertrag geregelt.

Kundensupport

Kommunikationswege

Genereller Ansprechpartner für alle Kunden von SoSafe ist der Kundensupport. Die Nutzer der Kunden haben nachstehende Möglichkeiten, Supportanfragen einzureichen:

- Support-Formular inkl. FAQ: http://support.sosafe.de
- E-Mail: support@sosafe.de
- Postalisch: SoSafe GmbH, Ehrenfeldgürtel 76, 50823 Köln, Deutschland

Die Administratoren der Kunden (Ziffer 8.2. der AGB) haben darüber hinaus die Möglichkeit, Supportanfragen an die Hotline (Telefon: +49 221 65083800) zu richten.

Sämtliche Kommunikation kann – je nach Kundenwunsch – auf Deutsch oder Englisch stattfinden. Andere Sprachen werden supportseitig aktuell nicht angeboten.

Zeitliche Erreichbarkeit

Der Kundensupport ist - außer an Feiertagen im Bundesland Nordrhein-Westfalen - Montag bis Freitag von 09:00 bis 17:00 Uhr erreichbar.

Reaktionszeiten

Die Reaktionszeit beginnt grundsätzlich mit dem Eingang der Supportanfrage eines Nutzers oder Administratoren beim Kundensupport. Voraussetzung für den Beginn der Reaktionszeit ist eine ausreichend spezifizierte Beschreibung der Anfrage bzw. des Fehlers in Bezug auf die jeweils geschuldeten Awareness-Building-Leistungen.

Die Reaktionszeiten sind nach Richtwerten folgendermaßen unterteilt:

- Bei allgemeinen Anfragen zu jeweils den geschuldeten Awareness-Building-Leistungen: innerhalb von zwei (2) Werktagen
- Bei Störungen der jeweils geschuldeten Awareness-Building-Leistungen (z. B. der Service ist nur eingeschränkt erreichbar): innerhalb von einem (1) Werktag

Die Einordnung der Supportanfrage nach den oben genannten Unterteilungen erfolgt durch den Kundensupport, basierend auf der Fehlerbeschreibung des Kunden.

Innerhalb der festgelegten Reaktionszeit erhält der Kunde eine qualifizierte Antwort vom Kundensupport. Im Idealfall beinhaltet diese qualifizierte Antwort bereits die Lösung bzw. den Abschluss des Vorgangs, zumindest aber eine erste Einschätzung der Supportanfrage und eine Auskunft über die weitere Vorgehensweise.

Im Falle einer Störung beinhaltet die qualifizierte Antwort ebenfalls Informationen über die voraussichtliche Dauer und den Umfang der gemeldeten Störung sowie einen ersten Lösungsansatz.

Leistungsumfang einzelner Awareness-Pakete

Die einzelnen Awareness-Pakete von SoSafe beinhalten unterschiedliche Leistungsumfänge und Supportlevel. Die Besonderheiten der einzelnen Pakete sind in den folgenden Abschnitten aufgelistet. Nachrangig, soweit Leistungen im diesem SLA nicht beschrieben sind, gilt der Leistungsumfang gemäß der Feature-Übersicht auf https://www.sosafe.de/produkt.

Paket Starter

- Das Paket Starter ist nur für Kunden mit 5-250 Nutzern buchbar.
- Für das Paket Starter müssen sämtliche Nutzer über dieselbe Maildomain registriert werden (Single domain only).
- Dem Kunden wird auf der Self-Service-Plattform https://app.sosafe.de eine Anleitung (PDF als Download) zur Verfügung gestellt, die alle notwendigen Schritte, wie z. B. die Einrichtung des Whitelistings, für einen durchschnittlichen Nutzer verständlich erklärt.
- Über die Plattform müssen alle relevanten Informationen (Kundenstammdaten, Abrechnungsdaten etc.) kundenseitig eingetragen werden.
- Für die Übermittlung der Nutzerliste wird eine Vorlage (Excel-Datei) zur Verfügung gestellt, deren Schema eingehalten werden muss, um einen sauberen Upload der Daten in die Self-Service-Plattform zu gewährleisten. Diese Nutzerliste kann kundenseitig aktualisiert werden. Dabei darf die tatsächliche, im System vorhandene Anzahl der Nutzer nicht die lizensierte Anzahl der Nutzer (vertraglich vereinbarte Obergrenze) überschreiten.
- Es wird ein Muster des AV-Vertrags zur Verfügung gestellt, welches vom Kunden zu unterschreiben und wieder hochzuladen ist.
- Interaktive Lernmodule und Lernvideos im E-Learning sind fix und können nicht verändert werden. Für die Phishing-Simulation ka nn ein passendes Branchenpaket ausgewählt werden.

Paket Essential

- Bei Bedarf wird ein 30-minütiges Gespräch zum Kick-Off telefonisch oder per Webkonferenz durchgeführt, in dem ein SoSafe-Awareness-Experte dem Kunden alle notwendigen technischen Vorbereitungen erklärt und die weiteren Schritte abstimmt.
- Freie Wahl der Maildomains bei Registrierung.
- Für die Übermittlung der Nutzerliste für die Phishing-Simulation und/oder das E-Learning wird eine Vorlage (Excel-Datei) zur Verfügung gestellt, deren Schema eingehalten werden muss. Die Übermittlung der Nutzerliste an SoSafe erfolgt über eine gesicherte Datenverbindung auf das SoSafe-Manager-Portal. Der Kunde erhält hierfür ein Nutzerkonto. Dabei darf die tatsächliche, im System vorhandene Anzahl der Nutzer grundsätzlich nicht die lizensierte Anzahl der Nutzer (vertraglich vereinbarte Obergrenze) überschreiten. Aus Kulanzgründen wird eine kostenneutrale Überschreitung der vereinbarten Obergrenze um bis zu 7 % gewährt.
- Eine Aktualisierung der Nutzerliste über den o.g. Zugang zum SoSafe-Manager-Portal kann der Kunde jederzeit selbstständig durchführen, sollten sich aufgrund von Fluktuation etc. Änderungen ergeben.
- Für die Einrichtung des Whitelistings wird von SoSafe eine Anleitung zur Verfügung gestellt.
- Für das E-Learning können aus den zur Verfügung stehenden interaktiven Lernmodulen (Schwierigkeitsgrad: Anfänger) und Lernvideos zum Thema IT-Sicherheit die vereinbarte Anzahl oder Auswahl für alle Nutzer des Kunden aktiviert werden. In Absprache mit dem Kunden kann durch SoSafe eine Erinnerungs-Funktion eingestellt werden, die z. B. Nutzer, welche sich noch nicht registriert oder einzelne Module noch nicht absolviert haben, per E-Mail an eine Registrierung/Finalisierung erinnert. Als Sprachen stehen Deutsch und Englisch zur Verfügung.
- Für die Phishing-Simulation: Wir versenden randomisiert und über das Jahr verteilt zwölf (12) simulierte Phishing-Mails, die auf Angriffen basieren, die z. B. in Ihrer Branche beobachtet werden. Diese Sammlung wird laufend aktualisiert. Eine inhaltliche Anpassung der E-Mails ist in diesem Paket nicht enthalten, dies ist nur in den Paketen Professional und Premium möglich. Als Sprachen stehen Deutsch und Englisch zur Verfügung.
- Rüstzeiten: Der Kick-Off kann innerhalb von einer Kalenderwoche ab Beauftragung (schriftliche Annahme des Angebotes durch SoSafe) durchgeführt werden, auf Kundenwunsch auch später. Sobald der Kick-Off durchgeführt wurde, sichert SoSafe einen möglichen Start des Awareness-Buildings innerhalb von 10 Werktagen zu, sofern alle hierfür benötigten Daten seitens des Kunden verzögerungsfrei bereitgestellt und mitwirkungspflichtige Tätigkeiten durchgeführt werden.
- Nutzerfeedback: Sie können Nutzerfeedback einsehen und es als CSV-Datei exportieren.
- Die Auswertung enthält Benchmarks zu allen Kennzahlen im Vergleich zum Kundendurchschnitt.
- Bei Nutzung der SoSafe-Lernplattform erhalten Nutzer ein Zertifikat über alle bestandenen Lernmodule.
- Gamification: Auf der SoSafe Lernplattform durchlaufen Nutzer Levels, sammeln Abzeichen und können ihre Fortschritte in einer persönlichen Erfolgsübersicht einsehen. (An- und abschaltbar)

Paket Professional

Alle Bestandteile aus Paket Essential , jedoch abweichend oder zusätzlich:

- Spear-Phishing-Simulation: Alle E-Mails werden über ein Platzhaltersystem für den jeweiligen Empfänger individualisiert (z. B. „Sehr geehrter Herr Müller, ...") und teilweise auch mit Details wie Name oder Sitz des Kunden versehen.
- Branding: Auf den zur Phishing-Simulation zugehörigen Lernseiten wird oben das Logo des Kunden eingeblendet, ebenso auf der Lernplattform von SoSafe. Die Buttons und farblichen Gestaltungselemente der Lernseiten sowie der Lernplattform können farblich an die Corporate Identity des Kunden angepasst werden. Außerdem kann der E-Mail-unspezifische Hinweistext auf den Lernseiten nach Kundenwunsch erstellt oder angepasst werden. Sofern Logo und Farbschema frei verfügbar sind, kann die Einrichtung durch SoSafe erfolgen. Anderenfalls werden die entsprechenden Daten vom Kunden zur Verfügung gestellt. Der Kunde garantiert für die Einbindung, dass er die Nutzungsrechte am Logo innehat und haftet für etwaige Verstöße gegen die Rechte Dritter.

- Multilinguales Paket: Phishing-Mail-Templates, Lernseiten und Lerninhalte stehen Ihnen in weiteren Sprachen zur Verfügung. Derzeit sind 23 Sprachen verfügbar, eine aktuelle Liste wird auf Anfrage zur Verfügung gestellt.
- Rüstzeiten: Der Kick-Off kann innerhalb von einer Kalenderwoche ab Beauftragung (schriftliche Annahme des Angebotes durch SoSafe) durchgeführt werden, auf Kundenwunsch auch später. Sobald der Kick-Off durchgeführt wurde, sichert SoSafe einen möglichen Start des Awareness-Buildings innerhalb von 20 Werktagen zu, sofern alle hierfür benötigten Daten seitens des Kunden verzögerungsfrei bereitgestellt und mitwirkungspflichtige Tätigkeiten durchgeführt werden.

Paket Premium

Alle Bestandteile aus Paket Professional, jedoch abweichend oder zusätzlich:

- Für die Einrichtung und Konfiguration des Phishing-Melde-Buttons wird von SoSafe eine Anleitung für die technisch unterstützen Infrastrukturalternativen zur Verfügung gestellt.
- Customization Engine: Ausgewählte Inhalte der E-Learning-Lernmodule können kundenspezifisch angepasst werden. Die Inhalte auf der Lernplattform sind über Platzhalter durch den Kunden selbst individuell an die Anforderungen und Vorschriften Ihrer Organisation anpassbar (z. B. Passwort-Länge, Ansprechpartner für Datenschutz).
- Maßgeschneiderte Spear-Phishing-Simulation: Wir versenden zusätzlich 3 simulierte Phishing-Mails, die wir gemeinsam mit Ihnen individuell für Ihre Organisation erstellen (z. B. Nachbildung eines CEO-Frauds). Die individuell erstellten Phishing-Mails werden in Deutsch und Englisch zur Verfügung gestellt.

Zusatzpaket Enterprise:

- Differenzierte Ausspielung: Auf Kundenwunsch können ausgewählte, simulierte Phishing-Mails spezifischen Nutzergruppen zugeordnet werden, um sie noch gezielter zu trainieren.
- Full-Service-Implementierung: Ihr persönlicher Implementierungsmanager unterstützt und berät Sie bei der erweiterten Konfiguration Ihrer Awareness-Plattform: Best-Practice-Ansätze, Whitelisting, Empfehlungen zur Kommunikation inkl. Vorlagen, Nutzermanagement mit Datenqualitätssicherung.
- Business-Review: Sie erhalten pro Jahr bis zu 4 Executive Business Reviews. Dies beinhaltet ein 60-minütiges Telefonat mit dem persönlichen Ansprechpartner bei SoSafe. Weiterhin einen Berichts des Inhalts: 1) Zielerreichung (z. B. Deep Dive in relevante Kennzahlen und Produktnutzungsdaten) 2) Benchmarking (z. B. gegen Kundenstammdaten, Branche des Kunden, Unternehmensgröße) 3) Beratung zu Maßnahmen (z. B. zur Verfügungstellung von Kommunikationsunterlagen an Mitarbeiter oder für internes Reporting, Best Practices von vergleichbaren Unternehmen) 4) Unterstützung und Beratung für die langfristige Cyber-Security-Awareness-Strategie des Kunden.
- Priority-Support: Ihr persönlicher Ansprechpartner behandelt all Ihre Support-Anfragen prioritär und unterstützt Sie innerhalb unserer Supportzeiten per E-Mail oder Telefon.
- ISO 27001 Reporting: Die Daten werden für ein ISO 27001 Audit konform ausgewertet.
- Experten-Auswertung: Ergänzend zu den Bestimmungen bezüglich der Nutzerliste kann die Liste um Ordnungskriterien ergänzt werden. Dies können z. B. Nutzergruppen basierend auf den Organisationseinheiten oder Standorten des Kunden sein. Die Auswertungen auf dem Reporting-Dashboard erfolgen dann differenziert nach diesem Ordnungskriterium. Bei der Festlegung des Ordnungskriteriums durch den Kunden sind dabei stets die vereinbarten Bestimmungen des AV-Vertrags zu beachten; so ist z. B. die Mindestgröße einer Nutzergruppe von 5 Personen aus Gründen des Datenschutzes nicht zu unterschreiten.
- Experten-Benchmarking: Die Auswertung enthält zusätzliche Benchmarks, z. B. zu Branche und Unternehmensgröße des Kunden.
- Fortgeschrittenes Scheduling: Wir passen die Versandzeiten individuell an Kundenwünsche an, z. B. an Urlaubszeiten und Zeitzonen.
- SCORM-Streaming: Sie erhalten Zugriff auf die Lernmodule als SCORM-Container und können sie in Ihr eigenes Learning Management System einbinden.
- Unterstützendes Awareness-Material: Sie erhalten unterstützendes digitales Material zu Ihrer Awareness-Kampagne, z. B. Poster, Screensaver, Flyer, Kommunikationsvorlagen.
- Datenexport: Sie können Auswertungsdaten als Excel- oder CSV-Datei exportieren.
- Zur Anmeldung auf der SoSafe Lernplattform ist auch die Nutzung eines Single-Sign-On via Azure Active Directory (AD) oder Google möglich. Damit sich die Lernplattform gegen das AD authentifizieren kann, ist ein Azure AD in der Cloud Voraussetzung (Hybrid-Setup möglich). Als Protokoll kommt OAuth 2.0 zum Einsatz, welches sich optimal für den Einsatz in Web-Apps eignet. Es ist lediglich die einmalige Autorisierung unserer Web-App durch den Azure AD Administrator des Kunden erforderlich. Die technischen Voraussetzungen für Single-Sign-On sind auf support.sosafe.de einsehbar. SCIM wird mit den folgenden Einschränkungen unterstützt:
    - Die SCIM-Anbindung an den SoSafe Manager unterstützt nur Datentransfers aus dem Microsoft Azure AD, es werden keine On-Premise Active Directories unterstützt.
    - Die SCIM-Anbindung unterstützt nur die Anbindung eines Azure-Tenants. Alle zu übertragenen Nutzerdaten müssen kundenseitig in einem Azure-Tenant verwaltet werden. Die Anbindung mehrerer Tenants wird nicht unterstützt.
    - Wenn eine SCIM-Anbindung an den SoSafe Manager hergestellt wird, erfolgt die Nutzerverwaltung ausschließlich über das Azure AD kundenseitig; es ist nicht möglich, parallel weitere Nutzer per Excel- oder CSV-Import in die SoSafe-Datenbank einzuspielen.

Paket „Datenschutz"

Zusätzlich zu oder anstelle der obigen Pakete buchbar.

Paket „Datenschutz Professional"

- Für das E-Learning können aus den zur Verfügung stehenden interaktiven Lernmodulen und Lernvideos zum Thema Datenschutz die vereinbarte Anzahl oder Auswahl für alle Nutzer des Kunden aktiviert werden. In Absprache mit dem Kunden kann durch SoSafe eine Erinnerungs-Funktion eingestellt werden, die z. B. Nutzer, welche sich noch nicht registriert oder einzelne Module noch nicht absolviert haben, per E-Mail an eine Registrierung/Finalisierung erinnert. Als Sprachen stehen Deutsch und Englisch zur Verfügung.

- Bei Bedarf wird ein 30-minütiges Gespräch zum Kick-Off telefonisch oder per Webkonferenz durchgeführt, in dem ein SoSafe-Awareness-Experte dem Kunden alle notwendigen technischen Vorbereitungen erklärt und die weiteren Schritte abstimmt.
- Nutzerfeedback: Sie können Nutzerfeedback einsehen und es als CSV-Datei exportieren.
- Die Auswertung enthält Benchmarks zu allen Kennzahlen im Vergleich zum Kundendurchschnitt.
- Bei Nutzung der SoSafe-Lernplattform erhalten Nutzer ein Zertifikat über alle bestandenen Lernmodule.

Paket „Datenschutz Premium"

Alle Bestandteile aus Paket Professional, jedoch abweichend oder zusätzlich:

- Customization Engine: Ausgewählte Inhalte der E-Learning-Lernmodule können kundenspezifisch angepasst werden. Die Inhalte auf der Lernplattform sind über Platzhalter durch den Kunden selbst individuell an die Anforderungen und Vorschriften Ihrer Organisation anpassbar (z. B. Passwort-Länge, Ansprechpartner für Datenschutz).
- Branding: Auf den zur Phishing-Simulation zugehörigen Lernseiten wird oben das Logo des Kunden eingeblendet, ebenso auf der Lernplattform von SoSafe. Die Buttons und farblichen Gestaltungselemente der Lernseiten sowie der Lernplattform können farblich an die Corporate Identity des Kunden angepasst werden. Sofern Logo und Farbschema frei verfügbar sind, kann die Einrichtung durch SoSafe erfolgen. Anderenfalls werden die entsprechenden Daten vom Kunden zur Verfügung gestellt. Der Kunde garantiert für die Einbindung, dass er die Nutzungsrechte am Logo innehat und haftet für etwaige Verstöße gegen die Rechte Dritter.

Zusatzpaket „Datenschutz Enterprise"

- Full-Service-Implementierung: Ihr persönlicher Implementierungsmanager unterstützt und berät Sie bei der erweiterten Konfiguration Ihrer Awareness-Plattform: Best-Practice-Ansätze, Whitelisting, Empfehlungen zur Kommunikation inkl. Vorlagen, Nutzermanagement mit Datenqualitätssicherung.
- Business Review: Sie erhalten pro Jahr bis zu 4 (vier) Executive Business Reviews. Dies beinhaltet ein 60-minütiges Telefonat mit dem persönlichen Ansprechpartner bei SoSafe. Weiterhin einen Bericht des Inhalts: 1) Zielerreichung (z. B. Deep Dive in relevante Kennzahlen und Produktnutzungsdaten) 2) Benchmarking (z. B. gegen Kundenstammdaten, Branche des Kunden, Unternehmensgröße) 3) Beratung zu Maßnahmen (zB. zur Verfügungstellung von Kommunikationsunterlagen an Mitarbeiter oder für internes Reporting, Best Practices von vergleichbaren Unternehmen) 4) Unterstützung und Beratung für die langfristige Cyber Security Awareness Strategie des Kunden.
- Priority Support: Ihr persönlicher Ansprechpartner behandelt all Ihre Support-Anfragen prioritär und unterstützt Sie innerhalb unserer Supportzeiten per E-Mail oder Telefon.
- Experten-Auswertung: Ergänzend zu den Bestimmungen bezüglich der Nutzerliste, kann die Liste um Ordnungskriteria ergänzt werden. Dies können z. B. Nutzergruppen basierend auf den Organisationseinheiten oder Standorten des Kunden sein. Die Auswertungen auf dem Reporting-Dashboard erfolgen dann differenziert nach diesem Ordnungskriterium. Bei der Festlegung des Ordnungskriteriums durch den Kunden sind dabei stets die vereinbarten Bestimmungen des AV-Vertrags zu beachten; so ist z. B. die Mindestgröße einer Nutzergruppe von 5 Personen aus Gründen des Datenschutzes nicht zu unterschreiten.
- Experten-Benchmarking: Die Auswertung enthält zusätzliche Benchmarks, z. B. zu Branche und Unternehmensgröße des Kunden.
- Fortgeschrittenes Scheduling: Wir passen die Versandzeiten individuell an Kundenwünsche an, z. B. an Urlaubszeiten und Zeitzonen.
- SCORM-Streaming: Sie erhalten Zugriff auf die Lernmodule als SCORM-Container und können Sie in Ihr eigenes Learning-Management-System einbinden. Es wird Version 1.2 des SCORM-Standards unterstützt.
- Unterstützendes Awareness-Material: Sie erhalten unterstützendes digitales Material zu Ihrer Awareness-Kampagne, z. B. Poster, Screensaver, Flyer, Kommunikationsvorlagen.
- Datenexport: Sie können Auswertungsdaten als Excel- oder CSV-Datei exportieren.
- Zur Anmeldung auf der SoSafe-Lernplattform ist auch die Nutzung eines Single-Sign-On via Azure Active Directory (AD) oder Google möglich. Damit sich die Lernplattform gegen das AD authentifizieren kann, ist ein Azure AD in der Cloud Voraussetzung (Hybrid-Setup möglich). Als Protokoll kommt OAuth 2.0 oder SAML in Version 2.0 zum Einsatz, welches sich optimal für den Einsatz in Web-Apps eignet. Es ist lediglich die einmalige Autorisierung unserer Web-App durch den Azure AD Administrator des Kunden erforderlich. Die technischen Voraussetzungen für Single-Sign-On sind auf support.sosafe.de einsehbar. SCIM wird mit den folgenden Einschränkungen unterstützt:
    - Die SCIM-Anbindung an den SoSafe Manager unterstützt nur Datentransfers aus dem Microsoft Azure AD, es werden keine On-Premise Active Directories unterstützt.
    - Die SCIM-Anbindung unterstützt nur die Anbindung eines Azure-Tenants. Alle zu übertragenen Nutzerdaten müssen kundenseitig in einem Azure-Tenant verwaltet werden. Die Anbindung mehrerer Tenants wird nicht unterstützt.
    - Wenn eine SCIM-Anbindung an den SoSafe Manager hergestellt wird, erfolgt die Nutzerverwaltung ausschließlich über das Azure AD kundenseitig, es ist nicht möglich parallel weitere Nutzer per Excel- oder CSV-Import in die SoSafe Datenbank einzuspielen.

Zusatzpaket „Arbeitsschutz"

- Für das E-Learning können aus den zur Verfügung stehenden interaktiven Lernmodulen zum Thema Arbeitsschutz die vereinbarte Anzahl oder Auswahl für alle Nutzer des Kunden aktiviert werden. In Absprache mit dem Kunden kann durch SoSafe eine Erinnerungs-Funktion eingestellt werden, die z. B. Nutzer, welche sich noch nicht registriert oder einzelne Module noch nicht absolviert haben, per E-Mail an eine Registrierung/Finalisierung erinnert. Als Sprache steht Deutsch zur Verfügung.

Zusatzpaket „Allgemeines Gleichbehandlungsgesetz"

- Für das E-Learning können aus den zur Verfügung stehenden interaktiven Lernmodulen zum Thema allgemeines Gleichbehandlungsgesetz die vereinbarte Anzahl oder Auswahl für alle Nutzer des Kunden aktiviert werden. In Absprache mit dem Kunden kann durch SoSafe eine Erinnerungs-Funktion eingestellt werden, die z. B. Nutzer, welche sich noch nicht registriert oder einzelne Module noch nicht absolviert haben, per E-Mail an eine Registrierung/Finalisierung erinnert. Als Sprache steht Deutsch zur Verfügung.

Zusatzpaket „Compliance"

- Für das E-Learning können aus den zur Verfügung stehenden interaktiven Lernmodulen zum Thema Compliance die vereinbarte Anzahl oder Auswahl für alle Nutzer des Kunden aktiviert werden. In Absprache mit dem Kunden kann durch SoSafe eine Erinnerungs-Funktion eingestellt werden, die z. B. Nutzer, welche sich noch nicht registriert oder einzelne Module noch nicht absolviert haben, per E-Mail an eine Registrierung/Finalisierung erinnert. Als Sprache steht Deutsch zur Verfügung.

Verfügbarkeit der Dienste

Generelle Verfügbarkeit

Für Awareness-Building-Leistungen, die von SoSafe über https://elearning.sosafe.de, die Lernseiten oder den Streaming-Server erbracht werden, sowie den Phishing-Melde-Button dürfen die nachfolgenden durchschnittlichen (bezogen auf das Monatsmittel) Verfügbarkeiten nicht unterschritten werden. Diese gelten als erfüllt, solange die tatsächliche Verfügbarkeit diesen Wert im Monatsmittel nicht unterschreitet.

Gemessen wird die Verfügbarkeit als Verhältnis von Uptime - also der Zeit, die der Service ordnungsgemäß bereitsteht - zur Gesamtzeit, also Uptime plus Downtime (Ausfallzeit):

Verfügbarkeit = Uptime / (Uptime + Downtime)

Verfügbarkeiten in Prozent - umgerechnet in Minuten für ein System, das 24 Stunden am Tag, an 365 Jahrestagen (24 × 365) zur Verfügung steht (8760 Stunden).

- E-Learning-Plattform: 97 %
- Streaming-Server von SoSafe (Zugriff via externe LMS): 97 %
- Lernseiten zur Simulation: 97 %
- Phishing-Melde-Button/Add-In: 97 %

Ausnahmen von der Verfügbarkeit

Nicht als Ausfallzeit im Sinne des Vorgenannten gelten Wartungsarbeiten an den Systemen von SoSafe und ihren Zulieferern, die für den Erhalt und die Sicherheit des laufenden Betriebes bzw. der Durchführung von Updates oder Upgrades notwendig sind.

In der Regel wird eine Wartung an Wochenenden zwischen Samstag 09:00 Uhr und Sonntag 18:00 Uhr oder nachts an jedem Wochentag in der Zeit zwischen 23:00 Uhr und 07:00 Uhr am nächsten Morgen durchgeführt. In Ausnahmefällen kann eine Systemwartung unter Berücksichtigung der geringstmöglichen Beeinträchtigung des laufenden Betriebs auch in allen übrigen Zeiten durchgeführt werden. In solchen Fällen informiert SoSafe den Kunden über geplante Systemwartungen so früh wie möglich, spätestens aber eine Kalenderwoche vor der Systemwartung.

Unterschreitung der Verfügbarkeit

Für jede Unterschreitung der monatlichen Generellen Verfügbarkeit um einen vollen Prozentpunkt, sofern nicht gemäß "Ausnahmen von der Verfügbarkeit" ausgeschlossen, erhält der Kunde einen zusätzlichen Tag der vereinbarten Leistungen am Ende der Vertragslaufzeit.