



Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

Stand 02.10.2026 (Fassung 1.0) · zwischen dem Kunden (Inhaber des Firmenkontos) und der secureIT UG (haftungsbeschränkt)

Hinweis: Dieser Vertrag kommt mit der Registrierung eines Firmenkontos bei secureIT zustande. Eine Unterschrift ist nicht erforderlich. Dieses Dokument dient als Nachweis für Ihre Unterlagen und Ihren Datenschutzbeauftragten.

Präambel

Der Auftraggeber (die Organisation, die ein Firmenkonto bei secureIT anlegt, im Folgenden „Kunde“) nutzt die Plattform secureIT der secureIT UG (haftungsbeschränkt), Weinstraße 9, 79282 Ballrechten-Dottingen, vertreten durch den Geschäftsführer Patrick Ihle (im Folgenden „Auftragnehmer“), für Awareness-Schulungen und Phishing-Simulationen seiner Beschäftigten. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Kunden. Dieser Vertrag regelt die Rechte und Pflichten beider Seiten nach Art. 28 DSGVO. Er kommt mit der Registrierung eines Firmenkontos zustande und gilt für alle Schulungen und Simulationen, die über dieses Konto gestartet werden.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Bereitstellung der Online-Schulung, der Versand simulierter Phishing-E-Mails, die Erfassung der Reaktionen darauf, die Erstellung von Teamauswertungen, Teilnahmezertifikaten und Schulungsnachweisen sowie optional monatliche Auffrischungslektionen.

(2) Der Vertrag gilt für die Dauer des Firmenkontos. Er endet mit dessen Löschung durch den Kunden oder mit der Beendigung der Nutzungsvereinbarung.

§ 2 Art und Zweck der Verarbeitung, Datenarten, Betroffene

(1) **Zweck:** Schulung und Sensibilisierung der Beschäftigten des Kunden zu Phishing und Informationssicherheit, Nachweis dieser Schulung gegenüber Versicherern, Auftraggebern und Aufsichtsbehörden.

(2) **Datenarten:** Vorname, Nachname, dienstliche E-Mail-Adresse; persönlicher Zugangslink; Lernfortschritt (bearbeitete Lektionen mit Zeitpunkt, Abschlussdatum, Lernweg, Ergebnis des Wissenstests, gestellte Fragen zu Lektionen); je simulierter E-Mail Versandzeitpunkt sowie ob sie geöffnet, ob ein Link angeklickt und ob auf der Übungsseite eine Eingabe gemacht wurde; dabei anfallende technische Daten (IP-Adresse, E-Mail-Programm, Zeitpunkt); Zertifikatsnummer und -datum. Eingegebene Passwörter werden nicht gespeichert.

(3) **Betroffene:** Beschäftigte und sonstige vom Kunden eingetragene Personen (etwa Auszubildende, Aushilfen, externe Mitarbeitende mit dienstlichem Postfach) sowie die Administratoren des Kunden.

§ 3 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen dieses Vertrags und nach den dokumentierten Weisungen des Kunden. Weisungen erteilt der Kunde über die Funktionen der Plattform (Personen eintragen, Schulung starten, Lauf stoppen, Personen löschen) oder in Textform an die im Impressum genannte Adresse.

(2) Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Kunden unverzüglich darauf hin und darf die Ausführung bis zur Bestätigung aussetzen.

(3) Der Auftragnehmer verwendet die Daten nicht für eigene Zwecke, insbesondere nicht für Werbung, und gibt sie nicht an Dritte weiter, soweit dieser Vertrag nichts anderes bestimmt.

§ 4 Vertraulichkeit und Beschränkung des Zugriffs

(1) Der Auftragnehmer ist ein Ein-Personen-Betrieb. Zugriff auf die Daten hat allein der Geschäftsführer, der sich zur Vertraulichkeit verpflichtet hat und dem Datengeheimnis unterliegt. Werden künftig Beschäftigte oder Auftragnehmer eingesetzt, werden sie vor dem Zugriff schriftlich zur Vertraulichkeit verpflichtet.

(2) Persönliche Ergebnisse der Phishing-Simulation (welche Person welche Mail geöffnet, angeklickt oder beantwortet hat) stellt der Auftragnehmer dem Kunden nicht zur Verfügung. Der Kunde erhält ausschließlich anonymisierte Teamauswertungen, die





eine Mindestgröße von drei Personen voraussetzen. Der Auftragnehmer selbst hat zu Wartungs- und Supportzwecken Zugriff auf Einzeldaten; dieser Zugriff wird protokolliert.

§ 5 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in der Anlage beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und entwickelt sie fortlaufend weiter. Maßnahmen dürfen durch gleichwertige ersetzt werden, das Schutzniveau darf dabei nicht sinken.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde stimmt dem Einsatz der folgenden Unterauftragsverarbeiter zu:

- **IONOS SE**, Elgendorfer Str. 57, 56410 Montabaur, Deutschland: Hosting der Plattform und der Datenbank, E-Mail-Versand und -Empfang. Verarbeitung ausschließlich in Rechenzentren in Deutschland.
- **ElevenLabs Inc.**, New York, USA: Sprachsynthese für einzelne Simulationsvorlagen mit Sprachnachricht. Übermittelt wird nur der vorzulesende Text, der höchstens den Vornamen der betroffenen Person enthält. Grundlage der Drittlandübermittlung ist das EU-US Data Privacy Framework, soweit der Anbieter dort zertifiziert ist, andernfalls die EU-Standardvertragsklauseln. Der Einsatz erfolgt nur, wenn der Kunde eine solche Vorlage auswählt.

(2) Über den Wechsel oder die Aufnahme weiterer Unterauftragsverarbeiter informiert der Auftragnehmer den Kunden mindestens vier Wochen vorab per E-Mail an die Administratoradresse. Der Kunde kann innerhalb dieser Frist aus wichtigem Grund widersprechen; kommt keine Einigung zustande, kann der Kunde das Firmenkonto beenden.

§ 7 Unterstützung des Kunden

(1) Der Auftragnehmer unterstützt den Kunden bei der Beantwortung von Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit). Löschungen und Berichtigungen einzelner Personen kann der Kunde direkt in der Plattform vornehmen.

(2) Der Auftragnehmer unterstützt den Kunden bei einer Datenschutz-Folgenabschätzung und bei Anfragen von Aufsichtsbehörden, soweit die Verarbeitung aus diesem Vertrag betroffen ist.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten, die Daten des Kunden betrifft, unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, an die Administratoradresse. Die Meldung enthält, soweit bekannt, Art und Umfang der Verletzung, betroffene Personen und Daten, wahrscheinliche Folgen und ergriffene Maßnahmen. Die Frist des Kunden nach Art. 33 DSGVO (72 Stunden) bleibt unberührt; der Auftragnehmer unterstützt die Meldung.

§ 9 Löschung und Rückgabe

(1) Nach Ende des Vertrags löscht der Auftragnehmer alle Daten des Kunden innerhalb von 30 Tagen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht (etwa Rechnungsdaten nach § 147 AO und § 257 HGB). Vorher kann der Kunde Teamauswertungen und Schulungsnachweise als PDF herunterladen.

(2) Während des Vertrags kann der Kunde einzelne Personen jederzeit löschen; die Löschung erfasst Zugangsdaten, Lernfortschritt und Simulationsergebnisse dieser Person. Bereits ausgestellte Zertifikate behalten ihre Prüfnummer, damit vorgelegte Nachweise prüfbar bleiben; der Kunde kann auch deren Löschung verlangen.

(3) Datensicherungen werden nach einem festen Zyklus überschrieben; gelöschte Daten verschwinden damit spätestens 30 Tage nach der Löschung auch aus den Sicherungen.

§ 10 Nachweise und Kontrollen

(1) Der Auftragnehmer weist die Einhaltung seiner Pflichten durch die Anlage zu diesem Vertrag, das Verarbeitungsverzeichnis und auf Anfrage durch eine schriftliche Selbstauskunft nach.

(2) Der Kunde kann nach angemessener Ankündigung (mindestens 14 Tage) während der üblichen Geschäftszeiten Kontrollen



durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, höchstens einmal je Kalenderjahr, sofern kein konkreter Anlass vorliegt. Der Aufwand des Auftragnehmers für Kontrollen über die Selbstauskunft hinaus wird nach Aufwand vergütet.

§ 11 Verantwortlichkeit des Kunden

Der Kunde ist als Verantwortlicher dafür zuständig, dass die Verarbeitung zulässig ist, insbesondere für die Rechtsgrundlage gegenüber seinen Beschäftigten (in der Regel § 26 Abs. 1 BDSG, Art. 6 Abs. 1 lit. f DSGVO), die Information der Beschäftigten nach Art. 13 DSGVO und, soweit ein Betriebsrat besteht, die Beteiligung nach § 87 Abs. 1 Nr. 6 BetrVG. Der Auftragnehmer stellt dafür ein Infoblatt und eine Muster-Betriebsvereinbarung bereit und nimmt die Information der Beschäftigten in die Einladungsmail auf.

§ 12 Haftung und Schlussbestimmungen

(1) Die Haftung richtet sich nach Art. 82 DSGVO und den Nutzungsbedingungen.

(2) Änderungen dieses Vertrags teilt der Auftragnehmer dem Kunden per E-Mail mit; die jeweils gültige Fassung ist unter secureit.icu/auftragsverarbeitung abrufbar. Es gilt deutsches Recht. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Zutritts- und Zugangskontrolle: Betrieb in einem ISO-27001-zertifizierten Rechenzentrum von IONOS in Deutschland. Serverzugang nur per SSH mit Schlüssel über einen nicht standardmäßigen Port, automatische Sperre bei wiederholten Fehlversuchen. Administrationszugang zur Plattform nur mit verifizierter E-Mail-Adresse und Passwort; Sitzungen laufen ab.

Zugriffskontrolle: Rollenmodell (Superadmin, Firmenadministrator, betreuender Partner, Lehrkraft, Teilnehmende). Firmenadministratoren sehen nur ihre eigene Organisation; persönliche Simulationsergebnisse sind für sie nicht abrufbar. Zugriffe betreuender Partner werden mit Name und Zeitpunkt protokolliert.

Weitergabe- und Transportkontrolle: Alle Verbindungen ausschließlich über TLS (HTTPS). E-Mail-Versand über den eigenen Mailserver mit SPF, DKIM und DMARC. Keine Übertragung von Teilnehmerdaten an Dritte außer den genannten Unterauftragsverarbeitern.

Eingabekontrolle: Sicherheitsrelevante Aktionen (Schulungsstart, Laufsteuerung, Löschungen, Rechnungen, Partnerzugriffe) werden mit Benutzer, Zeitpunkt und IP-Adresse in einem Audit-Protokoll festgehalten.

Datenminimierung: Es werden nur Name und dienstliche E-Mail-Adresse erhoben. Auf den Übungsseiten eingegebene Passwörter werden verworfen, gespeichert wird nur, dass eine Eingabe stattfand. Die Website-Statistik arbeitet ohne Cookies und ohne Nutzerprofile.

Verfügbarkeitskontrolle: Tägliche Datensicherungen der Datenbank, Aufbewahrung nach festem Zyklus, geprüfte Wiederherstellbarkeit; Sicherheitsupdates des Servers werden zeitnah eingespielt.

Trennungskontrolle: Daten verschiedener Kunden sind logisch durch Organisationskennungen getrennt; jede Abfrage ist auf die eigene Organisation beschränkt. Test- und Produktivsystem sind getrennt, Testdaten werden nicht mit Echtdaten vermischt.

Organisation: Verarbeitungsverzeichnis nach Art. 30 DSGVO; dokumentierter Ablauf für Sicherheitsvorfälle; regelmäßige Überprüfung der Maßnahmen und der Plattform auf Schwachstellen; Löschkonzept gemäß § 9 dieses Vertrags.

