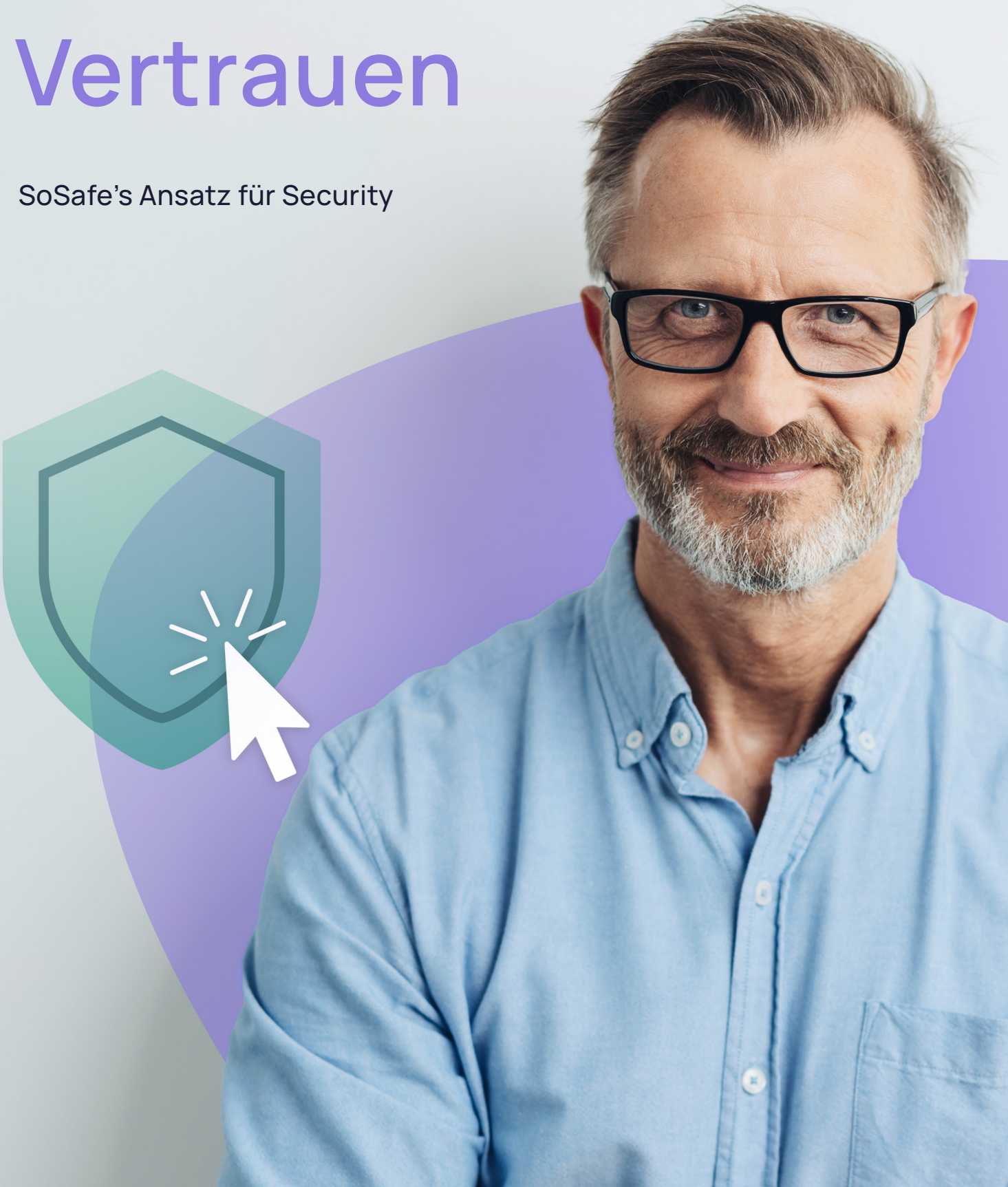
sosafe

Sicherheit und Vertrauen

SoSafe's Ansatz für Security



Index

Unser Ansatz zur Informationssicherheit

Unsere Motivation in Sachen Sicherheit 3
Unser Team 3
Assessments durch Dritte 4

Sicherheit im internen Betrieb

Access management 5
Grundprinzipien des Access Managements 5
Sicherheit unserer Endgeräte 6

Sicherheit im Arbeitsalltag

Log-Management 7
Business Continuity und Disaster Recovery Management 7
Back-up-Management 8

Sicherheit gespeicherter Daten

Datenzentren 8
Datenverschlüsselung 8
Key Management 8
Verwaltung des Zugriffs auf Kundendaten 9
Aufbewahrung und Löschung von Daten 9

Sicherheit im Team

Security Awareness Training 10
Security-Champions-Programm 10

Schutz vor Bedrohungen

Sicherheitsprüfung 11
Verwaltung von Schwachstellen 11
Protokoll bei Sicherheitsvorfällen 11

Unser Ansatz zur Informations-sicherheit

Dieses White Paper bietet Ihnen detaillierte Einblicke in den ganzheitlichen Sicherheitsansatz, den wir bei SoSafe verfolgen. Wir erläutern die wichtigsten Prozesse und Prüfungen in verschiedenen sicherheitsrelevanten Bereichen, die es uns ermöglichen, sowohl unsere eigene Umgebung (einschließlich unserer cloudbasierten Plattform) zu schützen als auch höchste Sicherheitsstandards bei der Entwicklung und Bereitstellung unserer Produkte für unsere Nutzenden zu gewährleisten.

Unsere Motivation in Sachen Sicherheit

Sicherheit gehört zu unseren höchsten Prioritäten. Als Anbieter für Security-Awareness-Produkte haben wir den Anspruch, einen hohen Sicherheitsstandard beim Schutz von Kundinnen und Kunden zu gewährleisten.

Je weiter unser Unternehmen wächst, desto mehr Organisationen setzen auf unsere Produkte und der Bedarf an starken Sicherheitsstrukturen gemäß modernster Standards steigt kontinuierlich.

Der Erfolg der SoSafe GmbH hängt maßgeblich davon ab, dass Kunden- sowie unsere eigenen Unternehmensdaten stets aktuell und unverfälscht sind und mit der nötigen Vertraulichkeit behandelt werden.

Unser Team

Zur Erfüllung unserer hohen Sicherheitsansprüche arbeiten wir mit Sicherheits-expertinnen und -experten aus verschiedenen Bereichen zusammen. Wir sind immer auf der Suche nach qualifizierten Profis, um bei SoSafe eine moderne Sicherheitsstruktur aufzubauen, aufrechtzuerhalten und weiter zu optimieren. Unser Ziel, zum führenden Unternehmen in der Sicherheit zu werden, spiegelt sich auch in der Struktur unseres Sicherheitsteams wider:

- **Chief Information Security Officer (CISO) -** Leitet die Sicherheits-maßnahmen bei SoSafe und ist für die Überwachung und den Erhalt der internen Sicherheit bei SoSafe verantwortlich, indem er die reibungslose Zusammenarbeit der verschiedenen Entscheidungsträger im Sicherheitsbereich sicherstellt.
- **Head of Information Security -** Verantwortlich für die kontinuierliche Entwicklung von modernen Informationssicherheitsprozessen, Risikomanagement, Compliance- und Governance-Regelungen.
- **Information Security Manager -** Verantwortlich für die Prozesse und die Überwachung der Informationssicherheit, einschließlich der Einhaltung der Anforderungen der Branche, der Zertifizierungen und der Aufrechterhaltung des Betriebs unseres ISMS.

- **Application Security -** Verantwortlich für die Sicherheit unserer Produkte und Plattformen.
- **SOC Team -** Verantwortlich für das Management von Sicherheitsvorfällen und die Überwachung unserer Systeme, Penetrationstests, prädiktive Angriffsanalyse und die Analyse der aktuellen Bedrohungslage.
- **Legal -** Verantwortlich für die Compliance mit rechtlichen Anforderungen und Zertifizierungen.
- **Data Protection Officer (DPO) -** Verantwortlich für die Compliance mit der DSGVO, wann immer SoSafe personenbezogene Daten verarbeitet.

Über unser Expertenteam hinaus absolvieren alle Mitarbeitenden bei SoSafe unsere Cyber Security E-Learnings und verfügen somit über das nötige Wissen, um aktiv zum Schutz unserer Sicherheit beizutragen.

Assessments durch Dritte

ISO-27001

Wir haben den ISO-27001-Audit erfolgreich abgeschlossen und sind ISO-zertifiziert, ab dem 20. Dezember 2022 mit jährlichen Leistungsüberwachungs-prüfungen. Wir sind bestrebt, unsere regelmäßigen Audits durch unabhängige Dritte beizubehalten, die sich ebenfalls regelmäßig SOC1-, SOC2- bzw. ISO/IEC 27001-Audits unterziehen, um ihre Praktiken zu verifizieren.

ISO-Zertifikat herunterladen →

TISAX

Die Themen Vertraulichkeit, Verfügbarkeit und Unversehrtheit von Daten haben bei SoSafe einen sehr hohen Stellenwert. Um höchste Standards der Sicherheit zu gewährleisten, nehmen wir am TISAX-Modell (Trusted Information Security Assessment Exchange) teil, das im Auftrag des Verbands der Automobilindustrie (VDA) von der ENX Association gesteuert und betreut wird.

TISAX-Assessments werden von zugelassenen Prüfdienstleistern durchgeführt, die ihre Qualifikationen regelmäßig nachweisen müssen. Bitte beachten Sie, dass die Ergebnisse der TISAX-Assessments nicht grundsätzlich öffentlich zugänglich sind. Um exklusiven Zugriff auf unsere Prüfergebnisse zu erhalten, besuchen Sie bitte das Portal der ENX Association: https://enx.com/TISAX/tisaxassessmentresults. Unsere Ergebnisse sind über die Assessment-ID ACMGNV und die Scope-ID S02C8M zugänglich.

Sicherheit im internen Betrieb

Ein wirksames Sicherheitskonzept beginnt mit der Sicherung unserer internen Umgebungen. Unsere interne Sicherheitsstrategie umfasst die folgenden Sicherheitsgrundsätze:

Access Management

In unserem spezifischen Anwendungsbereich bezieht sich „Access" auf die Nutzung von IT-Systemen, Systemkomponenten, Netzwerken und Daten.

Grundprinzipien des Access Managements

- **Need-to-know-Prinzip**
  Die Mitarbeitenden von SoSafe erhalten nur jene Rechte und privilegierten Rechte, die zur Ausführung ihrer Aufgaben unbedingt erforderlich sind. Darüber hinaus werden Administratorrechte äußerst sparsam vergeben.

- **Least-privilege-Prinzip**
  Nutzende erhalten nur jene Rechte und privilegierten Rechte, die für die Ausführung ihrer Aufgaben unbedingt erforderlich sind.

- **Aufgabentrennung und Vier-Augen-Prinzip**
  Bei der Vergabe von User-Rechten gilt das Prinzip der Aufgabentrennung und das Vier-Augen-Prinzip bei sich widersprechenden Zuständigkeiten.

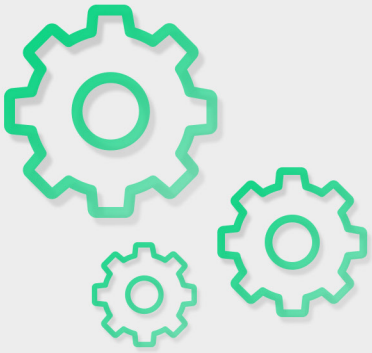
- **Nutzerverwaltung**
  Die Benutzer-, Gruppen- und Rechteverwaltung erfolgt mittels Methoden wie SSO zentralisiert, um die Anzahl an zu pflegenden Nutzerverzeichnissen möglichst gering zu halten.

- **Gewährung, Anpassung und Entzug von Rechten**
  Änderungen von Zugriffsrechten werden nach dem Vier-Augen-Prinzip durchgeführt. Wenn User-Rechte außerhalb der definierten Grundberechtigungen vergeben werden, ist dies zu dokumentieren. Für Administratorzugriff ist eine zweifache Genehmigung erforderlich, das heißt, er muss sowohl vom Asset Owner als auch von einem Vorgesetzten bestätigt werden.

  Alle Zugriffsrechte werden mindestens einmal im Jahr überprüft. Administrator-Zugriffsrechte werden gemäß unserer Access-Management-Richtlinie mindestens alle sechs Monate überprüft sowie bei relevanten Änderungen eines Assets.

  Gemäß dem Need-to-know- und Least-privilege-Prinzip werden inaktive Konten blockiert oder gelöscht.

  Zu guter Letzt werden alle Zugriffsrechte nach dem Offboarding von Mitarbeitenden innerhalb von 24 Stunden entzogen.



→ **Zugriff auf Quellcode**
Der Zugriff auf Quellcode und das Code Repository ist eingeschränkt, um nicht autorisierten Zugriff auf den Code sowie die Weitergabe von Unternehmensgeheimnissen zu verhindern. Das Need-to-know-Prinzip und Least-privilege-Prinzip sind, soweit möglich, immer einzuhalten. Mit besonders großer Sorgfalt wird bei temporären Mitarbeitenden, wie Werkstudierenden, Praktikantinnen und Praktikanten sowie externen Developern, vorgegangen.

→ **Authentifizierungsanforderungen**
Ein Account wird nach sechs fehlgeschlagenen Versuchen gesperrt.

Remote-Zugriff von externen öffentlichen Netzwerken ist nur über das Unternehmens-VPN möglich, das die übertragenen Daten verschlüsselt und nur mittels 2FA zugänglich ist.

Sicherheit unserer Endgeräte

Alle Endgeräte wie auch unsere Datenspeicher und File-Sharing-Plattformen werden durch Endpoint Protection gesichert.

Alle Mitarbeitenden von SoSafe verwenden unternehmenseigene, durch ein Antivirus-System geschützte Mobilgeräte, um maximale Sicherheit bei der Nutzung von Unternehmensdaten zu gewährleisten. Der Schutz der mobilen Geräte wird durch eine Mobile Device Management Software sichergestellt, die die Nutzenden selbst nicht deaktivieren können.

Freelancern, die eine Zusammenarbeit mit SoSafe beginnen, werden, je nach Aufgabe und Zugriffsanforderungen, ebenfalls Mobilgeräte bereitgestellt. So erhalten wir auch im Kontakt mit Dritten dasselbe hohe Sicherheitsniveau aufrecht. Die zur Verfügung gestellte Ausrüstung kann die Bereitstellung von Virtual Machines oder vollständig durch SoSafe verwaltete Mobilgeräte umfassen.

Alle Mitarbeitenden werden zudem im sicheren Umgang mit Mobilgeräten geschult.

Sicherheit im Arbeitsalltag

Log-Management

→ **Erforderliche Logging-Aktivitäten**
Alle Hosts und Netzwerkgeräte erzeugen für alle Systemkomponenten Sicherheitsprotokolle.

Alle Hosts und Netzwerkgeräte senden bei Verarbeitungsfehlern der Logging-Daten Warnungen, wie bei Software-/Hardwarefehlern, Störungen der Log-Speichermechanismen und bei Erreichen oder Überschreiten der maximalen Log-Speicherkapazität. Alle Warnungen müssen so zeitnah wie möglich ausgegeben werden.

→ **Zentralisiertes Loggen**
Sicherheitsvorfälle werden in Echtzeit oder so schnell es die Technologie erlaubt an einen Logging-Service übertragen. Die Integrität der Log-Infrastruktur bleibt erhalten, zum Beispiel werden Logs im Read-only-Modus gespeichert.

→ **Erforderliche Überwachungsaktivitäten**
Wir entwickeln und implementieren Prozesse zur Überprüfung der Log-Daten aller Systeme, um Abweichungen und verdächtige Aktivitäten zu erkennen, wie zum Beispiel durch unser SIEM-System. Es werden Security Baselines entwickelt und automatisierte Überwachungstools genutzt, die bei erkannten Ausnahmen eine Warnung ausgeben.

→ **Autorisierte Personen**
Gemäß dem Need-to-know-Prinzip werden Logs geschützt, indem nur jene Personen Zugriff darauf haben, die diesen zur Ausführung ihrer Aufgaben und zum Schutz der Dateien vor unautorisierten Änderungen benötigen. Der Zugriff auf Log-Management-Systeme wird aufgezeichnet.

→ **Compliance**
Daten werden an einem sicheren Ort geloggt, wobei die Aufbewahrungs-anforderungen, geschäftliche Anforderungen wie auch rechtliche und regulatorische Anforderungen (zum Beispiel DSGVO und Bundesdatenschutzgesetz) berücksichtigt werden.

Log-Dateien, die identifizierbare personenbezogene Daten enthalten, erfordern die Bestätigung durch unseren DPO.

→ **Aufbewahrung**
Elektronische Logs, die im Rahmen der in diesem Dokument beschriebenen Überwachung erstellt werden, werden mindestens 90 Tage lang aufbewahrt und bleiben während dieser Zeit zugänglich.

Business continuity und disaster recovery management

Wir agieren gemäß einem bestehenden Business-Continuity-Management-Plan. Dieser ist in einer Business-Continuity-Management-Richtlinie im Detail beschrieben und basiert auf der Norm ISO 22301:2019 für Business Continuity Management.

Back-up-Management

SoSafe folgt einem umfassenden Back-up-Plan für alle Datenelemente und Systeme. Für jedes einzelne gelten in unserer Back-up-Richtlinie spezifisch festgelegte Anforderungen. Für unsere Datenbanken, die Kundendaten enthalten, gelten spezielle Anforderungen.

→ **Zeitplan**
Jede Nacht wird ein vollständiges Back-up unserer Datenbank erstellt. Davon abgesehen wird sie kontinuierlich per WAL (Write-Ahead Logging) gesichert.

→ **Angestrebte Wiederherstellungsdauer (RTO)**
Eine vollständige Wiederherstellung (bei Zusammenbruch der gesamten Datenbank) nimmt je nach Umfang der WAL-Datensätze zwischen 60 und 90 Minuten in Anspruch.
Bei teilweisem Datenverlust ist es möglich, innerhalb von einer Stunde eine vollständig funktionsfähige Kopie zu erstellen und die Daten wiederherzustellen.

Sicherheit gespeicherter Daten

Datenzentren

Sowohl die Daten von SoSafe als auch die Daten seiner Kundinnen und Kunden werden in der AWS-Cloud gehostet, die einen sehr hohen physischen Sicherheitsstandard bietet. Unser physisches Sicherheitsrisiko ist als Cloud-basiertes Unternehmen vergleichsweise gering. Darüber hinaus bietet das Datenzentrum verschiedene Sicherheitsmaßnahmen, die den Schutz von Kundendaten gemäß höchster Sicherheitsstandards gewährleisten.

Datenverschlüsselung

Alle in unseren Produkten genutzten Kundendaten werden zum Schutz vor nicht autorisierter Weitergabe oder Änderung während der Übertragung über öffentliche Netzwerke mindestens mit TLS 1.2 verschlüsselt. Die TLS-Implementierung verlangt die Nutzung starker Cipher-Suites und Schlüssellängen, soweit vom Browser unterstützt. Alle unsere Systeme und Datenlaufwerke, die Kundendaten enthalten, nutzen nach Industriestandard im Ruhezustand Full-Disk AES-Verschlüsselung und folgen den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) bei der Auswahl von kryptografischen Protokollen, Algorithmen und Schlüssellängen.

Key management

SoSafe nutzt fortschrittlichste Technologien zur sicheren Erstellung, Speicherung, Archivierung, Wiederherstellung, Verteilung, Widerrufung und Löschung von Schlüsseln, die den Empfehlungen des National Institute of Standards and Technology (NIST) folgen.

Persönliche Kennwörter werden in einem Passwortmanager gespeichert, der unautorisierten Zugriff unmöglich macht.

Verwaltung des Zugriffs auf Kundendaten

Kunden und Kundinnen von SoSafe werden nicht dazu aufgefordert, personenbezogene Daten besonderer Kategorien mit uns zu teilen. Wir behandeln alle Kundendaten als gleichermaßen vertraulich und folgen strengen Protokollen bei deren Verwaltung. Innerhalb von SoSafe haben nur autorisierte Mitarbeitende Zugriff auf in unserem System gespeicherte Kundendaten. Der Zugriff ist auf Gruppen mit besonderen Rechten beschränkt, es sei denn es wird spezieller Zugriff auf Anfrage genehmigt, zum Beispiel wenn Kundinnen und Kunden auf ihre Daten zugreifen möchten. In solchen Fällen wird eine zusätzliche Authentifizierung per 2FA angefordert. Nicht autorisierter oder unangemessener Zugriff auf Kundendaten wird als Sicherheitsvorfall gewertet und demnach gemäß unserem Incident-Management-Prozess gehandhabt. Dieser besagt, dass betroffene Kunden über den festgestellten Verstoß gegen unsere Richtlinien informiert werden müssen.

Aufbewahrung und Löschung von Daten

→ **Kundendaten**
Nur Kundenstammdaten (falls als personenbezogene Daten qualifizierbar) werden gemäß § 147 AO und § 257 HGB über einen Zeitraum von zehn Jahren aufbewahrt.

Die Archivierung von Kundendaten erfolgt drei Monate nach Ablauf der Lizenzen (um die Datenqualität für folgende Lizenzen zu gewährleisten). Dieser Zeitraum kann auf Anfrage der Kundin oder des Kunden erweitert oder verkürzt werden.

Vier Wochen vor der Archivierung erhält unsere Kontaktperson beim Kundenunternehmen eine Erinnerung, die Reports/Zertifikate herunterzuladen.

SoSafe bewahrt gemäß der ISO-Norm 27001 zur Löschung und Vernichtung von Daten einen Nachweis der sachgemäßen Vernichtung auf. Der Norm zufolge muss jedes Speichermedium vor seiner Entsorgung oder Wiederverwendung überprüft werden, um sicherzustellen, dass alle sensiblen Daten und lizenzierte Software vollständig gelöscht oder sicher überschrieben wurde.

Wenn eine Datenlöschung aus dem SoSafe Management System durch eine Kundin oder einen Kunden erfolgt, wird ein Löschungsbericht erzeugt, der die Zeit und den Umfang der Löschung dokumentiert. Der Bericht wird aufbewahrt und dem Kunden auf Anfrage bereitgestellt.

→ **Mitarbeitendendaten unserer Kundinnen und Kunden**
Unsere Kundinnen und Kunden haben jederzeit die Möglichkeit, Daten einzelner Personen oder aller Mitarbeitenden manuell über die Systemsteuerung zu löschen.

Der Zugriff auf unsere E-Learning-Plattform wird für gelöschte Nutzende am Ende des Lizenzzeitraums deaktiviert.

Personenbezogene Daten der Teilnehmenden einer Phishing-Simulation oder einer E-Learning-Kampagne werden automatisch aus der User-Datenbank gelöscht, sobald die Kundin oder der Kunde archiviert wird (drei Monate nach Ablauf der Lizenz).

Nach der Löschung haben wir bei Bedarf noch 28 Tage lang die Möglichkeit, die Daten aus dem Back-up wiederherzustellen.

→ **Active directory**
Wenn bestimmte User von unseren Kundinnen und Kunden in Active Directory (AD) deaktiviert werden oder ihre Nutzungsrechte der SoSafe E-Learnings verlieren, werden sie auch auf der SoSafe-Plattform deaktiviert. Das heißt, sie können sich nicht mehr Einloggen und werden bei künftigen Phishing-Kampagnen nicht mehr mit einbezogen.

Wenn Nutzende innerhalb von 30 Tagen in Active Directory (AD) reaktiviert werden oder ihre Rechte zur Nutzung der SoSafe E-Learnings zurückerhalten, werden sie auch auf der SoSafe-Plattform reaktiviert und können ihren Lernpfad mit ihrem vorherigen Status fortsetzen.

Nach 30 Tagen werden deaktivierte User einschließlich ihrer Fortschrittsdaten gelöscht. Wenn ein Nutzender danach in AD reaktiviert wird, wird auf der SoSafe-Plattform ein neuer User erstellt – alle vorherigen Daten sind nicht mehr zugänglich.

Sicherheit im Team

Security Awareness Training

Als Teil ihres Onboardings durchlaufen alle Mitarbeitenden von SoSafe ausnahmslos unser Security Awareness Training und nehmen auch im weiteren Verlauf regelmäßig an Trainings teil, damit Cybersicherheit in ihrem Arbeitsalltag immer präsent bleibt. Als Teil der E-Learnings führen wir regelmäßige Phishing-Simulationen durch, damit unsere Mitarbeitenden optimal auf mögliche Angriffe vorbereitet sind und im Ernstfall selbstbewusst reagieren können.

Unser Security-Awareness-Programm deckt Themen wie aktuelle Bedrohungen und Scam-Taktiken, sichere Arbeitsweisen, potenziell gefährliche Verhaltensweisen, die zum Sicherheitsrisiko werden können, sowie Compliance und regulatorische Aspekte ab.

Security-Champions-Programm

Unser Security-Champions-Programm hilft uns, die Sicherheitskultur und die Cyber Security Awareness innerhalb von SoSafe zu stärken sowie die Sicherheit bei der Entwicklung und Einführung von Produkten zu verbessern.

Dabei liegt unser Fokus in erster Linie auf den Product-Development- und Engineering-Abteilungen, in denen unsere Security Champions die Lücke zwischen Application Security und Experience-Teams füllen. Zudem stellen sie sicher, dass verbindliche Prüfphasen (Security Gates) erfüllt sind und die Sicherheitskontrollen im Software-Entwicklungszyklus nicht umgangen werden.

Schutz vor Bedrohungen

Sicherheitsprüfung

Die Sicherheitsprüfung ist ein wichtiger Aspekt des Entwicklungszyklus und wird in der Implementierungsphase sowie in der Prüfphase des Secure Development Lifecycle (SDLC) umgesetzt.

In der Implementierungsphase erfolgt die Sicherheitsprüfung durch unsere Tools, die einem Shift-Left-Ansatz folgen und gewährleisten, dass der erstellte Code sicher ist. Darüber hinaus werden alle externen Open-Source-Bibliotheken in unserem Produkt kontinuierlich überwacht.

In der Testphase wird die Sicherheitsprüfung durch die Application Security Engineers gewährleistet, wobei die Sicherheit aller wichtigen Features dynamisch getestet wird.

Verwaltung von Schwachstellen

→ **Vulnerability Scans**
Unsere Plattform wird durchgehend mittels automatischer Schwachstellenscans überwacht, wobei aufgedeckte Schwachstellen umgehend behoben werden.

→ **Scannen externer Open-Source-Bibliotheken**
Die von SoSafe genutzten externen Open-Source-Bibliotheken werden stetig im Rahmen unserer Software Composition Analysis gescannt und zum Patchen an das zuständige Team weitergeleitet. Bibliotheken werden unter Berücksichtigung der Service Level Agreements und basierend auf dem Ausmaß der Schwachstelle gepatcht.

Protokoll bei Sicherheitsvorfällen

→ **Simulationen von Sicherheitsvorfällen**
Damit alle Beteiligten im Falle eines echten Cyberangriffs genau wissen, wie zu reagieren ist, müssen die Schritte bereits vorab wiederholt ausgeführt und so verinnerlicht werden. SoSafe führt regelmäßig Übungen zur Reaktion auf Zwischenfälle durch, um Praktiken zur Reaktion auf Zwischenfälle zu entwickeln.

Melden Sie uns Ihre Sicherheitsbedenken