Handshake

Datenschutz und Sicherheit

Unser Engagement für Datenschutz und Sicherheit

Mehr als 1.500 Universitäten in der EU, Großbritannien und den USA vertrauen auf Handshake, um die persönlichen Daten ihrer Studierenden zu schützen und ihre Studierenden während der Karriereorientierung zu begleiten.

Wir von Handshake verpflichten uns, eine branchenführende Infrastruktur für Datenschutz und Sicherheit zu schaffen, die volle Transparenz bietet. Wir stellen sicher, dass die Informationen, die wir erhalten, mit Sorgfalt behandelt werden und unser Datenschutz den anwendbaren Standards, Gesetzen und Vorschriften entspricht.

Das Engagement von Handshake für den Datenschutz geht sogar über die Einhaltung von Vorschriften hinaus. Wir evaluieren und verfeinern unsere Prozesse und Richtlinien kontinuierlich, um in der Branche führend zu sein, wenn es um den verantwortungsvollen Umgang mit Daten, das kontinuierliche Arbeitgeber-Screening und die volle Kontrolle durch die Studierenden geht.

Dieser Leitfaden gibt Antworten auf häufig gestellte Fragen und einen umfassenden Überblick über die Datenschutz- und Sicherheitsmaßnahmen bei Handshake, speziell für unsere europäische Plattform.

Häufig gestellte Fragen

Ist Handshake DSGVO-konform?

Als führendes globales Unternehmen, das personenbezogene Daten verwaltet, hält sich Handshake an alle geltenden Datenschutzbestimmungen, einschließlich der Datenschutz-Grundverordnung (DSGVO).

Erfahren Sie mehr über den Datenschutz bei Handshake.

Wie gewährleistet Handshake die Sicherheit der verarbeiteten Daten?

Bei Handshake ist die Sicherheit ein Kernelement unserer Plattform, Infrastruktur, Prozesse und Teamkultur, um den Schutz der Daten unserer Partner und Nutzer zu gewährleisten. Die folgende Zusammenfassung umreißt einige der wichtigsten Maßnahmen, die Handshake zum Schutz der verarbeiteten Daten ergreift, wobei detaillierte Informationen im Abschnitt "Sicherheit" dieses Leitfadens verfügbar sind.

- Handshake betreibt separate Plattformen in Europa und Amerika. Unsere europäische Plattform, die in der Google Cloud gehostet wird, stellt sicher, dass alle Daten, die über sie verwaltet werden, geschützt sind:
  - In Deutschland gespeichert
  - Gesichert während der Übertragung mit TLS 1.2 oder höher
  - Verschlüsselt im Ruhezustand mit 256-Bit-AES-Verschlüsselung oder stärker

- Nach dem Prinzip der geringsten Rechte kontrolliert Handshake sorgfältig den Zugang zu verarbeiteten Daten. Standardmäßig haben Teammitglieder keinen Zugang zu verarbeiteten Daten, und der Zugang wird regelmäßig überprüft.
- Unser Team befindet sich in der EU, im Vereinigten Königreich und in den USA, wobei unsere europäischen Produkt- und Entwicklungsteams hauptsächlich in Berlin ansässig sind.
- Unsere Sicherheitsmaßnahmen umfassen strenge Tests auf Schwachstellen in jedem Build, die die zehn größten Sicherheitsrisiken für Anwendungen abdecken, auch bekannt als die OWASP Top 10.
- Wir beauftragen führende externe Agenturen mit der vierteljährlichen Durchführung externer Scans des Handshake-Systems und führen mindestens einmal jährlich, bei Bedarf auch öfter, umfassende Penetrationstests der Anwendung sowie der zugrunde liegenden Cloud-Infrastruktur durch.
- Sicherheit und Datenschutz sind integraler Bestandteil unserer Einstellungs- und Einführungsprozesse, die durch regelmäßige Sensibilisierungs- und Schulungsprogramme unter der Leitung unserer engagierten Sicherheits- und Datenschutzteams unterstrichen werden, um sicherzustellen, dass unser Engagement für den Datenschutz in der gesamten Organisation aufrechterhalten wird.

Wo werden die Handshake-Daten gespeichert?

Unsere europäische Plattform wird in der Google Cloud betrieben, die Datenspeicherung erfolgt in Deutschland. Wir verpflichten uns dazu, personenbezogene Daten, die über unsere Dienste erhoben werden, innerhalb der EU oder des Vereinigten Königreichs zu speichern und zu verarbeiten, wann immer dies möglich ist. Sollte es notwendig sein, personenbezogene Daten außerhalb des Vereinigten Königreichs und der EU zu verwalten, ergreift Handshake alle notwendigen Maßnahmen, um sicherzustellen, dass die betroffenen Personen weiterhin den Schutz erhalten, der den EU-Datenschutzstandards entspricht.

Um einige unserer Dienstleistungen zu erbringen, bedient sich Handshake Dritter, mit denen wir Daten austauschen können. Unsere Liste der Unterauftragsverarbeiter enthält Einzelheiten zu den Dienstleistungen, dem Zweck, den Datenkategorien und dem Speicherort aller Datenübertragungen an Drittpartner.

Handshake verfügt über ein gut definiertes Risikomanagement-Programm für Anbieter und Sicherheitspersonal, das die Sicherheitslage von Drittanbietern als Teil des Beschaffungsprozesses überprüft, um den Umfang der übertragenen Daten zu begrenzen und sicherzustellen, dass vergleichbare Vertraulichkeits- und Datenverarbeitungs-Verträge (DPAs) vorhanden sind, um die Anforderungen der DSGVO zu erfüllen.

Erfahren Sie mehr über Datenspeicherung und -übertragung bei Handshake.

Ist Handshake nach dem Schrems-II-Urteil, das das Privacy Shield für ungültig erklärt hat, für die Einhaltung der neuen Grundsätze des EU-U.S. Data Privacy Framework zertifiziert?

Handshake ist vom US-Handelsministerium für die Einhaltung des EU-U.S. Data Privacy Framework zertifiziert.

Nach dem Schrems-II-Urteil des Gerichtshofs der Europäischen Union (EuGH), mit dem der Privacy Shield im Jahr 2020 für ungültig erklärt wurde, hat die Europäische Kommission einen neuen Angemessenheitsbeschluss für den EU-US-Datenschutz Rahmen erlassen. Der Angemessenheitsbeschluss stellt fest, dass die Vereinigten Staaten bei der Übermittlung personenbezogener Daten aus der EU in die USA für Unternehmen, die am EU-US-Datenschutz Rahmen teilnehmen, ein Schutzniveau für personenbezogene Daten bieten, das mit dem der EU vergleichbar ist.

Im Einklang mit dem EU-US-Datenschutz Rahmen verfügen wir über umfassende Datenschutzrichtlinien und -verfahren, die die Erhebung, Nutzung und Speicherung personenbezogener Daten überwachen. Diese Initiativen umfassen die Gewährleistung der Transparenz unserer Datenverarbeitungs-Praktiken, die Wahrung der Datenintegrität und die Beschränkung der Zwecke, für die Daten verwendet werden sowie die Durchsetzung strenger Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff und Datenverletzungen.

Unsere Zertifizierung unterstreicht unser Engagement für die Einhaltung der höchsten Datenschutzstandards für alle unsere Nutzer in der Europäischen Union. Das Engagement von Handshake für den Schutz der Privatsphäre geht über die Einhaltung von Vorschriften hinaus. Wir bewerten und verfeinern unsere Datenschutzrichtlinien kontinuierlich, um mit den sich ändernden Vorschriften und den besten Praktiken der Branche Schritt zu halten.

Erfahren Sie mehr über den Datenschutz bei Handshake.

Haben die Studierenden die Kontrolle über ihre persönlichen Daten?

In Übereinstimmung mit der DSGVO behält der Einzelne die Kontrolle über seine persönlichen Daten. Handshake verarbeitet Daten ausschließlich wie in unserer Datenschutzrichtlinie und den Nutzungsbedingungen beschrieben und in Übereinstimmung mit den Datenverarbeitungs-Verträgen, die mit Universitätspartnern abgeschlossen wurden.

Unsere Produkt- und Sicherheitsteams sind bestrebt, Best Practices im Bereich DSGVO in Kenntnis der Sachlage in die Handshake-Plattform einzubetten. Wir respektieren die Rechte der Studierenden an ihren persönlichen Daten und verpflichten uns, mit Universitäten zusammenzuarbeiten, um die Effektivität ihrer Career Services zu verbessern und gleichzeitig die Privatsphäre der Studierenden zu schützen.

Erfahren Sie mehr über den Datenschutz bei Handshake.

Wer ist für die Verarbeitung der personenbezogenen Daten der Studierenden zuständig?

Bei personenbezogenen Daten, die von Universitäten an Handshake übermittelt werden, um die Erbringung von Dienstleistungen zu verbessern, fungiert die Universität als Datenverantwortlicher, während Handshake als Verarbeiter fungiert.

Wenn studentische Nutzer persönliche Daten an Handshake übermitteln, indem sie ihr Konto aktivieren sowie den Handshake-Nutzungsbedingungen und Datenschutzrichtlinien zustimmen, übernehmen sowohl Handshake als auch die Universität

gemeinsam die Rolle der Daten Verantwortlichen. Dies ermöglicht es den Studierenden, die Sichtbarkeit ihres Profils im Handshake-Netzwerk zu kontrollieren, während die Universitäten detaillierte Einblicke in das Engagement der Studierenden erhalten und so die Verbindungen und die Qualität der angebotenen Dienstleistungen verbessern können.

Erfahren Sie mehr über die Rollen von Data Controller und Processor bei Handshake

Wie verwendet Handshake persönliche Daten?

Handshake verarbeitet personenbezogene Daten ausschließlich, um allen Nutzern unserer Plattform die wertvollsten und effektivsten Dienstleistungen zu bieten. Die Verwendung personenbezogener Daten variiert je nach den Interaktionen unserer Partner und Nutzer mit Handshake, den von ihnen genutzten Diensten und den von ihnen gewählten Präferenzen. In Bezug auf unsere europäischen Kunden und Nutzer stellen wir sicher, dass personenbezogene Daten nur innerhalb der Grenzen der DSGVO verarbeitet werden. Handshake ist dem Datenschutz verpflichtet und wird niemals persönliche Daten an Dritte verkaufen.

Erfahren Sie mehr über die Verwendung personenbezogener Daten durch Handshake.

Wie werden die Nutzer darüber informiert, wie Handshake Daten verarbeitet?

Die Nutzer werden durch unsere Datenschutzrichtlinien und Nutzungsbedingungen, denen sie bei der Registrierung zustimmen, über die Verarbeitung personenbezogener Daten durch Handshake aufgeklärt. Darüber hinaus sorgen wir für Transparenz, indem wir Informationen über die Verarbeitung personenbezogener Daten in wichtigen Bereichen der Handshake-Plattform bereitstellen, um die Nutzer zu informieren und aufzuklären. Schließlich können sich unsere Nutzer jederzeit an uns wenden, um Informationen darüber zu erhalten, welche spezifischen Daten wir zu welchen Zwecken verarbeiten.

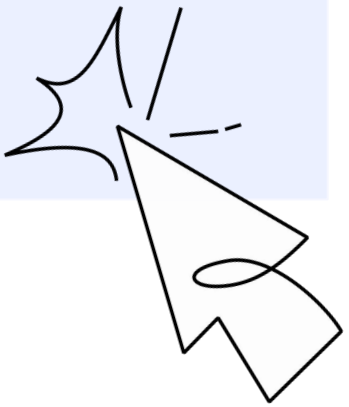
Führt Handshake Datenschutz-Folgenabschätzungen (DPIAs) durch?

Ja, im Rahmen unserer Verpflichtung zum Schutz Ihrer Privatsphäre und zur Einhaltung der Datenschutzbestimmungen führen wir bei Bedarf Datenschutz-Folgenabschätzungen (Data Protection Impact Assessments, DPIA) durch. Diese Bewertungen helfen uns, potenzielle Risiken im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten zu ermitteln und zu mindern, um sicherzustellen, dass Ihre Daten mit größtmöglicher Sorgfalt und Sicherheit behandelt werden.

Wie wir unser Engagement umsetzen

Datenschutz

Handshake legt großen Wert auf den Schutz der Privatsphäre und die Integrität der persönlichen Daten. Wir stellen immer den einzelnen Nutzer in den Mittelpunkt unserer Datenverarbeitungs-Entscheidungen und gewährleisten die Einhaltung der Datenschutzstandards. Der folgende Abschnitt bietet einen detaillierten Einblick in unsere Datenschutzpraktiken, die speziell auf unsere europäische Plattform zugeschnitten sind.



Datenschutzbestimmungen

Unsere Datenschutzrichtlinie beschreibt unsere Praktiken in Bezug auf die von Handshake verarbeiteten Informationen.

Daten, die wir sammeln

Wir erhalten Daten, die uns nach dem Ermessen unserer Partner und Nutzer mitgeteilt werden, und sammeln Informationen über Interaktionen auf unserer Plattform. Wir verarbeiten verschiedene Arten von Daten, wie unten beschrieben.

Daten von Studierenden oder Alumni: Wir erhalten personenbezogene Daten über Studierende, wenn sie ein Studierenden- oder Alumni-Konto anlegen, ihr Profil aktualisieren, auf Fragen oder Umfragen auf unserer Website antworten oder die Handshake-Dienste anderweitig nutzen sowie von unseren Partneruniversitäten und von anderen Datenquellen Dritter.

Von Universitätspartnern: Unsere Hochschulpartner geben Informationen über ihre Studierenden an uns weiter, damit wir ihnen Dienste zur Verfügung stellen können, die sie zur Verwaltung ihrer Career Center nutzen. Jeder Hochschulpartner wählt aus, welche Daten er weitergibt, darunter Name, Postanschrift und E-Mail-Adresse, Kurs und Abschlussdatum. Dazu können auch geschützte Merkmale gehören, die für ihre Berichtszwecke verwendet werden. Der Hochschulpartner ist der Datenverantwortliche für diese Daten und sie werden von Handshake nur auf Anweisung des Partners verarbeitet.

Von den Studierenden, ihren Konten und ihren Profilen: Die Studierenden können sich dafür entscheiden, uns zusätzliche Informationen mitzuteilen, z. B. eine persönliche E-Mail-Adresse, Telefonnummer, Berufserfahrung, Lebenslauf und Zeugnisse sowie Antworten auf Fragen zu ihren Interessen und Aktivitäten, Diese Angaben unterliegen unserer Datenschutzrichtlinie und unseren Nutzungsbedingungen. Sie können diese Informationen auch weitergeben, indem sie ihr Profil aktualisieren, Dokumente mit persönlichen Informationen hochladen oder Fragen oder Umfragen (z. B. die First Destination Survey) beantworten, die sie per E-Mail erhalten oder die ihnen im Rahmen der Dienste vorgelegt werden. Wir werden ihre Telefonnummer nicht verwenden, um Werbe- oder Marketing Nachrichten zu versenden.

Von Arbeitgeberbewertungen: Wir erhalten alle persönlichen Informationen, die Studierende in den eingereichten Arbeitgeberbewertungen angeben. Handshake sammelt diese Informationen auch dann, wenn die Bewertung nicht veröffentlicht oder publik gemacht wird.

Von Kommunikation, Abschriften oder Aufnahmen: Wir erhalten und speichern personenbezogene Daten, wenn Studierende sich entscheiden, an einem Video- oder Audio-Meeting, Anruf oder Webinar teilzunehmen, das über den Handshake-Service initiiert wurde, oder wenn sie sich entscheiden, während einer Handshake-Video- oder Audiokonferenz oder eines Anrufs mit anderen Nutzern per

Video, Audio oder Messaging zu kommunizieren (zusammenfassend "Handshake-Kommunikation"). Durch die Teilnahme an der Handshake-Kommunikation geben die Studierende Handshake die Erlaubnis, den Inhalt und die Aufzeichnungen der Handshake-Kommunikation zu speichern. Bei Audio- oder Videoaufzeichnungen erhalten sie eine Benachrichtigung (visuell oder anderweitig), wenn die Aufzeichnung aktiviert ist, und sie sollten das Meeting oder Webinar verlassen, wenn sie nicht damit einverstanden sind, aufgezeichnet zu werden. Wenn wir einen Drittanbieter von Video- und/oder Kommunikationsdiensten nutzen, um die Handshake-Kommunikation zu erleichtern, darf dieser Anbieter die persönlichen Daten der Studierenden oder den Inhalt der Kommunikation für keinen anderen Zweck als die Bereitstellung des Dienstes für uns verwenden.

Von Dritten: Wir können zusätzliche Informationen über Studierende von anderen Universitäten, Alumni- oder Berufsberatung Organisationen oder aus anderen Quellen erhalten.

Nutzungs- und Protokolldaten: Wenn Studierende die Website besuchen, protokollieren und speichern wir ihre IP-Adresse und technische Informationen über ihren Besuch, wie z. B. ihren Browsertyp und wie sie auf der Website vorankommen, wo sie sie verlassen haben usw. ("Nutzungsdaten"). Anhand der IP-Adresse können wir ihren allgemeinen Standort bestimmen.

Mobile Daten: Wenn Studierende die Handshake-Mobil-App nutzen, sammeln wir analytische Informationen über ihr Gerät, wie IP-Adresse, Betriebssystemversion und Clickstream.

Präzise Standortdaten: Für eine begrenzte Anzahl von Funktionen erlauben wir den Nutzern sich für die Erfassung von genauen Standortdaten (GPS-Daten) zu entscheiden. Wir verwenden diese Informationen nur, um Funktionen zu aktivieren, wie z. B. die Anzeige des genauen Standorts des Studierenden auf einer Karte bei einer Karrieremesse. Wir geben keine genauen Standortdaten an Dritte weiter und kombinieren keine genauen Standortdaten mit persönlichen Informationen zu Werbezwecken.

Daten des Arbeitgebers: Wenn Arbeitgeber ein Handshake-Arbeitgeber Konto einrichten, bitten wir um Kontaktinformationen, einschließlich E-Mail-Adresse und Telefonnummer, um eine Anlaufstelle für Universitäten und Verwaltungspersonal zu schaffen, die auf dem öffentlichen Profil der Studierenden zur Verfügung gestellt wird. Wir werden ihre Telefonnummer nicht verwenden, um ihnen ohne ihre ausdrückliche Zustimmung Werbe- oder Marketing Nachrichten zukommen zu lassen, die nicht im Zusammenhang mit ihrer Nutzung der Handshake-Dienste stehen.

Sicherheit der Finanzdaten

Handshake verwaltet, verarbeitet, speichert oder übermittelt keine sensiblen Finanzdaten. Wir bieten Hochschulpartnern die Integration mit Kreditkartenverarbeitern von Drittanbietern an, um Zahlungen für Karrieremessen, Veranstaltungen und Interviewtermine einzuziehen. Zu den aktuellen Integrationen gehören Stripe, CashNet und TouchNet.

Handshake hält als Händler die geltenden PCI-Vorschriften ein. Handshake führt vierteljährliche Scans für die Sicherheit-Konformität durch und verwendet einen vollständig PCI-konformen Infrastruktur-Stack. Ein AOC kann auf Anfrage zur Verfügung gestellt werden.

Wie wir personenbezogene Daten verwenden

Handshake verarbeitet personenbezogene Daten, um sicherzustellen, dass wir allen Nutzern der Plattform die wertvollsten und effektivsten Dienste zur Verfügung stellen und um unser Angebot zu verbessern. Die Verwendung personenbezogener Daten durch Handshake variiert je nachdem, wie Partner und Nutzer mit unserer Plattform interagieren, auf welche Dienste sie zugreifen und welche Einstellungen sie wählen.

Handshake beispielsweise erleichtert die Kontakte zwischen Arbeitgebern und Talenten in ganz Europa und ermöglicht es Arbeitgebern, Studierende mit sichtbaren Profilen über Veranstaltungen oder offene Stellen zu informieren. Dieser Ansatz trägt dazu bei, dass sich Studierende nicht aufgrund ihrer Vorstellungen von den Erwartungen der Arbeitgeber von Chancen ausschließen.

Die Studierenden haben die volle Kontrolle über die Sichtbarkeit ihrer Daten und können die Datenschutzeinstellungen ihres Profils nach ihren Wünschen anpassen.

Darüber hinaus ermöglicht Handshake den Universitätsmitarbeitenden die Bereitstellung von Karriere Dienstleistungen zu verwalten und zu

überwachen und einen umfassenden Überblick über die Karriereentwicklung und die Bedürfnisse der Studenten und Absolventen zu erhalten, sowohl individuell als auch in großem Umfang.

Handshake verpflichtet sich zum Schutz der Privatsphäre und wird niemals persönliche Daten an Dritte verkaufen oder sie ohne ausdrückliche Zustimmung für Marketing- oder Werbezwecke verwenden. Für unsere europäischen Kunden und Nutzer stellen wir sicher, dass persönliche Daten nur innerhalb der Grenzen der DSGVO verarbeitet werden.

Verantwortlicher für die Datenverarbeitung und Auftragsverarbeiter

Wenn Hochschulen personenbezogene Daten an Handshake übermitteln, fungiert die Hochschule als Datenverantwortlicher und Handshake als Auftragsverarbeiter, der im Einklang mit der Datenverarbeitungsvereinbarung und den Weisungen der Hochschule handelt. Die Universitäten haben die vollständige Kontrolle darüber, welche Studierendendaten sie an Handshake weitergeben. Eine Kopie unserer Standard-Datenverarbeitungsvereinbarung ist auf Anfrage erhältlich.

Für persönliche Daten, die studentische Nutzer Handshake zur Verfügung stellen, indem sie ihr Konto beantragen und den Handshake-Produkt Nutzungsbedingungen und der Datenschutzrichtlinie zustimmen, fungieren Handshake und die Universität beide als Datenverantwortliche, wie in unserer Datenschutzrichtlinie beschrieben.

Speicherort der Daten

Unsere europäische Plattform wird in der Google Cloud betrieben, die Datenspeicherung erfolgt in Deutschland. Wir bemühen uns, personenbezogene Daten, die über unsere Dienste erhoben werden,

innerhalb der EU oder des Vereinigten Königreichs zu speichern und zu verarbeiten, wann immer dies möglich ist.

Um einige unserer Dienstleistungen zu erbringen, arbeitet Handshake mit Drittanbietern zusammen, von denen eine kleine Anzahl Daten in den USA speichert. Einzelheiten zu allen Unterauftrags-Verarbeitern finden Sie hier.

Handshake ist vom Handelsministerium für die Einhaltung des EU-U.S. Data Privacy Framework zertifiziert. Diese Zertifizierung unterstreicht unser Engagement für die Einhaltung der höchsten Datenschutz- und Sicherheitsstandards und stellt sicher, dass die betroffenen Personen weiterhin einen Schutz erhalten, der dem EU-Datenschutzstandard entspricht.

Datenübertragungen

Um unsere Dienstleistungen zu erbringen, arbeitet Handshake mit Drittanbietern zusammen, mit denen wir Daten, einschließlich personenbezogener Daten, teilen können. Einzelheiten zu diesen Unterauftrags-Verarbeitern finden Sie hier.

Das Sicherheitsteam von Handshake prüft und genehmigt alle Drittanbieter, die an der Handshake-Plattform und den Anwendungen beteiligt sind, um sicherzustellen, dass sie Sicherheits- und Datenschutzstandards einhalten, die mindestens so streng sind wie die, die Handshake seinen Kunden zusagt.

Diese Anbieter sind an Vertraulichkeitsvereinbarungen gebunden, und wir unterhalten eine "Datenverarbeitungsvereinbarung" (DPA) für alle Drittanbieter Technologien, die innerhalb der Handshake-Plattform verwendet werden. Um DPAs anzufordern, wenden Sie sich bitte an das Datenschutzteam von Handshake unter privacy@joinhandshake.com.

Vorratsspeicherung von Daten

Die Daten werden so lange gespeichert, wie die Nutzer die Handshake-Plattform nutzen. Nachdem ein Nutzer die Plattform verlassen hat (Konto deaktiviert), werden seine Daten gelöscht, es sei denn, berechtigte Interessen oder andere (rechtliche) Gründe für die Speicherung stehen der Löschung entgegen.

Universitätspartner haben die Möglichkeit, mit Handshake zusammenzuarbeiten, um einen Prozess zur Löschung von Daten in Verbindung mit inaktiven Konten zu entwickeln, der auf ihren spezifischen Anforderungen basiert. Die Nutzer haben das Recht, jederzeit die Löschung ihrer Daten zu verlangen.

Löschung personenbezogener Daten von Studenten

Alle Nutzer haben das Recht, die dauerhafte Löschung ihrer Daten von der Plattform zu verlangen, und Handshake wird diesen Prozess in Übereinstimmung mit der DSGVO durchführen. Studierende haben auch die Möglichkeit, ihre Konten vorübergehend zu deaktivieren oder sie auf privat zu setzen. Es ist wichtig zu wissen, dass Handshake, wenn es eine Partnerschaft mit einer Universität eingeht, als Verarbeiter von Universitätsdaten agiert. In solchen Fällen kann es sein, dass Handshake die Daten der Studierenden aufbewahren muss, die die Universität an die Plattform weitergeleitet. Studierende, die ihr Konto deaktivieren oder löschen möchten, können dies per E-Mail an privacy@joinhandshake.com tun oder ihre Universität bitten, ihre Daten zu löschen.

Wenn ein Studierender ein doppeltes Konto hat oder die Löschung eines Kontos beantragt, haben die Universitäten die Möglichkeit, das Konto aus dem System zu entfernen. Einmal gelöscht, ist das Konto für das Handshake-Team unwiederbringlich. Um zu verhindern, dass das Konto neu erstellt wird, muss die Person, die den Abgleich der

Studierendendaten verwaltet, sicherstellen, dass das gelöschte Konto auch aus dem Abgleich der Studierendendaten entfernt wird.

Wenn der Studierende historische Daten mit dem Konto verknüpft hat, wie z. B. Termine, Bewerbungen, Erfahrungen oder Umfragen zum ersten Studienort, erlaubt das System der Universität nicht, den Studierenden zu löschen. In der Mitte des Bildschirms erscheint ein Pop-up-Fenster, das die Daten bestätigt, mit denen der Studierende in Handshake verbunden ist. In diesem Fall muss die Hochschule ein Ticket an den Handshake Support senden, um die Löschung zu bearbeiten.

Rechtmäßige Grundlage für die Verarbeitung

Handshake sammelt und verarbeitet personenbezogene Daten nur dann, wenn wir über eine rechtmäßige Grundlage verfügen. Zu den rechtmäßigen Grundlagen gehören die Einwilligung (wenn Personen ihre Zustimmung gegeben haben) und der Vertrag (wenn die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist).

Als bevorzugtes Karriere Managementsystem für Hochschulen unterstützt Handshake die Hochschulen bei der Bereitstellung einer Vielzahl von Dienstleistungen, von Beratungsterminen bis hin zu Karrieremessen und Veranstaltungen. Hochschulen, die mit Handshake zusammenarbeiten, haben die Möglichkeit, Studierendendaten, die ihnen mit Zustimmung der Studierenden übermittelt wurden, in Handshake zu importieren. Diese Daten können den Namen des Studierenden, seine E-Mail-Adresse, Kursinformationen usw. enthalten. Wenn Daten von einer Universität an Handshake übertragen werden, wird die Universität als Datenverantwortlicher benannt, und Handshake fungiert als Datenverarbeiter.

Handshake verarbeitet diese Studierendendaten ausschließlich für die

Zwecke, die in einer Datenverarbeitungsvereinbarung (DPA) zwischen Handshake und der Universität festgelegt sind.

In Bezug auf personenbezogene Daten, die von studentischen Nutzern zur Verfügung gestellt werden, die ihr Konto aktivieren, indem sie den Nutzungsbedingungen und der Datenschutzrichtlinie von Handshake zustimmen, fungieren sowohl Handshake als auch die Universität als Datenverantwortliche. Nachdem ein Studierender sein Handshake-Konto aktiviert hat, behält er die Möglichkeit, auf die Plattform zuzugreifen und sie zu nutzen, selbst wenn seine Universität ihre Partnerschaft mit Handshake beendet.

Gemäß den Grundsätzen der Rechtmäßigkeit, Transparenz und Fairness stellt Handshake sicher, dass die Zustimmung der Personen während des Einführungsprozesses der Studierenden zur Datenverarbeitung eingeholt wird.
In Übereinstimmung mit den Grundsätzen der Rechtmäßigkeit, Transparenz und Fairness holt Handshake die Zustimmung der Personen während des Anmeldeverfahrens für Studierenden zur Verarbeitung ihrer Daten ein.

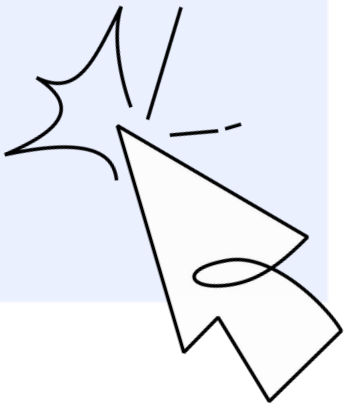
Datenschutzbeauftragter

Der Datenschutzbeauftragte von Handshake ist die Datenschutz Nord GmbH, die Sie per E-Mail an office@datenschutznord.de erreichen können.

Wie wir unsere Verpflichtung einhalten

Sicherheit

Bei Handshake ist Sicherheit ein Kernelement unserer Plattform, Infrastruktur, Prozesse und Teamkultur, um den Schutz der Daten unserer Partner und Nutzer zu gewährleisten. Der folgende Abschnitt bietet einen umfassenden Überblick über die Sicherheit bei Handshake.



Prüfung und Einhaltung der Vorschriften

Handshake ist nach SSAE 18 SOC 2 Typ II, TX RAMP und UK Cyber Essentials zertifiziert. Handshake erfüllt außerdem die Anforderungen von DSGVO, PCI SAQ-D und CCPA. Handshake arbeitet kontinuierlich mit Sicherheitsagenturen und Konsortien zusammen, um mit den Branchenstandards für Sicherheit und Datenschutz Schritt zu halten.

Sicherheit der Plattform

Zugangskontrollen

Rahmen für die Zugangskontrolle

Handshake setzt innerhalb seiner Plattform strenge Zugangskontrollen durch, indem es verschiedene Berechtigungsstufen für verschiedene Nutzergruppen (Career Services, Studierende, Arbeitgeber) eingerichtet, um die Dateizugriffsrechte effektiv zu verwalten.

Unsere Methode zur Einrichtung von Zugriffsrechten umfasst vordefinierte Rollen mit spezifischen Berechtigungen, die gängige Anwendungsfälle und Best Practices widerspiegeln. Dieser Ansatz vereinfacht den Prozess der Zugriffsrechtezuweisung für Administratoren, unabhängig davon, ob es sich um Karrieredienste, Arbeitgeber oder das Handshake-Team handelt. Er stellt sicher, dass Benutzer Rollen erhalten, die ihren Anforderungen entsprechen und dem Prinzip der geringsten Privilegien entsprechen. Vierteljährliche Überprüfungen des Benutzerzugriffs werden durchgeführt, um die Richtigkeit und Gültigkeit der Berechtigungen zu verifizieren.

Sicheres Single Sign-On (SSO)

Handshake unterstützt moderne SSO-Lösungen, die den sicheren und unkomplizierten Plattform-Zugang für Studierende von jeder vertrauenswürdigen Identität oder jedem Gerät aus ermöglichen. Unsere SSO-Funktionen umfassen unter anderem Protokolle wie SAML, SAML 2.0, Shibboleth, LDAP, CAS und TFA.

Bereitstellung und Provisionierung von Benutzer-Zugängen

Die Schnittstellen für Career Services und Arbeitgeber ermöglichen die Konfiguration von Benutzerrollen nach Bedarf. Der Zugang zu den Verwaltungsschnittstellen ist durch die Verwendung der Industriestandard-Protokolle HTTPS und TLS 1.3 gesichert. Handshake-Administratoren verwalten die Registrierung und Deregistrierung von Benutzern.

Produktionsinfrastruktur-Zugang

Handshake verfügt über robuste Kontrollmechanismen, die sicherstellen, dass der Zugang zur Produktionsinfrastruktur nach dem Prinzip der geringsten und rechtzeitigen Privilegien verwaltet und gesteuert wird. Der Zugang zu Änderungen an kritischen Infrastrukturen erfordert eine ausdrückliche Genehmigung und ist je nach Zweck zeitlich begrenzt. Alle Änderungen werden geprüft und auf verdächtige Aktivitäten überwacht. Darüber hinaus ist device trust

implementiert, um sicherzustellen, dass der Zugriff auf die Produktionsinfrastruktur ausschließlich von Handshake-verwalteten Geräten erfolgt.

Der Leiter des Infrastruktur-Teams überwacht die Zugriffsberechtigungen, während das Sicherheitsteam diese Zugriffe prüft.

IP-Beschränkungen

Der privilegierte Zugriff ist auf bestimmte Quell-IP-Adressen beschränkt, was die Sicherheitsmaßnahmen verbessert.

Moderation von Arbeitgebern und Inhalten

Validierung durch den Arbeitgeber

Als Teil des Vertrauens- und Sicherheitsprozesses von Handshake nutzt unser Vertrauens- und Sicherheitsteam Informationen von Sift und Googles Web Risk API, um neue Arbeitgeber-Konten manuell zu überprüfen und zu validieren, wenn sie erstellt werden. Falls erforderlich, fordern wir zusätzliche Unterlagen an, die mit dem Arbeitgeber in Verbindung stehen, einschließlich, aber nicht beschränkt auf:

- Beweise für das Unternehmen auf öffentlichen Plattformen
- Eine Empfehlung von einer bestehenden Handshake-Partnerinstitution

Kennzeichnung von Arbeitgebern

Handshake ermöglicht es Universitätspartnern und studentischen Nutzern im gesamten Netzwerk, verdächtige Aktivitäten oder Missbrauch in Bezug auf ein Unternehmen, einen Nutzer oder eine Stellenausschreibung direkt an unser Vertrauens- und Sicherheitsteam zu melden, wodurch ein starkes Team für die Zusammenarbeit entsteht.

Sobald eine Meldung eingereicht wurde, wird sie von unserem Vertrauens- und Sicherheitsteam geprüft. Wenn sich herausstellt, dass ein Unternehmen, ein Nutzer oder ein Job gegen unsere Nutzungsbedingungen verstößt, kann er gesperrt werden. Unser Team benachrichtigt den Nutzer, der die Meldung gemacht hat, sowie alle anderen betroffenen Nutzer. Falls ein Job, ein Benutzer oder ein Arbeitgeber gesperrt wird, sendet unser Team Benachrichtigungen in Handshake und per E-Mail an die betroffenen Institutionen.

Inhaltsmoderation, Spam-Filterung

Die Inhalte der Handshake-Plattform werden von unserem engagierten Vertrauens- und Sicherheits-Team moderiert, um die Integrität und Sicherheit der Interaktionen auf der Plattform zu gewährleisten.

Cloud-Sicherheit

Plattform-Hosting

Handshake nutzt die Google Cloud für das Hosting der Handshake-Anwendung, einschließlich Datenspeicherung, System-Backups, Server-Management und Cloud-Management-Tools. Google Cloud ist als führendes Unternehmen im Bereich der Datensicherheit anerkannt. Die Bemühungen von Google Cloud zur Gewährleistung des Datenschutzes können hier näher erläutert werden: Google Cloud-Sicherheit.

GCP-Zertifizierungen

Google Cloud Platform (GCP) wurde gründlich auf die Einhaltung von Industriestandards geprüft und verfügt unter anderem über die folgenden Zertifizierungen:

- ISO 9001:2015
- ISO 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO 22301:2019 & BS EN ISO 22301:2019
- ISO 50001:2018
- ISO/IEC 27110
- ISO/IEC 27701
- SOC1, SOC2, SOC3
- EU-Verhaltenskodex für die Cloud
- DSGVO

Handshake profitiert von diesen Zertifizierungen, indem es die zertifizierten Einrichtungen von GCP nutzt.

Architektur

Unsere Netzsicherheitsarchitektur umfasst mehrere Sicherheitszonen, wobei sensible Systeme wie Datenbankserver in hoch vertrauenswürdigen Zonen untergebracht sind, die nur vom internen Netz aus zugänglich sind. Der Verkehr zwischen den Zonen wird durch Firewalls geregelt.

Segregation in Netzen

Unsere Infrastruktur auf GCP nutzt verschiedene Netzwerksicherheitsfunktionen, um den Datenverkehr von außen zu isolieren und unbefugten Zugriff zu blockieren, darunter Virtual Private Cloud (VPC) und Sicherheitsgruppen (virtuelle Stateful Firewalls).

Netzwerküberwachung

Die Netzwerküberwachung in unserer GCP-Infrastruktur wird über unsere globale Infrastruktur-Überwachung verwaltet. Alle Protokolle werden zur Überwachung, Analyse und Alarmierung an einen zentralisierten Protokollierungsdienst gesendet.

Physische Begrenzungen und Standort

Die in GCP-Einrichtungen innerhalb der EU untergebrachten Rechenzentren sind diskret und verfügen über strenge Zugangskontrollen, darunter professionelles Sicherheitspersonal, Videoüberwachung, Einbruchserkennung und Multi-Faktor-Authentifizierung für den Zugang zum Rechenzentrum.

Physische Zugangskontrolle

Die GCP-Rechenzentren verfügen über robuste Sicherheitsmaßnahmen, einschließlich mehrstufiger Sicherheitszonen, 24/7-Sicherheit, CCTV, Multi-Faktor-Identifikation und Alarme bei Sicherheitsverletzungen.

GCP gewährt nur Mitarbeitenden und Vertragspartnern Zugang zum Rechenzentrum und zu Informationen, die einen legitimen geschäftlichen Bedarf für diese Berechtigungen haben. Wenn ein Mitarbeiter keine geschäftliche Notwendigkeit mehr für diese Berechtigungen hat, wird ihm der Zugang sofort entzogen, auch wenn er weiterhin ein Mitarbeitender von Google oder Google Cloud Platform ist. Jeder physische Zugang von GCP-Mitarbeitenden zu Rechenzentren wird protokolliert und routinemäßig überprüft.

Branderkennung und -unterdrückung

Die Rechenzentren sind so konzipiert, dass das Brandrisiko minimiert wird. Sie sind mit automatischen Branderkennungs- und -unterdrückungssystemen in allen Rechenzentrumsumgebungen, mechanischen und elektrischen Infrastrukturräumen, Kühlräumen und Generatoranlagenräumen ausgestattet. Der Schutz erfolgt entweder durch Nassrohr-, doppelt verriegelte Pre-Action- oder Gas-Sprinkleranlagen.

Strom

Die Stromversorgungssysteme des Rechenzentrums sind so konzipiert, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs 24 Stunden am Tag und sieben Tage die Woche gewartet werden können. Unterbrechungsfreie Stromversorgungseinheiten (USV) liefern im Falle eines Stromausfalls Notstrom für kritische und wichtige Verbraucher in der Einrichtung. Rechenzentren verwenden Generatoren, um die gesamte Einrichtung mit Strom zu versorgen.

Klima- und Temperaturkontrolle

Um optimale Bedingungen für die Hardware aufrechtzuerhalten, sind die Rechenzentren mit Klima-Kontrollsystemen ausgestattet, die Überhitzungs- und Service-Ausfälle verhindern.

Die Datenzentren sind so klimatisiert, dass die atmosphärischen Bedingungen auf einem optimalen Niveau gehalten werden. Personal und Systeme überwachen und steuern Temperatur und Luftfeuchtigkeit auf einem angemessenen Niveau.

Verwaltung

GCP überwacht elektrische, mechanische und lebenserhaltende Systeme und Geräte, so dass Probleme sofort erkannt werden. Es wird eine vorbeugende Wartung durchgeführt, um die Betriebsfähigkeit der Geräte aufrechtzuerhalten.

Außerbetriebnahme von Speichergeräten

GCP befolgt einen strengen Stilllegungs-Prozess für ausgediente Speichergeräte, um eine unbefugte Daten-Exposition zu verhindern, und hält sich dabei an die Richtlinien NIST 800-88 ("Guidelines for Media Sanitization").

Vernichtung von Datenspeichermedien

Die physische Vernichtung von Datenträgern wird von unserem Hosting-Provider GCP verwaltet, um eine sichere Datenentsorgung zu gewährleisten.

Datensicherheit

Daten im Transit

Handshake stellt sicher, dass alle übertragenen Daten mit modernen Verschlüsselungsprotokollen (HTTPS und TLS 1.3) verschlüsselt werden, die mit den besten Praktiken der Branche übereinstimmen. Diese Verschlüsselung sichert den Datenaustausch zwischen allen Nutzern der Plattform - Studierenden, Arbeitgebern, Career Services und Handshake-Mitarbeitenden. Handshake unterstützt nur TLS 1.2 und höher.

E-Mail-Signierung (DKIM/DMARC)

Handshake pflegt sichere E-Mail-Praktiken, die sicherstellen, dass E-Mails, die über die Plattform gesendet und empfangen werden, geschützt sind.

Daten im Ruhezustand

Innerhalb der Google Cloud Platform-Infrastruktur werden alle gespeicherten Daten, die nicht-öffentliche Informationen enthalten, mit dem branchenüblichen AES-256-Verschlüsselungsalgorithmus verschlüsselt, um einen zuverlässigen Datenschutz zu gewährleisten.

Datei Uploads

Handshake führt bei allen Datei-Uploads Virenschutz-Prüfungen durch, wobei der Zugriff auf hochgeladene Dateien nur autorisierten Benutzern vorbehalten ist, was die Datensicherheit erhöht.

Schutz vor Malware

Handshake setzt umfassende Anti-Malware-Maßnahmen ein, einschließlich Endpoint Protection durch Crowdstrike Falcon und Antiviren-Software, die alle Endgeräte schützen.

Sicherung

Unsere Backup-Strategie stellt sicher, dass die Daten der Handshake-Plattform an mehreren Standorten in Westeuropa repliziert werden, um die Ausfallsicherheit der Daten zu erhöhen. Die Produktions-Datenbanken werden täglich gesichert, wobei die Backups sieben Tage lang aufbewahrt und zur zusätzlichen Sicherheit auf der gesamten Festplatten-Ebene verschlüsselt werden.

Log-Verwaltung

Handshake verwendet Anwendungsserver-Protokolle, die alle Benutzeraktionen enthalten, die eine HTTPS-Anfrage an die Anwendung auslösen (z. B. das Laden einer Seite, das Absenden eines Formulars, das Auslösen von HTTPS-Anfragen im Hintergrund, usw.), sowie einige zugehörige Daten. In diesen Protokollen werden auch die Aktivitäten der administrativen Konten aufgezeichnet, wobei der Zugriff auf diese Protokolle streng auf bestimmte Mitglieder des technischen Teams beschränkt ist, um den Datenschutz und die Sicherheit zu gewährleisten.

Anwendungssicherheit

Veränderungsmanagement

Der Entwicklungszyklus von Handshake basiert auf dem Scrum-Framework, insbesondere auf Agile. Agile ist ein Projektmanagement-Ansatz, der Projekte in kurze, sich wiederholende Zyklen unterteilt, die "Sprints" genannt werden. Im Kern basiert Agile auf der Annahme, dass sich die Umstände während der Entwicklung eines Projekts ändern. Sie ändern sich weiter, während das Projekt Gestalt annimmt. Das Änderungsmanagement ist direkt in den Prozess integriert.

Scannen auf Schwachstellen

Eine automatisierte Web-Scanning-Anwendung wird auf der Handshake-Plattform in der Vorproduktionsphase eingesetzt. Sie sendet Warnmeldungen über gefundene Schwachstellen, bevor die Plattform bereitgestellt wird. Mit diesem Tool werden potenzielle Schwachstellen genauestens identifiziert, sodass unser Sicherheitsteam Prioritäten setzen und sie effizient beheben kann. Regelmäßige Scans werden vierteljährlich durchgeführt, um unseren Schutz aufrechtzuerhalten.

Statische Code-Analyse

Bei Handshake setzen wir auf einen automatisierten Ansatz, um die Qualität, Zuverlässigkeit und Sicherheit unseres Codes zu gewährleisten. Dieses System scannt unsere Codebasis akribisch und identifiziert alle Fehler, Schwachstellen oder verbesserungswürdige Bereiche, um sicherzustellen, dass unsere Software den höchsten Standards entspricht.

Penetrationstests

Wir arbeiten mit einem führenden externen Sicherheitsunternehmen zusammen, das mindestens einmal jährlich externe Penetrationstests für verschiedene Bereiche unserer Plattform und Anwendungen durchführt. Der gesamte Umfang unserer öffentlich zugänglichen Produkte wird mindestens einmal im Jahr getestet und überprüft.

Entwicklungsprozess

Handshake unterhält ein branchenführendes Programm für den sicheren Lebenszyklus der Softwareentwicklung. Jeder Code durchläuft einen gründlichen Überprüfungs- und Genehmigungsprozess, der eine Aufgabentrennung und Genehmigungen über den Änderungsmanagement-Prozess beinhaltet. Vor jedem Einsatz werden Code-Sicherheits- und Abhängigkeits-Prüfungen durchgeführt. Die Tests umfassen Überprüfungen auf die OWASP Top 10 Sicherheitsrisiken, einschließlich SQL Injections, Cross-Site Request Forgery, Sitzungs-Schwachstellen, Cross-Site Scripting, Dateizugriff, Authentifizierung und viele andere potenzielle Sicherheitsrisiken. Jede Änderung an der Handshake-Codebasis wird von einem qualifizierten Ingenieur begutachtet. Darüber hinaus ist der Zugang zum Quellcode stark eingeschränkt, und eine Versionskontrolle verfolgt alle Änderungen am Quellcode.

Umwelt Trennung

Wir sorgen für eine klare Abgrenzung zwischen unseren Entwicklungs-, Test- und Vorproduktionsumgebungen sowie unserer Live-Produktionsumgebung, indem wir Virtual Private Clouds verwenden. Diese Trennung garantiert, dass Produktionsdaten niemals in niedrigeren Umgebungen verwendet werden.

Sichere Entwicklungsumgebung

Handshake nutzt Github Enterprise als Plattform für die Code-Entwicklung, die ein angemessenes Maß an Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit gewährleistet.

Web-Frameworks Sicherheitskontrollen

Handshake verwendet moderne Web-Frameworks (z. B. React, Ruby on Rails) und führt kontinuierlich Sicherheitsbewertungen durch, um die Plattform zu untersuchen und auf bekannte Schwachstellen von Webanwendungen zu testen (z. B. OWASP Top 10). Dazu gehören inhärente Kontrollen, die u. a. die Anfälligkeit für Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) und SQL Injection (SQLi) verringern.

Technische Überprüfung von Anwendungen nach Plattformänderungen

Jede Quellcode-Änderung bei Handshake durchläuft einen strengen Überprüfungsprozess, der Folgendes beinhaltet:

- Peer Code Review
- Funktionsprüfung und/oder Nicht-Regressionstests
- Sicherheitsrelevante Änderungen werden gekennzeichnet und vom Sicherheitsteam überprüft, um zu gewährleisten, dass bewährte Sicherheitsverfahren in den Entwurf und die Entwicklung von Funktionen einbezogen werden.

Patch-Verwaltung

Die Patch-Verwaltung erfolgt im Rahmen unserer Infrastruktur-Upgrade-Richtlinie. Unser Ziel ist es, nie etwas patchen zu müssen, indem wir unsere Infrastruktursysteme stets auf dem neuesten Stand halten.

Beziehungen zu Dritten

Alle Drittanbieter, die für die Handshake-Plattform und -Anwendungen verwendet werden, wurden von Handshakes Sicherheitsteam überprüft und genehmigt. Alle Drittanbieter unterliegen Sicherheits- und Datenschutzkontrollen, die mindestens so streng sind wie die, die Handshake von seinen Kunden auferlegt werden. Alle Anbieter unterliegen Vertraulichkeitsvereinbarungen.

Geschäftskontinuitätsplan

Handshake verfügt über einen robusten Business Continuity Plan (BCP), der jährlich überprüft wird, um die Bereitschaft zu gewährleisten und auf Anfrage erhältlich ist.

Der Kontinuitätsplan von Handshake hängt von der durch GCP garantierten Verfügbarkeit ab: Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist "kalt". Im Falle eines Ausfalls wird der Datenverkehr der Kunden durch automatisierte Prozesse aus dem betroffenen Bereich umgeleitet. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass bei einem Ausfall eines Rechenzentrums genügend Kapazität vorhanden ist, um

den Datenverkehr automatisch auf die verbleibenden Standorte zu verlagern.

- RTO< 24 Stunden
- RPO< 6 Stunden

Implementierung der Kontinuität der Informationssicherheit

Kritische Komponenten der Infrastruktur, wie Webserver, Anwendungsserver und Datenspeicher, sind in Clustern zusammengefasst, und die Redundanz gewährleistet die Verfügbarkeit im Falle eines Systemausfalls. Unsere Backup-Politik garantiert, dass die Daten unserer Plattform an mehreren geografischen Standorten repliziert werden. Unsere replizierten Instanzen werden gemäß unseren Richtlinien eingerichtet und ihre Zuverlässigkeit wird durch GCP gewährleistet.

Wiederherstellung im Katastrophenfall

Der Infrastruktur-as-Code-Ansatz von Handshake ermöglicht eine schnellere Wiederherstellung im Falle einer größeren Katastrophe, die einen Neuaufbau der gesamten Infrastruktur erfordert.

Tests zur Wiederherstellung im Katastrophenfall

Die Konfiguration der gesamten Plattform und aller Anwendungen erfolgt in Skripten. Im Falle einer Katastrophe ist das technische Team in der Lage, die Plattform durch den Einsatz laufender Konfigurationsskripte wiederherzustellen. Die Datenbanken werden automatisch aus ihren Snapshots zu einem Zeitpunkt zwischen null und fünf Minuten ab dem Zeitpunkt der Katastrophe wiederhergestellt. Die Konfigurationen werden jeden Tag verwendet und ständig getestet.

Verfügbarkeit von Dienstleistungen

Handshake hat sich verpflichtet, eine außergewöhnliche Serviceverfügbarkeit aufrechtzuerhalten, die durch eine 99,9 %ige Betriebszeit Garantie, die in unserem SLA festgelegt ist, unterstützt wird. Unser engagiertes Technikerteam, das von automatisierten Überwachungssystemen unterstützt wird, die den Bereitschafts-Ingenieur bei Problemen vor Ort informiert, gewährleistet die Zuverlässigkeit unserer Plattform rund um die Uhr.

Für Echtzeit-Leistungsüberwachung und -aktualisierungen besuchen Sie bitte

https://status.joinhandshake.com/

Unternehmenssicherheit

Governance

Sicherheitspolitik für Informationssysteme (ISSP)

Handshake hat in Zusammenarbeit mit Sicherheitsmanagement-Spezialisten eine Sicherheitsrichtlinie für Informationssysteme ausgearbeitet, die mit branchenführenden Frameworks wie SSAE 18, NIST und ISO 27001 übereinstimmt. Handshake ist SOC 2 Typ 2 zertifiziert. Der jährliche Auditbericht kann auf Anfrage zur Verfügung gestellt werden.

Allgemeines Management-Engagement

Wir bei Handshake sind uns der überragenden Bedeutung unseres Informationssystems (IS) als Rückgrat unseres Betriebs und unserer Dienstleistungen bewusst. Die Sicherheit unseres IS ist nicht nur eine technische Notwendigkeit, sondern ein zentraler Bestandteil unserer Mission, unseren Benutzern, Kunden und Partnern mit unerschütterlicher Zuverlässigkeit und Vertrauen zu dienen. Wir sind dazu verpflichtet:

- Schutz der Vertraulichkeit und Integrität der Daten, die uns von unseren Nutzern, Kunden und Partnern anvertraut werden, mit besonderem Augenmerk auf personenbezogenen Daten.
- Sicherstellung der ununterbrochenen Verfügbarkeit unserer Dienste, einschließlich der Handshake-Plattform, der App, der Website und aller anderen von uns angebotenen Webanwendungen.

- Aufbau und Aufrechterhaltung eines starken Vertrauensverhältnisses zu unseren Partnern und Kunden durch Einhaltung unserer Datenschutz Verpflichtungen.
- Wahrung der Vertraulichkeit und Integrität der personenbezogenen Daten unserer Kunden und Partner.
- Beherrschen und Einhalten der rechtlichen und regulatorischen Rahmenbedingungen in Deutschland und weltweit, um die Einhaltung der Vorschriften zu gewährleisten und proaktiv auf sich ändernde Anforderungen zu reagieren.
- Aufrechterhaltung der Kontinuität des Betriebs von Handshake, um unsere Gemeinschaft effektiv zu unterstützen.

Um diese Ziele zu erreichen, ist die Geschäftsleitung von Handshake bestrebt, die notwendigen Mittel und Ressourcen bereitzustellen. Unser Engagement für die Sicherheit ist ein wesentlicher Bestandteil unserer Strategie, um sicherzustellen, dass Handshake eine vertrauenswürdige und sichere Plattform für alle unsere Interessengruppen bleibt.

Team

Verantwortung der Mitarbeitenden

Alle Angestellten stimmen den internen Richtlinien und der Tabelle zur Nutzung von Informationssystemen zu, einschließlich der Sicherheitsrichtlinien und verbindlichen Verfahren.

Kontrollen des Einstellungsprozesses

Fähigkeiten und Ausbildung werden bei allen Neueinstellungen während des Einstellungsprozesses kontrolliert. Bevor ein neuer Mitarbeitender zu Handshake kommt, überprüft unser Team die Ausbildung und frühere Beschäftigung der Person und führt interne und externe Referenz-Prüfungen durch. Wenn es das lokale Arbeitsrecht oder die gesetzlichen Bestimmungen erlauben, kann Handshake auch strafrechtliche Überprüfungen, Bonitätsprüfungen, Einwanderungsprüfungen und Sicherheitsüberprüfungen durchführen. Der Umfang dieser Hintergrundüberprüfungen hängt von der gewünschten Position ab.

Vertraulichkeitsvereinbarungen

Die Arbeitsverträge von Handshake enthalten eine Vertraulichkeits- und Geheimhaltungsklausel. Alle Mitarbeitende unterzeichnen eine Vertraulichkeitsvereinbarung.

Sensibilisierung und Schulung

Alle neuen Mitarbeitende müssen im Rahmen ihrer Einführungsschulung und danach jährlich an einer Schulung zum Thema Informationssicherheit und Datenschutz teilnehmen. Regelmäßige Sensibilisierungs- und Schulungsmaßnahmen werden mit allen Handshake-Mitarbeitenden geteilt und an sie gerichtet. Diese Maßnahmen decken ein breites Spektrum an Themen ab, zum

Beispiel:

- allgemeine bewährte Sicherheitsverfahren;
- Sicherheit am Arbeitsplatz;
- Verwaltung von sensiblen Informationen;
- Bewusstsein für Angriffsvektoren (Phishing, Malware, usw.)
- DSGVO

Sensibilisierung und Schulung des technischen Teams

Handshake fördert das Sicherheitsbewusstsein eines technischen Teams durch regelmäßige Kommunikation und Programme zur Sensibilisierung der Mitarbeitenden. Die Mitglieder des technischen Teams treffen sich monatlich, um bewährte Praktiken, Informationen und Ressourcen zu diskutieren und auszutauschen sowie Sicherheitsmaßnahmen zu identifizieren, die ergriffen werden müssen.

Sicherheitsartikel und Präsentationen werden regelmäßig im Team durch interne Kommunikationskanäle und regelmäßige Schulungen weitergegeben. Handshake führt derzeit Schulungen zu sicherem Code durch, die die OWASP Top 10 und andere gängige Angriffsvektoren abdecken.

Geräteüberwachung

Die Geräte der Mitarbeitenden werden über eine Lösung zur Verwaltung mobiler Geräte überwacht und verwaltet.

Verwaltung des internen Anwendungszugriffs

Neue Mitarbeitende erhalten Zugang zu internen Anwendungen auf einer Need-to-know-Basis. Der Zugang wird widerrufen, wenn der Mitarbeitende das Unternehmen verlässt. Alle Zugriffsanfragen werden durch Aufgabentrennung und Genehmigungen geregelt. Der Zugang zu allen sensiblen Anwendungen wird regelmäßig überprüft. Der gesamte Zugang unterliegt einer Mehrfaktor-Authentifizierung.

OKTA-Authentifizierung

Handshake verwendet eine rollenbasierte Sicherheitsarchitektur und verlangt, dass die Benutzer des Systems identifiziert und authentifiziert werden, bevor sie die Systemressourcen nutzen können. Die Ressourcen werden durch den Einsatz systemeigener Sicherheits- und Zusatzsoftwareprodukte geschützt, die Benutzer identifizieren und authentifizieren und Zugriffsanfragen anhand der autorisierten Rollen der Benutzer in den Zugriffskontrolllisten validieren.

Alle Ressourcen werden im Inventar-System verwaltet, und jeder Ressource wird ein Eigentümer zugewiesen. Die Eigentümer sind für die Genehmigung des Zugriffs auf die Ressource und für die regelmäßige Überprüfung des Zugriffs nach Rollen verantwortlich.

Mitarbeitende melden sich bei Cloud-Ressourcen mit Okta für Single Sign On (MFA/SSO) an. Darüber hinaus hat Handshake auf passwortlose Authentifizierung umgestellt, um

Passwortdiebstahl zu bekämpfen und Geräte Vertrauen zu erzwingen, um sicherzustellen, dass kritische Assets nur auf Unternehmensgeräten zugänglich sind.

Passwortsicherheit

Die Informationssicherheitspolitik von Handshake verlangt die Einhaltung der modernen NIST 800-53b Passwort Standards an den Stellen, an denen Passwörter erforderlich sind. Handshakes Einsatz von biometrischer Authentifizierung für den Zugang zu allen Unternehmensressourcen reduziert die Anzahl der Fälle, in denen Passwörter erforderlich sind, weiter.

Die Mitarbeitenden von Handshake erhalten eine Lösung zur Verwaltung von Passwörtern, um die Passwortsicherheit zu verbessern. Die Lösung ermöglicht die Erstellung komplexer Passwörter, schränkt die Wiederverwendung bestehender Passwörter ein und ermöglicht bei Bedarf die sichere Weitergabe von Passwörtern.

Vermögenswerte

Sicherheit am Arbeitsplatz

Alle Workstations sind auf Festplatten-Ebene verschlüsselt und werden durch eine branchenführende Malware-Schutzlösung und Endpunkt-Verwaltung geschützt.

Sicherheit der Räumlichkeiten

Die Einrichtungen von Handshake werden durch personalisierte Ausweise und Videoüberwachung durch CCTV geschützt. Die Bürotüren sind vor 7 Uhr morgens und nach 22 Uhr sowie an den Wochenenden verschlossen.

Netzwerksicherheit

Das interne Netz, das Handshake seinen Mitarbeitenden zur Verfügung stellt, wird durch eine Firewall-Lösung nach Industriestandard geschützt. Es wurden mehrere Netzwerkbereiche definiert, um die verschiedenen Rollen der Handshake-Mitarbeitenden und der vernetzten Geräte zu isolieren. Insbesondere Drucker und persönliche Geräte sind mit verschiedenen Netzwerk-Bereichen verbunden, die von den Arbeitsplätzen der Mitarbeitenden isoliert sind.

Wer trägt die Verantwortung dafür, dass wir unsere Verpflichtungen erfüllen?

Handshake ist stolz darauf, spezialisierte Teams und Führungskräfte zu haben, die sich dem Datenschutz und der Sicherheit widmen. Zu diesen Teams gehören erfahrene Ingenieure, Anwälte, die sich auf den Schutz der Privatsphäre der Nutzer spezialisiert haben, und Mitglieder der Geschäftsführung von Handshake.

Ihr ständiger Fokus liegt darauf, Handshake an der Spitze der Datensicherheit und des Datenschutzes in der Branche zu positionieren. Darüber hinaus engagieren sie sich für die Förderung einer Sicherheitskultur bei Handshake und stellen sicher, dass jedes Teammitglied unsere hohen Standards des Datenschutzes und der Privatsphäre der Nutzer versteht und dazu beiträgt.

Oliver Preeg
Rechtsberaterin für Datenschutz,
Handshake Europe

"Bei Handshake legen wir großen Wert darauf, Studierende, Hochschulen und Arbeitgeber weltweit zu unterstützen. Wir sind uns bewusst, dass jedes Land seine eigenen Datenschutzgesetze und -vorschriften hat, und verpflichten uns daher, die uns anvertrauten Informationen mit höchster Sorgfalt und Integrität zu schützen."

Handshake