DATENTRANSFER-FOLGENABSCHÄTZUNG

Datum der Überprüfung: 1. August 2025

Übersicht

Dieses Dokument enthält Informationen, die iSpring-Kunden bei der Durchführung von Datentransfer-Folgenabschätzungen im Zusammenhang mit der Nutzung von iSpring-Produkten und -Diensten „gemeinsam als ‚Produkte' bezeichnet" im Lichte des „Schrems II"-Urteils des Gerichtshofs der Europäischen Union und der Empfehlungen des Europäischen Datenschutzausschusses helfen sollen.

Dieses Dokument beschreibt insbesondere die für iSpring in den USA geltenden rechtlichen Regelungen, die Sicherheitsvorkehrungen, die iSpring im Zusammenhang mit der Übermittlung von persönlichen Daten von Kunden aus dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz („Europa") trifft, sowie die Fähigkeit von iSpring, ihren Verpflichtungen als „Datenimporteur„ gemäß den Standardvertragsklauseln („SCCs") nachzukommen.

Schritt 1: Kennen Sie Ihre Übermittlung

Wenn iSpring als Auftragsverarbeiter (im Auftrag unserer Kunden) persönliche Daten verarbeitet, die den europäischen Datenschutzgesetzen unterliegen, kommt iSpring ihren Verpflichtungen aus dem Auftragsverarbeitungsvertrag (im Folgenden DPA) nach.

Die DPA von iSpring umfasst die SCCs und enthält die folgenden Informationen:

- eine Beschreibung der Verarbeitung der persönlichen Kundendaten durch iSpring, und
- eine Beschreibung der Sicherheitsmaßnahmen von iSpring.

Informationen über die Art der Verarbeitungstätigkeiten von iSpring im Zusammenhang mit der Bereitstellung der Produkte, die Arten der von uns verarbeiteten und übertragenen persönlichen Kundendaten sowie die Kategorien der betroffenen Personen finden Sie in der DSGVO. Wir können persönliche Kundendaten überall dorthin übertragen, wo wir oder unsere Drittanbieter tätig sind, um die Produkte für Kunden bereitzustellen. Die Orte hängen von den jeweiligen iSpring-Produkten ab, die der Kunde nutzt, wie in der nachstehenden Tabelle dargestellt.

iSpring-Produkt	In welchen Ländern speichert iSpring persönliche Kundendaten?	In welchen Ländern verarbeitet iSpring persönliche Kundendaten (z. B. durch Zugriff, Übertragung oder anderweitige Bearbeitung)?
iSpring Learn LMS	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
iSpring Suite Max (einschließlich iSpring Cloud)	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
iSpring Cloud	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
iSpring Presenter	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
Free QuizMaker	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
iSpring Presenter Pro	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
iSpring QuizMaker	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
iSpring Cam Pro	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA
iSpring Free	Irland (Dublin) Deutschland (Frankfurt) Frankreich (Paris)	USA

Schritt 2: Identifizierung des Übermittlungsinstruments

Wenn persönliche Daten aus dem Europäischen Wirtschaftsraum an iSpring übermittelt werden, verlässt sich iSpring auf die SCCs der Europäischen Kommission, um einen angemessenen Schutz für die Übermittlung zu bieten. Wenn persönliche Kundendaten aus dem Europäischen Wirtschaftsraum von iSpring an Drittanbieter weitergegeben werden, schließt iSpring mit diesen Parteien SCCs ab.

Schritt 3: Identifizierung der anwendbaren Gesetze und Vorschriften im Hinblick auf die Übertragung

3.1 US-Überwachungsgesetze

3.2 FISA 702 und Executive Order 12333

Die folgenden US-Gesetze wurden vom Gerichtshof der Europäischen Union in der Rechtssache Schrems II als mögliche Hindernisse für die Gewährleistung eines im Wesentlichen gleichwertigen Schutzes persönlicher Daten in den USA identifiziert:

- FISA Section 702 („FISA 702“) – erlaubt es den US-Regierungsbehörden, die Offenlegung von Informationen über Nicht-US-Personen, die sich außerhalb der USA befinden, für die Zwecke der Informationsbeschaffung durch ausländische Geheimdienste zu erzwingen. Diese Informationsbeschaffung muss vom Foreign Intelligence Surveillance Court in Washington, DC, genehmigt werden. Anbieter, die unter FISA 702 fallen, sind Anbieter von elektronischen Kommunikationsdiensten („ECSP“) im Sinne von 50 U.S.C. § 1881(b)(4), zu denen auch Anbieter von Ferncomputerdiensten („RCSP“) gemäß der Definition in 18 U.S.C. § 2510 und 18 U.S.C. § 2711 gehören können.
- Executive Order 12333 („EO 12333“) – ermächtigt Geheimdienste (wie die US National Security Agency) zur Überwachung außerhalb der USA. Sie ermächtigt insbesondere die US-Nachrichtendienste, ausländische „Signals Intelligence“-Informationen zu sammeln, d. h. Informationen, die aus der Kommunikation und anderen Daten gewonnen werden, die über Funk, Draht und andere elektromagnetische Mittel übertragen werden oder zugänglich sind. Dazu kann auch der Zugriff auf Unterwasserkabel gehören, über die Internetdaten in die USA übertragen werden. EO 12333 stützt sich nicht auf die erzwungene Hilfe von Dienstanbietern, sondern scheint stattdessen auf die Ausnutzung von Schwachstellen in der Telekommunikationsinfrastruktur zu setzen.

Einzelheiten zur Umsetzung finden Sie im Dokument U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after Schrems II (https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF) [1]

3.3 US-CLOUD-Act

Der Clarifying Lawful Overseas Use of Data (CLOUD) Act änderte den Electronic Communications Privacy Act (ECPA) ab, das US-Gesetz, das regelt, wie Strafverfolgungsbehörden Informationen erhalten können, die sich im Besitz von bestimmten Technologieunternehmen, einschließlich Cloud-Service-Anbietern, befinden.

Der CLOUD Act besteht aus zwei Teilen. Der erste Teil stellt klar, dass Anordnungen, die unter dem bestehenden gesetzlichen Rahmen des ECPA erlassen werden, auf Daten zugreifen können, unabhängig davon, wo diese Daten gespeichert sind. Der zweite Teil schafft einen neuen Rahmen für Verträge zwischen Regierungen zur Regelung von grenzüberschreitenden Strafverfolgungsanfragen[2] .

Gelten FISA 702 und EO 12333 für iSpring?

iSpring könnte, wie die meisten SaaS-Unternehmen, technisch gesehen unter FISA 702 fallen. Allerdings verarbeitete iSpring keine persönlichen Daten, die für die US-Geheimdienste von Interesse sein könnten.

[1] In Bezug auf FISA 702 stellt das Whitepaper fest: „Für die meisten Unternehmen ist es unwahrscheinlich, dass die von Schrems II hervorgehobenen Bedenken hinsichtlich des Zugriffs der nationalen Sicherheit auf Unternehmensdaten aufkommen, da die Daten, die sie verarbeiten, für die US-Geheimdienste nicht von Interesse sind.“ Unternehmen, die „gewöhnliche Geschäftsdaten wie Mitarbeiter-, Kunden- oder Verkaufsdaten verarbeiten, haben keinen Grund zu der Annahme, dass die US-Geheimdienste versuchen würden, diese Daten zu sammeln.“ Es gibt Rechtsmittel für Einzelpersonen, auch für EU-Bürger, bei Verstößen gegen FISA Section 702 durch Maßnahmen, die vom Gericht in der Schrems-II-Entscheidung nicht angesprochen wurden, einschließlich FISA-Bestimmungen, die private Klagen auf Schadenersatz und Strafschadensersatz ermöglichen. Zu Executive Order 12333 heißt es in dem Whitepaper: „EO 12333 ermächtigt die US-Regierung nicht von sich aus, Unternehmen oder Personen zur Herausgabe von Daten zu verpflichten.“ Stattdessen muss sich EO 12333 auf ein Gesetz wie FISA 702 stützen, um Daten zu erheben. Die Sammlung von Massendaten, die Art der Datenerhebung, um die es in Schrems II ging, ist unter EO 12333 ausdrücklich verboten.

[2] Das Whitepaper stellt fest: Der CLOUD Act erlaubt den Zugriff der US-Regierung auf Daten im Rahmen von strafrechtlichen Ermittlungen nur dann, wenn eine richterliche Anordnung vorliegt, die von einem unabhängigen Gericht auf der Grundlage eines wahrscheinlichen Grundes für eine bestimmte Straftat genehmigt wurde. Der CLOUD Act erlaubt den Zugriff der US-Regierung auf Daten im Rahmen von Ermittlungen zur nationalen Sicherheit nicht und erlaubt keine Massenüberwachung.

Schritt 4: Identifizierung der technischen, vertraglichen und organisatorischen Maßnahmen, die zum Schutz der übertragenen Daten angewendet werden

4.1 Technische Maßnahmen

iSpring ist verpflichtet, angemessene technische und organisatorische Maßnahmen zum Schutz persönlicher Daten zu ergreifen (sowohl im Rahmen des Auftragsverarbeitungsvertrags als auch der SCCs, die wir mit Kunden und Dienstleistern abschließen). Technische Maßnahmen finden Sie im Anhang „iSpring-Webdienste: Überblick über die Sicherheitsprozesse“.

4.2 Vertragliche Maßnahmen

Die vertraglichen Maßnahmen sind in der DPA von iSpring enthalten. Die wichtigsten Anforderungen:

- Technische Maßnahmen: iSpring ist vertraglich verpflichtet, angemessene technische und organisatorische Maßnahmen zum Schutz persönlicher Daten zu ergreifen (sowohl im Rahmen des Auftragsverarbeitungsvertrags als auch in den SCCs, die wir mit Kunden, Dienstleistern und Lieferanten abschließen).

- Transparenz: iSpring ist gemäß den SCCs verpflichtet, ihre Kunden zu benachrichtigen, wenn eine staatliche Behörde ein staatliches Auskunftsersuchen zu persönlichen Daten von Kunden an sie richtet. Sollte es iSpring rechtlich untersagt sein, eine solche Offenlegung vorzunehmen, ist iSpring vertraglich verpflichtet, dieses Verbot anzufechten und eine Verzichtserklärung einzuholen.

- Aktionen zur Anfechtung des Zugangs: Gemäß den SCCs ist iSpring verpflichtet, die Rechtmäßigkeit von staatlichen Auskunftsersuchen zu überprüfen und solche Ersuchen anzufechten, wenn sie als widerrechtlich erachtet werden.

4.3 Organisatorische Maßnahmen

- Weitergabe: Wann immer wir Ihre Daten an mit iSpring verbundene Parteien weitergeben, sind wir Ihnen gegenüber für deren Nutzung verantwortlich. Wir verlangen von allen unseren Lieferanten und Anbietern, dass sie eine gründliche Due-Diligence-Prüfung durchlaufen.

- Datenschutz durch Design: Die Datenschutzrichtlinie von iSpring beschreibt den Ansatz von iSpring zum Datenschutz.

- Während der Verarbeitung der Daten bedienen wir uns der Hilfe von Unterauftragsverarbeitern. Eine Liste aller unserer Unterauftragsverarbeiter finden Sie unten:

Name	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten für den Fall, dass mehrere Unterauftragsverarbeiter zugelassen sind):	Adresse
1. SendGrid, Inc.	E-Mail-Dienste	889 Winslow St, Redwood City, CA 94063, USA
2. Amazon Web Dienste, Inc.	Rechenzentrum	410 Terry Avenue North, Seattle, WA 98109-5210
3. Ringcentral, Inc.	Kommunikationsdienste	20 Davis Dr, Belmont, CA 94002, USA
4. First Colo GmBH	Rechenzentrum	Kruppstraße 105, 60388 Frankfurt am Main, Deutschland
5. Avoxi, Inc.	Kommunikationsdienste	1000 Circle 75 Parkway, Suite 500, Atlanta GA 30339, USA
6. Telephonic Solutions OU	Kommunikationsdienste	Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 5, 10117, Estland
7. Liquid Web, LLC	Rechenzentrum	2703 Ena Dr. Lansing, MI 48917, US
8. Leaseweb USA, Inc.	Rechenzentrum	9301 Innovation Drive / Suite 100 Manassas, VA 20110
9. ActiveCampaign LLC	E-Mail-Dienste	1 N Dearborn St, 5. Etage, Chicago, IL 60602, USA

10. OpenAI, LLC	KI-gestützte Dienste	3180 18th Street, San Francisco, CA 94110, USA, 1. Etage, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
11. AssemblyAI, Inc.	KI-basierte Dienste	12 South Michigan Ave, Chicago, IL 60603, USA
12. Scaleway SAS	Reserve-Rechenzentrum EU	8 Rue de la Ville-l'Évêque, 75008 Paris, Frankreich
13. DigitalOcean, LLC	Reserve-Rechenzentrum USA	101 Avenue of the Americas, New York, NY 10013, USA
14. Amazon Web Services EMEA SARL	Rechenzentrum (Dublin, Ireland; Frankfurt, Germany)	Mr. Treublaan 7, Amsterdam, 1097DP, Netherlands

4.4 Zertifizierungen und Compliance

Bei iSpring steht der Schutz von Kunden- und Endbenutzerdaten an erster Stelle. Wir gewährleisten die Einhaltung globaler Datenschutzbestimmungen und setzen branchenführende Standards ein. Unser Sicherheitsansatz umfasst die Einhaltung international anerkannter Zertifizierungen, umfassender Richtlinien und robuster technischer Maßnahmen.

Zertifizierungen und Compliance-Rahmenwerke

- ISO 27001 Zertifizierung: iSpring erfüllt die Anforderungen der ISO 27001, einem weltweit anerkannten Standard für Informationssicherheitsmanagement. Diese Zertifizierung bestätigt unsere Fähigkeit, Informationswerte zu schützen, und unterstreicht unser Engagement für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten.
- ISO 27701 Zertifizierung: Als Erweiterung der ISO 27001 belegt diese Zertifizierung unsere Einhaltung der Anforderungen an Privacy Information Management Systeme (PIMS). Sie minimiert Risiken für die Privatsphäre von Einzelpersonen und gewährleistet umfassende Datenschutzkontrollen.

- Datenschutz-Grundverordnung (DSGVO/GDPR): iSpring stellt die Einhaltung der DSGVO sicher und wendet rechtmäßige Verarbeitung, Datenminimierung und Datenschutzprinzipien auf alle personenbezogenen Daten aus dem Europäischen Wirtschaftsraum (EWR), der Europäischen Union (EU), der Schweiz und dem Vereinigten Königreich an. Unsere Vereinbarung zur Auftragsverarbeitung (AVV) und die Standardvertragsklauseln (SCCs) erfüllen sämtliche Anforderungen gemäß Artikel 28(3) und 29(3) der DSGVO.

4.5 Datensicherheitsmaßnahmen

- Sichere Infrastruktur: iSpring setzt HTTPS-Verbindungen, Firewalls und Echtzeitüberwachung ein, um die Datenintegrität und Verfügbarkeit zu gewährleisten. Unsere Systeme nutzen mehrere Hosting-Anbieter, um Redundanz und bei Notfällen die Umleitung des Datenverkehrs sicherzustellen.
- Datensicherung und Wiederherstellung: iSpring verwendet fortschrittliche Backup-Technologien, um Datenverluste zu verhindern und Ausfallzeiten durch Hardwareprobleme zu minimieren.
- 24/7 Überwachung: Die kontinuierliche Überwachung der Systemleistung, einschließlich CPU-Auslastung, RAM-Nutzung und Festplattenspeicher, gewährleistet, dass unsere Dienste effizient und sicher bleiben.
- Penetrationstests: Regelmäßige interne und externe Sicherheitsprüfungen identifizieren Schwachstellen und verbessern unsere Sicherheitslage.

4.6 Zugriffssteuerung für Mitarbeiter

iSpring beschränkt den administrativen Zugriff auf Mitarbeiter, Auftragnehmer und Beauftragte mit nachgewiesenem geschäftlichem Bedarf. Hintergrundprüfungen und regelmäßige Überprüfungen stellen sicher, dass nur vertrauenswürdige Fachkräfte Zugang zu Kundendaten erhalten.

4.7 Transparenz und Kundensupport

Unsere Kunden können sich auf volle Transparenz hinsichtlich der Datenverarbeitungsaktivitäten verlassen. Detaillierte Dokumentationen und Zertifizierungen sind auf Anfrage verfügbar. Für weitere Informationen oder technischen Support wenden Sie sich bitte an den technischen Support oder unser Datenschutzteam unter privacy@ispring.com.

Schritt 5: Erforderliche Verfahrensschritte zur Umsetzung wirksamer zusätzlicher Maßnahmen

Unter Berücksichtigung der technischen, vertraglichen und organisatorischen Maßnahmen, die iSpring zum Schutz der persönlichen Daten ihrer Kunden ergriffen hat, ist iSpring der Ansicht, dass die Risiken, die mit der Übermittlung und Verarbeitung europäischer persönlicher Daten in die/den USA verbunden sind, unsere Fähigkeit nicht beeinträchtigen, unseren Verpflichtungen gemäß den SCCs (als „Datenimporteur“) nachzukommen oder sicherzustellen, dass die Rechte der Einzelpersonen geschützt bleiben.

Schritt 6: Neubewertung in angemessenen Abständen

iSpring wird die damit verbundenen Risiken und die Maßnahmen, die iSpring ergriffen hat, um den sich ändernden Datenschutzbestimmungen und Risiko Umgebungen im Zusammenhang mit der Übertragung persönlicher Daten außerhalb des Europäischen Wirtschaftsraums, des Vereinigten Königreichs und der Schweiz („Europa”) zu begegnen, überprüfen und gegebenenfalls überdenken.