DATA TRANSFER IMPACT ASSESSMENT

Overview

This document provides information to help iSpring customers conduct data transfer impact assessments in connection with their use of iSpring Products and Services (collectively-Products), in light of the “Schrems II” ruling of the Court of Justice for the European Union and the recommendations from the European Data Protection Board.

In particular, this document describes the legal regimes applicable to iSpring in the US, the safeguards iSpring puts in place in connection with transfers of customer personal data from the European Economic Area, the United Kingdom and Switzerland ("Europe"), and iSpring ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

Step 1: Know your transfer

Where iSpring processes personal data governed by European data protection Laws as a data processor (on behalf of our customers), iSpring complies with its obligations under its Data Processing Agreement (hereinafter-DPA).

iSpring’s DPA incorporates the SCCs and provides the following information:

- description of iSpring’s processing of customer personal data; and
- description of iSpring’s security measures;

Please refer to the DPA for information on the nature of iSpring's processing activities in connection with the provision of the Products, the types of customer personal data we process and transfer, and the categories of data subjects. We may transfer customer personal data wherever we or our third-party service providers operate for the purpose of providing the Products to Customers. The locations will depend on the particular iSpring Products which Customers use, as outlined in the chart below.

iSpring Product	**In what countries does iSpring store Customer Personal Data?**	**In what countries does iSpring process (e.g., access, transfer, or otherwise handle) Customer Personal Data?**
iSpring Learn LMS	Ireland (Dublin), Germany(Frankfurt) France (Paris)	USA

iSpring Product	In what countries does iSpring store Customer Personal Data?	In what countries does iSpring process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
iSpring Suite Max (including iSpring Cloud)	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA
iSpring Cloud	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA
iSpring Presenter	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA
Free Quiz Maker	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA
iSpring Presenter Pro	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA
iSpring Quiz Maker	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA
iSpring Cam Pro	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA
iSpring Free	Ireland(Dublin), Germany(Frankfurt) France (Paris)	USA

Step 2: Identification of Transfer tool.

Where personal data originating from European Economic Area is transferred to iSpring, iSpring relies upon the European Commission's SCCs to provide an appropriate safeguard for the transfer. Where customer personal data originating from European Economic Area is transferred by iSpring to third-party subprocessors, iSpring enters into SCCs with those parties.

Step 3: Identification of Applicable Laws and Regulations in light of transfer.

3.1 U.S. Surveillance Laws

3.2 FISA 702 and Executive Order 12333

The following US laws were identified by the Court of Justice of the European Union in Schrems II as being potential obstacles to ensuring essentially equivalent protection for personal data in the US:

- *FISA Section 702 ("FISA 702")* – allows US government authorities to compel disclosure of information about non-US persons located outside the US for the purposes of foreign intelligence information gathering. This information gathering must be approved by the Foreign Intelligence Surveillance Court in Washington, DC. In-scope providers subject FISA 702 are electronic communication service providers ("ECSP") within the meaning of 50 U.S.C. § 1881(b)(4), which can include remote computing service providers ("RCSP"), as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711.

- *Executive Order 12333 ("EO 12333")* - authorizes intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. In particular, it provides authority for US intelligence agencies to collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means. This may include accessing underwater cables carrying internet data in transit to the US. EO 12333 does not rely on the compelled assistance of service providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure.

For implementation details please check 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

The Clarifying Lawful Overseas Use of Data (CLOUD) Act amended the Electronic Communications Privacy Act (ECPA), which is the US statute governing how law enforcement agencies may obtain information held by certain technology companies, including cloud service providers.

[1] Regarding FISA 702 the White paper notes:For most companies, the concerns about national security access to company data highlighted by Schrems II are "unlikely to arise because the data they handle is of no interest to the U.S. intelligence community." Companies handling "ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data." There is individual redress, including for EU citizens, for violations of FISA section 702 through measures not addressed by the court in the Schrems II ruling, including FISA provisions allowing private actions for compensatory and punitive damages. Regarding Executive Order 12333 the whitepaper notes:EO 12333 does not on its own "authorize the U.S. government to require any company or person to disclose data." Instead, EO 12333 must rely on a statute, such as FISA 702 to collect data.Bulk data collection, the type of data collection at issue in Schrems II, is expressly prohibited under EO 12333.

The CLOUD Act has two parts. The first part clarifies that orders issued under the existing statutory framework in ECPA can reach data regardless of where that data is stored. The second part creates a new framework for government-to-government agreements to govern cross-border law enforcement requests[2].

Do FISA 702, EO 12333 apply to iSpring?

iSpring, like most SaaS companies, could technically be subject to FISA 702. However, iSpring does not process personal data that is likely to be of interest to US intelligence agencies.

Step 4: Identification of the technical, contractual and organizational measures applied to protect the transferred data

4.1 Technical measurers iSpring is obligated to have in place appropriate technical and organizational measures to safeguard personal data (both under the Data Processing Agreement as well as the SCCs we enter into with customers, service providers). For technical measurers please see attached the iSpring Web Services: Overview of Security Processes.

4.2 Contractual measurers

Contractual measures are incorporated into iSpring's DPA. Main requirements:

-Technical measures: iSpring is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data (both under the Data Processing Agreement as well as the SCCs we enter into with customers, service providers, and suppliers)

-Transparency: iSpring is obligated under the SCCs to notify its customers in the event it is made subject to a request for government access to customer personal data from a government authority. In the event that iSpring is legally prohibited from making such a disclosure, iSpring is contractually obligated to challenge such prohibition and seek a waiver.

-Actions to challenge access: Under the SCCs, iSpring is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

4.3 Organizational measurers

[2] The White paper notes: The CLOUD Act only permits U.S. government access to data in criminal investigations after obtaining a warrant approved by an independent court based on probable cause of a specific criminal act.The CLOUD Act does not allow U.S. government access in national security investigations, and it does not permit bulk surveillance

-Onward transfers: Whenever we share Your data with iSpring affiliated parties, we remain accountable to You for how it is used. We require all our suppliers and vendors to undergo a thorough due diligence process.

-Privacy by design: iSpring's Privacy Policy outlines iSpring approach to privacy

-While processing the data, we use the help of the subprocessors. A list of all of our data subprocessors is available below:

Name	Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Address
1. SendGrid, Inc.	Email services	889 Winslow St, Redwood City, CA 94063, USA
2. Amazon Web Services, Inc.	Data center	410 Terry Avenue North, Seattle, WA 98109-5210
3. Ringcentral, Inc	Communication services	20 Davis Dr, Belmont, CA 94002, USA
4. First Colo GmBH	Data center	Kruppstraße 105, 60388 Frankfurt am Main, Germany
5. Avoxi, Inc.	Communication services	1000 Circle 75 Parkway, Suite 500, Atlanta GA 30339, USA
6. Telephonic Solutions OU	Communication services	Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 5, 10117, Estonia
7. Liquid Web, LLC	Data center	2703 Ena Dr. Lansing, MI 48917, US
8. Leaseweb USA, Inc.	Data center	9301 Innovation Drive / Suite 100 Manassas, VA 20110
9. ActiveCampaign LLC	Email services	1 N Dearborn St, 5th Floor, Chicago, IL 60602, USA

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

4.4 Certifications and Compliance

At iSpring, we prioritize the protection of customer and end-user data, maintaining compliance with global data protection regulations and employing industry-leading standards. Our approach to security includes adherence to internationally recognized certifications, comprehensive policies, and robust technical measures.

Certifications and Compliance Frameworks

- **ISO 27001 Certification**: iSpring complies with ISO 27001, a globally recognized standard for information security management. This certification validates our ability to safeguard information assets and demonstrates our commitment to maintaining the confidentiality, integrity, and availability of customer data.
- **ISO 27701 Certification**: As an extension of ISO 27001, this certification establishes our compliance with Privacy Information Management System (PIMS) requirements, reducing risks to individuals' privacy rights and ensuring robust privacy controls.
- **General Data Protection Regulation (GDPR)**: iSpring ensures compliance with GDPR, applying lawful processing, data minimization, and data protection principles to all personal data originating from the European Economic Area (EEA), the European Union (EU), Switzerland, and the United Kingdom. Our Data Processing Agreement (DPA) and Standard Contractual Clauses (SCCs) address all requirements under GDPR Articles 28(3) and 29(3).

4.5 Data Security Practices

- **Secure Infrastructure**: iSpring employs HTTPS connections, firewalls, and real-time monitoring to ensure data integrity and availability. Our systems include multiple hosting providers to ensure redundancy and traffic rerouting in emergencies.
- **Data Backup and Recovery**: iSpring implements advanced backup technologies to prevent data loss and minimize service disruptions due to hardware issues.
- **24/7 Monitoring**: Continuous performance monitoring, including CPU load, RAM usage, and disk space, ensures our services remain efficient and secure.
- **Penetration Testing**: Regular internal and third-party security assessments identify vulnerabilities and enhance our security posture.

4.6 Employee Access Controls

iSpring restricts administrative access to employees, contractors, and agents with verified business needs. Background checks and periodic reviews ensure that only trustworthy professionals have access to customer data.

4.7 Transparency and Customer Support

Our customers can rely on full transparency regarding data processing activities. Detailed documentation and certifications are available upon request. For further information or technical assistance, contact tech support or our privacy team at privacy@ispring.com.

Step 5: Procedural steps necessary to implement effective supplementary measures

Taking into account technical, contractual, and organizational measures iSpring has implemented to protect customer personal data, iSpring considers that the risks involved in transferring and processing European personal data in/to the US do not impinge on our ability to comply with our obligations under the SCCs (as "data importer") or to ensure that individuals' rights remain protected.

Step 6: Re-evaluate at appropriate intervals

iSpring will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data outside of the European Economic Area, the United Kingdom and Switzerland ("Europe").