EVALUACIÓN DEL IMPACTO DE LA TRANSFERENCIA DE DATOS

Fecha de revisión: 1 de agosto de 2025

Resumen

El presente documento ofrece información para ayudar a los clientes de iSpring a realizar evaluaciones del impacto de la transferencia de datos en relación con el uso de los Productos y servicios de iSpring (denominados colectivamente «Productos»), a la luz de la sentencia «Schrems II», dictada por el Tribunal de Justicia de la Unión Europea y las recomendaciones del Comité Europeo de Protección de Datos.

En concreto, este documento describe los regímenes legales aplicables a iSpring en EE. UU., las garantías que iSpring implementa en relación con las transferencias de datos personales de clientes desde el Espacio Económico Europeo, el Reino Unido y Suiza («Europa»), así como la capacidad de iSpring para cumplir sus obligaciones como «importador de datos», en virtud de las Cláusulas Contractuales Tipo («CCT»).

Paso 1: Conocimiento de su transferencia.

Cuando iSpring procesa datos personales regidos por las leyes europeas de protección de datos como encargado del tratamiento (en nombre de nuestros clientes), la compañía cumple sus obligaciones en virtud de su Acuerdo de Tratamiento de Datos (en adelante, DPA).

El DPA de iSpring incorpora las CCT y proporciona la siguiente información:

- descripción del tratamiento de los datos personales de los clientes por parte de iSpring; y
- descripción de las medidas de seguridad de iSpring;

Rogamos que consulte el DPA para obtener información sobre la naturaleza de las actividades de tratamiento de iSpring en relación con la prestación de los Productos, los tipos de datos personales de los clientes que procesamos y transferimos, además de las categorías de interesados. Podemos transferir datos personales de los clientes a cualquier lugar donde nosotros o nuestros proveedores de servicios externos operen con el fin de proporcionar los Productos a los Clientes. Las ubicaciones dependerán de los Productos de iSpring que utilicen los Clientes, como se indica en la siguiente tabla.

Producto de iSpring	**¿En qué países almacena iSpring los datos personales de clientes?**	**¿En qué países trata iSpring los datos personales de cliente (p. ej., el acceso, la transferencia y otro tratamiento)?**
iSpring Learn LMS	Irlanda (Dublín) Alemania (Frankfurt)	EE. UU.

Producto de iSpring	¿En qué países almacena iSpring los datos personales de clientes?	¿En qué países trata iSpring los datos personales de cliente (p. ej., el acceso, la transferencia y otro tratamiento)?
	Francia (París)	
iSpring Suite Max (incluido iSpring Cloud)	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.
iSpring Cloud	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.
iSpring Presenter	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.
Free Quiz Maker	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.
iSpring Presenter Pro	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.
iSpring Quiz Maker	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.
iSpring Cam Pro	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.
iSpring Free	Irlanda (Dublín) Alemania (Frankfurt) Francia (París)	EE. UU.

Paso 2: Identificación de la herramienta de Transferencia.

Cuando se transfieren a iSpring datos personales procedentes del Espacio Económico Europeo, la compañía se basa en las CCT de la Comisión Europea para garantizar la protección adecuada de la transferencia. Cuando iSpring transfiere datos personales de clientes procedentes del Espacio Económico Europeo a subencargados del tratamiento de datos externos, iSpring suscribe CCT con dichas partes.

Paso 3: Identificación de leyes y regulaciones aplicables en vista de la transferencia.

3.1 Leyes de vigilancia de EE. UU.

3.2 FISA (Ley de Vigilancia de Inteligencia Extranjera) 702 y Resolución ejecutiva 12333

El Tribunal de Justicia de la Unión Europea en Schrems II identificó las siguientes leyes estadounidenses como obstáculos potenciales para garantizar una protección esencialmente equivalente de los datos personales en Estados Unidos:

- *Apartado 702 de FISA («FISA 702»):* permite a las autoridades del gobierno de EE.UU. obligar a la divulgación de información sobre personas no estadounidenses que se encuentren fuera de EE.UU. con el fin de recopilar información de inteligencia extranjera. Esta recopilación de información debe ser aprobada por el Tribunal de Vigilancia de Inteligencia Extranjera en Washington, D. C. Los proveedores incluidos y sujetos a la FISA 702 son proveedores de servicios de comunicaciones electrónicas («ECSP», por sus siglas en inglés), en el sentido del Título 50 del Código de los Estados Unidos, artículo 1881(b)(4), que puede incluir a los proveedores de servicios informáticos remotos («RCSP», por sus siglas en inglés), según se define en el Título 18 del Código de los Estados Unidos, artículos 2510 y 2711.

- *Resolución Ejecutiva 12333 («EO 12333»)*: autoriza a las agencias de inteligencia (como la Agencia de Seguridad Nacional de EE. UU.) a realizar vigilancia fuera de EE. UU. En particular, otorga autoridad a las agencias de inteligencia estadounidenses para recopilar información de «inteligencia de señales» extranjera, es decir, información obtenida de las comunicaciones y otros datos transmitidos o accesibles por radio, cable y otros medios electromagnéticos. Esto puede incluir el acceso a cables submarinos que transportan datos de Internet en tránsito hacia EE. UU. La EO 12333 no depende de la asistencia obligatoria de los proveedores de servicios, sino que parece depender de la explotación de vulnerabilidades en la infraestructura de telecomunicaciones.

Para conocer los detalles de implementación, consulte las Medidas de Protección de la Privacidad de EE. UU correspondientes a las CCT y otras bases legales de la UE para las transferencias de datos entre la UE y EE. UU. después de Schrems II (https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF)[1]

3.3 Ley Cloud de EE. UU.

[1] En relación con la FISA 702, el libro blanco señala: Para la mayoría de las empresas, las preocupaciones sobre el acceso a los datos empresariales por motivos de seguridad nacional, señaladas en Schrems II «es improbable que surjan porque los datos que manejan no interesan a la comunidad de inteligencia estadounidense». Las compañías que manejan «información comercial ordinaria, como registros de empleados, clientes o ventas, no tendrían fundamento para creer que las agencias de inteligencia estadounidenses intentarían recopilar dichos datos». Existe reparación individual, incluso para ciudadanos de la UE, por infracciones del artículo 702 de la FISA mediante medidas no contempladas por el tribunal en la sentencia Schrems II, incluidas las disposiciones de la FISA que permiten acciones privadas por daños compensatorios y punitivos. En cuanto a la Orden Ejecutiva 12333, el libro blanco señala: La Orden Ejecutiva 12333 por sí sola «no autoriza al gobierno de EE. UU. a exigir a ninguna empresa o persona a revelar datos». En su lugar, la EO 12333 debe basarse en una ley, como FISA 702, para recopilar datos. La recopilación masiva de datos, el tipo de recopilación de datos en cuestión en Schrems II, está expresamente prohibida por la EO 12333.

La Ley de Aclaración del Uso Legal de Datos en el Extranjero (CLOUD) modificó la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA), que es el estatuto estadounidense que rige cómo las agencias policiales pueden obtener información en poder de ciertas empresas de tecnología, incluidos los proveedores de servicios en la nube.

La Ley CLOUD consta de dos partes. La primera aclara que las resoluciones emitidas en virtud del marco legal vigente en la ECPA pueden acceder a los datos, independientemente de dónde se almacenen. La segunda crea un nuevo marco para los acuerdos intergubernamentales que rigen las solicitudes transfronterizas de las fuerzas del orden[2].

¿Se aplican Do FISA 702, EO 12333 a iSpring?

iSpring, como la mayoría de las empresas SaaS, podría estar sujeta técnicamente a FISA 702. Sin embargo, iSpring no trata datos personales que puedan ser de interés para las agencias de inteligencia estadounidenses.

Paso 4: Identificación de las medidas técnicas, contractuales y organizativas aplicadas para proteger los datos transferidos.

4.1 Medidas técnicas: iSpring está obligada a implementar medidas técnicas y organizativas adecuadas para proteger los datos personales (tanto en virtud del Acuerdo de Tratamiento de Datos como de las CCT que suscribe con clientes y proveedores de servicios). Para obtener información sobre las medidas técnicas, consulte el documento adjunto «Servicios Web de iSpring: Resumen de los procesos de seguridad».

4.2 Medidas contractuales

Las medidas contractuales se incorporan al DPA de iSpring. Requisitos principales:

- Medidas técnicas: iSpring está obligada contractualmente a contar con medidas técnicas y organizativas apropiadas para salvaguardar los datos personales (tanto en virtud del Acuerdo de Tratamiento de Datos como de las CCT, que suscribimos con clientes, proveedores de servicios y agentes).

-Transparencia: iSpring está obligada, en virtud de las CCT, a notificar a sus clientes en caso de que una autoridad gubernamental le solicite acceso a sus datos personales. En caso de que iSpring tenga prohibido legalmente realizar dicha divulgación, está obligada contractualmente a impugnar dicha prohibición y solicitar una exención.

- Acciones para impugnar el acceso: según las CCT, iSpring está obligada a revisar la legalidad de las solicitudes de acceso de las autoridades gubernamentales y a impugnar dichas solicitudes cuando se consideren ilegales.

4.3 Medidas organizativas

[2] El libro blanco señala: La Ley CLOUD solo permite al gobierno de EE. UU. acceder a los datos de investigaciones penales después de obtener una orden judicial aprobada por un tribunal independiente basada en la causa probable de un acto delictivo específico. La Ley CLOUD no permite el acceso del gobierno de EE. UU. en investigaciones de seguridad nacional ni la vigilancia masiva.

- Transferencias posteriores: Siempre que compartimos sus datos con afiliados de iSpring, somos responsables ante Usted de su uso. Exigimos a todos nuestros proveedores y vendedores que se sometan a un riguroso proceso de diligencia debida.

- Privacidad por diseño: la Política de privacidad de iSpring describe el enfoque de la compañía hacia la privacidad.

- Durante el tratamiento de datos, contamos con la ayuda de los subencargados del tratamiento. A continuación, encontrará una lista de todos nuestros subencargados del tratamiento de datos:

Nombre	Descripción del tratamiento (incluida una clara delimitación de responsabilidades en caso de que se autoricen varios subencargados del tratamiento):	Dirección
1. SendGrid, Inc.	Servicios de correo electrónico	889 Winslow St, Redwood City, California 94063, EE. UU.
2. Amazon Web Services, Inc.	Centro de datos	410 Terry Avenue North, Seattle, Washington 98109-5210
3. Ringcentral, Inc	Servicios de comunicación	20 Davis Dr, Belmont, California 94002, EE. UU.
4. First Colo GmBH	Centro de datos	Kruppstraße 105, 60388 Frankfurt am Main, Alemania
5. Avoxi, Inc.	Servicios de comunicación	1000 Circle 75 Parkway, Suite 500, Atlanta, Georgia 30339, EE. UU.
6. Telephonic Solutions OU	Communication services	Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 5, 10117, Estonia
7. Liquid Web, LLC	Centro de datos	2703 Ena Dr. Lansing, Míchigan 48917, EE. UU.
8. Leaseweb USA, Inc.	Centro de datos	9301 Innovation Drive / Suite 100 Manassas, Virginia 20110
9. ActiveCampaign LLC	Servicios de correo electrónico	1 N Dearborn St, 5th Floor, Chicago, Illinois 60602, EE. UU.
10. OpenAI, LLC	Servicios basados en IA	3180 18th Street, San Francisco, California 94110,

		EE. UU., 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublín 1, D01 YC43, UE
11. AssemblyAI, Inc.	Servicios basados en IA	12 South Michigan Ave, Chicago, Illinois 60603, EE. UU.
12. Scaleway SAS	Centro de datos de reserva de la UE	8 Rue de la Ville-l'Évêque, 75008 París, Francia
13. DigitalOcean, LLC	Centro de datos de reserva de EE. UU.	101 Avenue of the Americas, Nueva York, NY 10013, EE. UU.
14. Amazon Web Services EMEA SARL	Centro de datos (Dublin, Ireland; Frankfurt, Germany)	Mr. Treublaan 7, Amsterdam, 1097DP, Netherlands

4.4 Certificaciones y cumplimiento

En iSpring, priorizamos la protección de los datos de clientes y usuarios finales, cumpliendo con las normativas globales de protección de datos y aplicando estándares líderes en la industria. Nuestro enfoque en seguridad incluye el cumplimiento de certificaciones reconocidas internacionalmente, políticas integrales y sólidas medidas técnicas.

Certificaciones y marcos de cumplimiento

- Certificación ISO 27001: iSpring cumple con la ISO 27001, norma reconocida a nivel mundial para la gestión de la seguridad de la información. Esta certificación valida nuestra capacidad para proteger los activos de información y demuestra nuestro compromiso con la confidencialidad, integridad y disponibilidad de los datos de nuestros clientes.
- Certificación ISO 27701: Como una extensión de la norma ISO 27001, esta certificación establece nuestro cumplimiento con los requisitos del Sistema de Gestión de la Información de Privacidad (SGIP), reduciendo los riesgos a los derechos de privacidad de las personas y garantizando controles de privacidad sólidos.
- Reglamento General de Protección de Datos (RGPD): iSpring garantiza el cumplimiento del RGPD, aplicando los principios de tratamiento lícito, minimización de datos y protección de datos a todos los datos personales procedentes del Espacio Económico Europeo (EEE), la Unión Europea (UE), Suiza y el Reino Unido. Nuestro Acuerdo de Tratamiento de Datos (ADT) y nuestras Cláusulas Contractuales Tipo (CCT) cumplen todos los requisitos de los artículos 28(3) y 29(3) del RGPD.

4.5 Prácticas de seguridad de datos

- Infraestructura segura: iSpring utiliza conexiones HTTPS, cortafuegos y monitorización en tiempo real para garantizar la integridad y disponibilidad de los datos. Nuestros sistemas incluyen múltiples proveedores de alojamiento para garantizar la redundancia y el redireccionamiento del tráfico en caso de emergencia.

- Copia de seguridad y recuperación de datos: iSpring implementa tecnologías de copia de seguridad avanzadas para evitar la pérdida de datos y minimizar las interrupciones del servicio debido a problemas de hardware.
- Supervisión 24/7: la supervisión continua del rendimiento, incluida la carga de la CPU, el uso de RAM y el espacio en disco, garantiza que nuestros servicios se mantengan eficientes y seguros.
- Pruebas de penetración: las evaluaciones de seguridad periódicas internas y de terceros identifican vulnerabilidades y mejoran nuestra postura de seguridad.

4.6 Controles de acceso de empleados

iSpring restringe el acceso administrativo a empleados, contratistas y agentes con necesidades comerciales verificadas. Las verificaciones de antecedentes y las revisiones periódicas garantizan que solo profesionales de confianza tengan acceso a los datos de los clientes.

4.7 Transparencia y atención al cliente

Nuestros clientes pueden confiar en la total transparencia en las actividades de tratamiento de datos. Disponemos de documentación detallada y certificaciones previa solicitud. Para obtener más información o asistencia técnica, contacte con el soporte técnico o con nuestro equipo de privacidad en privacy@ispring.com**.**

Paso 5: Pasos procesales necesarios para implementar medidas complementarias efectivas.

Teniendo en cuenta las medidas técnicas, contractuales y organizativas que iSpring ha implementado para proteger los datos personales de los clientes, la compañía considera que los riesgos involucrados en la transferencia y el procesamiento de datos personales europeos hacia/en EE. UU. no afectan nuestra capacidad de cumplir con nuestras obligaciones bajo las CCT (como «importador de datos») ni de garantizar la protección de los derechos de las personas.

Paso 6: Reevaluación en intervalos apropiados.

iSpring revisará y, de ser necesario, reconsiderará los riesgos involucrados y las medidas que ha implementado para abordar las normativas cambiantes en materia de privacidad de datos y los entornos de riesgo asociados con las transferencias de datos personales fuera del Espacio Económico Europeo, del Reino Unido y de Suiza («Europa»).