ÉVALUATION DE L'IMPACT DU TRANSFERT DES DONNÉES

Date de révision : 1er août 2025

Résumé

Le présent document fournit des informations destinées à aider les clients d'iSpring à réaliser des évaluations de l'impact du transfert des données dans le cadre de leur utilisation des Produits et Services iSpring, “collectivement désignés sous le nom de ‘produits’”, compte tenu de l'arrêt “Schrems II” de la Cour de justice de l'Union européenne et des recommandations du Conseil européen de la protection des données.

Ce document décrit notamment les régimes juridiques applicables à iSpring aux États-Unis, les garanties mises en place par iSpring dans le cadre des transferts de données personnelles de clients depuis l'Espace économique européen, le Royaume-Uni et la Suisse (“Europe”), ainsi que la capacité d'iSpring à respecter ses obligations en tant qu'”importateur de données” en vertu des Clauses contractuelles types (“CCT”).

Étape 1 : Connaître votre transfert

Lorsque iSpring traite des données personnelles régies par les lois européennes sur la protection des données en tant que sous-traitant (pour le compte de nos clients), iSpring se conforme aux obligations qui lui incombent en vertu de son Accord de traitement des données (ci-après ATD).

L'ATD d'iSpring intègre les CCT et fournit les informations suivantes :

- description du traitement des données personnelles des clients par iSpring ; et
- description des mesures de sécurité d'iSpring ;

Veuillez consulter l'ATD pour obtenir des informations sur la nature des activités de traitement d'iSpring dans le cadre de la fourniture des Produits, les types de données personnelles des clients que nous traitons et transférons, et les catégories de personnes concernées. Nous pouvons transférer les données personnelles des clients partout où nous ou nos prestataires de services tiers opèrent dans le but de fournir les Produits aux Clients. Les lieux dépendront des Produits iSpring particuliers que les Clients utilisent, comme indiqué dans le tableau ci-dessous.

Produit iSpring	Dans quels pays iSpring stocke-t-il les données personnelles des clients ?	Dans quels pays iSpring procède-t-il au traitement (par exemple, accès, transfert ou autre traitement) des données personnelles des clients ?
iSpring Learn LMS	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
iSpring Suite Max (y compris iSpring Cloud)	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
iSpring Cloud	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
iSpring Presenter	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
Free Quiz Maker	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
iSpring Presenter Pro	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
iSpring Quiz Maker	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
iSpring Cam Pro	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis
iSpring Free	Irlande (Dublin) Allemagne (Francfort) France (Paris)	Etats-Unis

Étape 2 : Identification de l'outil de transfert

Lorsque des données personnelles provenant de l'Espace économique européen sont transférées à iSpring, iSpring s'appuie sur les CCT de la Commission européenne pour fournir une protection appropriée au transfert. Lorsque les données personnelles des clients provenant de l'Espace économique européen sont transférées par iSpring à des sous-traitants tiers, iSpring conclut des CCT avec ces parties.

Étape 3 : Identification des lois et règlements applicables compte tenu du transfert

3.1 Lois américaines sur la surveillance

3.2 FISA 702 et Executive Order 12333

Les lois américaines suivantes ont été identifiées par la Cour de justice de l'Union européenne dans l'affaire Schrems II comme étant des obstacles potentiels à la garantie d'une protection essentiellement équivalente des données personnelles aux États-Unis :

- *FISA Section 702 ("FISA 702")* - permet aux autorités gouvernementales américaines d'obliger la divulgation d'informations sur des personnes non américaines situées en dehors des États-Unis à des fins de collecte d'informations de renseignement étranger. Cette collecte d'informations doit être approuvée par le Foreign Intelligence Surveillance Court à Washington, DC. Les fournisseurs dans le champ d'application de la FISA 702 sont les fournisseurs de services de communication électronique ("FSCE") au sens de 50 U.S.C. § 1881(b)(4), qui peuvent inclure les fournisseurs de services informatiques à distance ("FSID"), tels que définis dans 18 U.S.C. § 2510 et 18 U.S.C. § 2711.
- *Executive Order 12333 ("EO 12333")* - autorise les agences de renseignement (comme la US National Security Agency) à mener des activités de surveillance en dehors des États-Unis. En particulier, il autorise les agences de renseignement américaines à collecter des informations étrangères de "renseignements d'origine électromagnétique", c'est-à-dire des informations recueillies à partir de communications et d'autres données transmises ou accessibles par radio, câble et autres moyens électromagnétiques. Cela peut inclure l'accès aux câbles sous-marins transportant des données Internet en transit vers les États-Unis. L'EO 12333 ne compte pas sur l'assistance contrainte des fournisseurs de services, mais semble plutôt s'appuyer sur l'exploitation des vulnérabilités de l'infrastructure des télécommunications.

Pour les détails de la mise en œuvre, veuillez consulter 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 Loi américaine sur le Cloud

La loi CLOUD (Clarifying Lawful Overseas Use of Data (Clarification de l'utilisation licite des données à l'étranger)) a modifié la loi ECPA (Electronic Communications Privacy Act), qui est la loi américaine régissant la manière dont les organismes chargés de l'application de la loi peuvent obtenir des informations détenues par certaines entreprises technologiques, y compris les fournisseurs de services en cloud.

La loi CLOUD comporte deux parties. La première partie clarifie le fait que les ordonnances émises en vertu du cadre légal existant dans l'ECPA peuvent atteindre les données, quel que soit l'endroit où elles sont stockées. La deuxième partie crée un nouveau cadre pour les accords de gouvernement à gouvernement afin de régir les demandes transfrontalières d'application de la loi[2].

FISA 702, EO 12333 s'appliquent-ils à iSpring ?

iSpring, comme la plupart des entreprises SaaS, pourrait techniquement être soumise à la norme FISA 702. Toutefois, iSpring ne traite pas de données personnelles susceptibles d'intéresser les agences de renseignement américaines.

---

[1] En ce qui concerne FISA 702, le White Paper note : Pour la plupart des entreprises, les préoccupations concernant l'accès de la sécurité nationale aux données de l'entreprise mises en évidence par Schrems II sont "peu susceptibles de survenir parce que les données qu'elles traitent ne présentent aucun intérêt pour la communauté du renseignement américain". Les entreprises qui traitent "des informations commerciales ordinaires comme les dossiers des employés, des clients ou des ventes, n'ont aucune raison de croire que les agences de renseignement américaines cherchent à collecter ces données." Il existe un recours individuel, y compris pour les citoyens de l'UE, pour les violations de la section 702 de la FISA par le biais de mesures non abordées par la cour dans l'arrêt Schrems II, y compris les dispositions de la FISA permettant des actions privées pour des dommages compensatoires et punitifs. En ce qui concerne l'Executive Order 12333, le white paper note : EO 12333 n'autorise pas à lui seul "le gouvernement américain à obliger toute entreprise ou personne à divulguer des données." Au lieu de cela, l'EO 12333 doit s'appuyer sur une loi, telle que FISA 702 pour collecter des données. La collecte de données en masse, le type de collecte de données en question dans Schrems II, est expressément interdite par l'EO 12333.

[2] Le White paper note : La loi CLOUD n'autorise l'accès du gouvernement américain aux données dans le cadre d'enquêtes criminelles qu'après l'obtention d'un mandat approuvé par un tribunal indépendant sur la base d'une cause probable d'un acte criminel spécifique.La loi CLOUD n'autorise pas l'accès du gouvernement américain dans le cadre d'enquêtes de sécurité nationale, et elle n'autorise pas la surveillance en masse

Étape 4 : Identification des mesures techniques, contractuelles et organisationnelles appliquées pour protéger les données transférées

4.1 Mesures techniques.

iSpring est tenu de mettre en place des mesures techniques et organisationnelles appropriées pour sauvegarder les données personnelles (à la fois en vertu du Contrat de traitement des données et des CCT que nous concluons avec nos clients et fournisseurs de services). Pour les mesures techniques, veuillez voir en annexe les Services Web iSpring : Aperçu des processus de sécurité.

4.2 Mesures contractuelles

Les mesures contractuelles sont intégrées dans l'ATD d'iSpring. Principales exigences :

-Mesures techniques : iSpring est contractuellement tenu de mettre en place des mesures techniques et organisationnelles appropriées pour sauvegarder les données personnelles (à la fois dans le cadre du contrat de traitement des données ainsi que des CCT que nous concluons avec les clients, les prestataires de services et les fournisseurs).

-Transparence : iSpring est tenu, en vertu des CCT, d'informer ses clients dans le cas où il ferait l'objet d'une demande d'accès aux données personnelles d'un client de la part d'une autorité gouvernementale. Dans le cas où iSpring est légalement interdit de procéder à une telle divulgation, iSpring est contractuellement obligé de contester cette interdiction et de demander une dérogation.

-Actions pour contester l'accès : En vertu des CCT, iSpring est tenu d'examiner la légalité des demandes d'accès des autorités gouvernementales et de contester ces demandes lorsqu'elles sont considérées comme illégales.

4.3 Mesures organisationnelles

-Transferts vers l'extérieur : Chaque fois que nous partageons vos données avec des parties affiliées à iSpring, nous restons responsables devant Vous de la manière dont elles sont utilisées. Nous obligeons tous nos fournisseurs et revendeurs à se soumettre à un processus de diligence raisonnable approfondi.

-La politique de confidentialité d'iSpring décrit l'approche d'iSpring en matière de confidentialité.

-Lorsque nous traitons les données, nous utilisons l'aide des sous-traitants. Une liste de tous nos sous-traitants de données est disponible ci-dessous :

Nom	Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants secondaires sont autorisés) :	Adresse
1. SendGrid, Inc.	Services email	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	Services de communication	20 Davis Dr, Belmont, CA 94002, USA
4. First Colo GmBH	Data Center	Kruppstraße 105, 60388 Frankfurt am Main, Allemagne
5. Avoxi, Inc.	Services de communication	1000 Circle 75 Parkway, Suite 500, Atlanta GA 30339, USA
6. Telephonic Solutions OU	Services de communication	Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 5, 10117, Estonie
7. Liquid Web, LLC	Data Center	2703 Ena Dr. Lansing, MI 48917, USA
8. Leaseweb USA, Inc.	Data Center	9301 Innovation Drive / Suite 100 Manassas, VA 20110
9. ActiveCampaign LLC	Services d’e-mail	1 N Dearborn St, 5th Floor, Chicago, IL 60602, États-Unis
10. OpenAI, LLC	Services basés sur l’IA	3180 18th Street, San Francisco, CA 94110, États-Unis,

		1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irlande
11. AssemblyAI, Inc.	Services basés sur l'IA	12 South Michigan Ave, Chicago, IL 60603, États-Unis
12. Scaleway SAS	Centre de données de réserve UE	8 Rue de la Ville-l'Évêque, 75008 Paris, France
13. DigitalOcean, LLC	Centre de données de réserve États-Unis	101 Avenue of the Americas, New York, NY 10013, États-Unis
14. Amazon Web Services EMEA SARL	Data Centre (Dublin, Ireland; Frankfurt, Germany)	Mr. Treublaan 7, Amsterdam, 1097DP, Netherlands

4.4 Certifications et conformité

Chez iSpring, nous donnons la priorité à la protection des données des clients et des utilisateurs finaux en maintenant la conformité avec les réglementations mondiales en matière de protection des données et en employant des normes à la pointe de l'industrie. Notre approche de la sécurité comprend l'adhésion à des certifications internationalement reconnues, des politiques exhaustives et des mesures techniques robustes.

Certifications et cadres de conformité

- Certification ISO 27001: iSpring est conforme à la norme ISO 27001, une norme mondialement reconnue pour la gestion de la sécurité de l'information. Cette certification valide notre capacité à protéger les actifs informationnels et démontre notre engagement à maintenir la confidentialité, l'intégrité et la disponibilité des données de nos clients.

- Certification ISO 27701: En tant qu'extension de la norme ISO 27001, cette certification établit notre conformité aux exigences du Système de gestion des données personnelles (PIMS), réduisant les risques pour les droits à la vie privée des individus et garantissant des contrôles robustes de la vie privée.

- Règlement général sur la protection des données (RGPD) : iSpring assure sa conformité au RGPD, en appliquant les principes de traitement licite, de minimisation des données et de protection des données à tous les renseignements personnels provenant de l'Espace économique européen (EEE), de l'Union européenne (UE), de la Suisse et du Royaume-Uni. Notre accord de traitement des données (ATD) et nos clauses contractuelles types répondent à toutes les exigences des articles 28(3) et 29(3) du RGPD.

4.5 Pratiques en matière de sécurité des données

- Infrastructure sécurisée: iSpring utilise des connexions HTTPS, des pare-feu et une surveillance en temps réel pour garantir l'intégrité et la disponibilité des données. Nos systèmes incluent plusieurs fournisseurs d'hébergement afin de garantir la redondance et le réacheminement du trafic en cas d'urgence.

- Sauvegarde et récupération des données : iSpring met en œuvre des technologies de sauvegarde avancées afin de prévenir la perte de données et de minimiser les interruptions de service dues à des problèmes matériels.

- Surveillance 24h/24 7j/7: Une surveillance continue des performances, notamment de la charge du processeur, de l'utilisation de la mémoire vive et de l'espace disque, garantit l'efficacité et la sécurité de nos services.

- Tests d'intrusion: Des évaluations régulières de la sécurité en interne et par des tiers permettent d'identifier les vulnérabilités et d'améliorer notre posture en matière de sécurité.

4.6 Contrôles d'accès des employés

iSpring limite l'accès administratif aux employés, aux sous-traitants et aux agents dont les besoins professionnels ont été validés. Des vérifications des antécédents et des vérifications périodiques garantissent que seuls des professionnels dignes de confiance ont accès aux données des clients.

4.7 Transparence et assistance à la clientèle

Nos clients peuvent compter sur une transparence totale concernant les activités de traitement des données. Une documentation détaillée et des certifications sont disponibles sur demande. Pour de plus amples informations ou une assistance

technique, contactez le support technique ou notre équipe chargée de la protection de la vie privée à l'adresse privacy@ispring.com.

Étape 5 : Étapes procédurales nécessaires à la mise en œuvre de mesures supplémentaires efficaces

Compte tenu des mesures techniques, contractuelles et organisationnelles qu'iSpring a mises en œuvre pour protéger les données personnelles des clients, iSpring considère que les risques liés au transfert et au traitement des données personnelles européennes aux/vers les États-Unis n'empiètent pas sur notre capacité à respecter nos obligations en vertu des CCT (en tant que “importateur de données”) ou à garantir que les droits des personnes restent protégés.

Étape 6 : Réévaluation à intervalles appropriés

iSpring examinera et, si nécessaire, reconsidérera les risques encourus et les mesures qu'elle a mises en œuvre pour faire face à l'évolution des réglementations sur la confidentialité des données et des environnements à risque associés aux transferts de données personnelles en dehors de l'Espace économique européen, du Royaume-Uni et de la Suisse (“Europe”).