_swissprivacy.law

Swiss-US Data Privacy Framework : un premier pas vers une approche plus pragmatique ?

Katharina Martin et Philipp Fischer, le 17 janvier 2025

L'entrée en force du Swiss-U.S. DPF a offert un cadre juridique plus solide aux entreprises et organismes publics suisses utilisant des services cloud américains. Les auteurs de cette contribution argumentent qu'au-delà des cas de transferts « directs » de données personnelles à des entreprises américaines certifiées (soit le scénario expressément visé par le Swiss-U.S. DPF), la reconnaissance de ce mécanisme a une portée plus large et assure une sécurité juridique dans d'autres situations.

Durant ces 15 dernières années (i.e., depuis l'adoption du premier US-Swiss Safe Harbor Framework en 2008), peu de sujets ont fait couler autant d'encre dans le domaine de la protection des données que les transferts de données personnelles. Est-ce que l'entrée en force du Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) le 15 septembre 2024 met un terme à toutes les controverses ? L'avenir le dira. Cela étant dit, cette reconnaissance devrait, selon nous, apporter un éclairage nouveau sur la compatibilité du US CLOUD Act avec le droit suisse.

A. Le US CLOUD Act : une source de préoccupations

Dès son adoption en 2018, le US CLOUD Act a suscité de vives inquiétudes au sein de l'Union européenne et en Suisse. En effet, cette loi a modifié le Stored Communications Act (pour faciliter la lisibilité, nous utiliserons le terme US CLOUD Act dans cette contribution) afin de permettre aux autorités américaines d'accéder, à certaines conditions, à des données personnelles qui sont « sous le contrôle » de groupes américains, même si ces données sont stockées par des filiales de ces groupes se trouvant à l'étranger (pour une présentation du US CLOUD Act, cf. www.swissprivacy.law/101).

Certaines autorités de protection des données (dans l'Union européenne), de même que des experts, ont pris la position que les droits d'accès qui figurent dans le US CLOUD Act en faveur des autorités américaines seraient contraires à l'ordre public européen, respectivement suisse, créant ainsi une incertitude juridique pour toutes les entreprises privées et administrations publiques qui utilisent des infrastructures reposant sur la technologie cloud (un secteur dominé par des groupes américains, donc soumis au US CLOUD Act), que ce soit

directement ou indirectement (.p. ex. à travers un prestataire de services de premier niveau qui lui-même recours à une infrastructure cloud).

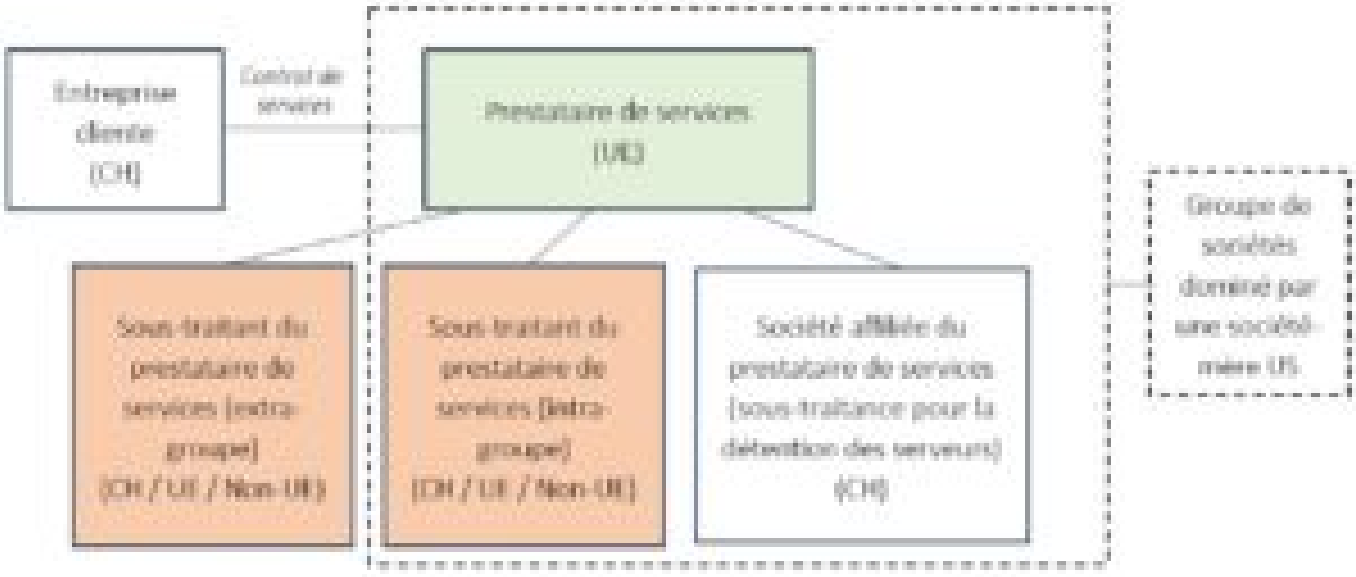
B. La position du Conseil fédéral : ce qui a été dit lors de la reconnaissance du Swiss-U.S. DPF

Le Conseil fédéral a estimé que le Swiss-U.S. DPF garantit un niveau de protection adéquat pour le transfert de données personnelles vers des entreprises certifiées aux États-Unis, sans qu'il soit nécessaire de mettre en place des garanties supplémentaires. Les États-Unis (en ce qui concerne les entreprises américaines certifiées) ont donc été ajoutés, à compter du 15 septembre 2024, à la liste des pays garantissant un niveau adéquat de protection des données (Annexe 1 de l'Ordonnance sur la protection des données). La liste des entreprises américaines certifiées précise (i) si l'entreprise américaine est effectivement certifiée selon le Swiss-U.S. DPF, ainsi que (ii) les types de données personnelles pour lesquelles la certification s'applique (« HR Data » et/ou « Non-HR Data »).

Concrètement, cette décision de reconnaissance permet aux data exporters localisés en Suisse qui mandatent des prestataires américains certifiés de renoncer à la conclusion des EU Standard Contractual Clauses (« EU SCC ») et à la conduite d'un Transfer Impact Assessment (« TIA ») avec un résultat satisfaisant. Force est toutefois de constater que la pratique de marché semble être, pour de nombreux data exporters, de maintenir les EU SCC comme solution de repli (fallback) si le Swiss-U.S. DPF devait être enlevé de la liste des pays adéquats suite à une invalidation en justice de son équivalent UE, le UE-U.S. DPF, comme l'ont été ses deux prédécesseurs (Swiss-U.S. Safe Habour et Swiss-U.S. Privacy Shield, suite à l'invalidation de leurs équivalents UE par la CJUE).

C. La position du Conseil fédéral : ce que le praticien devrait pouvoir tirer de la reconnaissance du Swiss-US DPF

La satisfaction qui a accompagné l'entrée en vigueur du Swiss-US DPF n'a pas pu masquer le fait que ce mécanisme ne couvre en réalité pas le principal scénario auquel les entreprises suisses sont confrontées, i.e., la situation dans laquelle le service cloud-based est contracté auprès d'une société basée dans l'Union européenne, mais affiliée à un groupe américain, les informations (y compris les données personnelles) étant stockées sur un serveur en Suisse (ou dans l'Union européenne), mais accessibles par des sous-traitants du prestataire basés dans différents pays. Cette situation peut être illustrée par le schéma suivant :



Un tel scénario (scénario 1) peut déclencher un risque sous l'angle du US CLOUD Act (i.e., en raison de données personnelles « sous le contrôle » d'un groupe basé aux États-Unis par le biais de ses filiales dans l'Union européenne ou en Suisse), mais n'est pas expressément couvert par le Swiss-U.S. DPF, faute d'un transfert (ou d'une accessibilité) effectif de données personnelles vers les États-Unis dans le cadre du business-as-usual.

Cela étant dit, avant de confier une mission à un prestataire de services (agissant ici en qualité de sous-traitant dans la perspective des règles de protection des données) ayant des liens avec les États-Unis, l'entreprise cliente (agissant ici en qualité de responsable du traitement) doit s'assurer que le prestataire de services (sous-traitant) en question est en mesure de traiter les données personnelles dans le respect des exigences de la LPD, en tenant compte du risque découlant du US CLOUD Act.

Bien que le rapport d'évaluation de l'Office fédéral de la justice à l'appui de la décision de reconnaissance du Swiss-U.S. DPF soit bref, cette décision pourrait, selon nous, être vue comme une prise de position favorable des autorités fédérales suisses sur la compatibilité du US CLOUD Act avec le droit suisse.

Nous sommes ainsi d'avis que, du point de vue de la protection des données, la reconnaissance du Swiss-U.S. DPF apporte une clarification importante pour le scénario 1 présenté dans le schéma ci-dessus. En rendant sa décision, le Conseil fédéral a en effet considéré que les dispositions de droit américain régissant l'accès des autorités américaines aux données personnelles traitées par les entités certifiées ne sont pas contraires aux principes fondamentaux du droit suisse de la protection des données, mais garantissent au contraire une protec-

tion adéquate. S'il n'en était pas ainsi, le Conseil fédéral n'aurait pas pu reconnaître l'équivalence des entreprises américaines certifiées.

Ainsi, la reconnaissance du Swiss-U.S. DPF implique qu'un accès (même effectif) par les autorités américaines (dans le scénario analysé ici par le biais du US CLOUD Act) ne devrait plus constituer un « no-go » absolu pour une entreprise ou une administration suisse. En effet, un tel accès devrait être considéré comme compatible avec les principes fondamentaux du droit suisse de la protection des données. Partant, les conséquences concrètes de la décision de reconnaissance du Swiss-U.S. DPF devraient constituer un élément important pour les entreprises et administrations suisses qui envisagent de collaborer avec des sous-traitants potentiellement soumis aux demandes des autorités américaines dans le cadre du US CLOUD Act. L'analyse de risques auquel il convient, selon nous de procéder dans un tel scénario, devrait être le lieu pour documenter le raisonnement suivi pour retenir l'admissibilité, sous l'angle de la LPD, d'un éventuel accès des autorités américaines aux données stockées auprès de l'entité sise dans l'Union européenne d'un groupe basé aux États-Unis.

A nos yeux, les mêmes considérations peuvent s'appliquer à un second scénario (scénario 2). Ce dernier concerne le cas dans lequel des données personnelles sont transférées par une entreprise suisse à destination d'un importateur de données aux États-Unis non certifié sous l'angle du Swiss-U.S. DPF, mais éligible à une telle certification. En effet, les entreprises s'appuyant sur les EU SCC pour de tels transferts peuvent, dans le cadre de leur Transfer Impact Assessment (qui est nécessaire dans ce scénario, au vu de la pratique du Préposé fédéral en cas de recours aux EU SCC pour fonder un transfert de données personnelles vers un État non-adéquat), considérer que l'accès des autorités américaines aux données personnelles traitées par les entités certifiées rendues possibles en vertu du US CLOUD Act a été jugé acceptable par le Conseil fédéral dans la décision de reconnaissance du Swiss-U.S. DPF.

L'on relèvera que ce raisonnement inclut également, par exemple, les pouvoirs des services de renseignement américains, qui ont été reconnus comme « non-problématiques » dans le cadre du Swiss-U.S. DPF. En effet, le nouveau mécanisme de protection juridique (aux États-Unis) introduit en lien avec le Swiss-U.S. DPF concernant l'accès aux données personnelles par les services de renseignement américains s'applique également lorsque le traitement des données personnelles est réalisé par des entreprises non certifiées sous l'empire du Swiss-U.S. DPF.

Cela étant dit, il est important de souligner que tout risque identifié lors d'un transfert en dehors de Suisse doit être limité à un niveau raisonnable (qui ne peut être nul vu que le

risque zéro n'existe pas, contrairement aux exigences formulées dans la prise de position « SUVA/M365 » du Préposé fédéral), par le biais de moyens techniques, organisationnels et juridiques (Technical and Operational Measures, TOMs). Un tel risque limité à un niveau raisonnable doit pouvoir être accepté conformément à l'approche fondée sur les risques qui sous-tend le droit suisse de la protection des données. Cette approche fondée sur les risques a été explicitement intégrée dans la LPD et rappelée dans le cadre des travaux de révision (cf. FF 2017 6565, 6593). L'art. 8 LPD impose en effet aux responsables du traitement et aux sous-traitants de garantir une sécurité des données adaptée au risque grâce à des mesures techniques et organisationnelles appropriées. Or, l'art 8 LPD s'applique à tous les traitements des données personnelles, donc également à un transfert de celles-ci en-dehors de Suisse› .

D. Et qu'en est-il si les données sont (en sus) couvertes par un secret professionnel ?

En revanche, dans les deux scénarios, s'agissant d'un éventuel secret professionnel qui pourrait s'appliquer aux données remises au prestataire, il est important de souligner que le Swiss-U.S. DPF n'apporte aucun changement à l'obligation de respecter un tel secret.

Ceci est en particulier vrai pour le secteur bancaire. Qu'il s'agisse de suivre l'approche traditionnelle, selon laquelle une renonciation valable au secret bancaire (accordée par le client) serait nécessaire afin de pouvoir confier des client-identifying data (CIDs) à un prestataire de services localisé en-dehors de Suisse, ou d'adopter la position plus récente prise, entre autres, dans les Cloud Guidelines publiées par l'Association suisse des banquiers, selon laquelle une telle renonciation ne serait pas requise, une règle est claire : la communication de CIDs à un auxiliaire à l'étranger doit toujours faire objet de TOMs adéquats, qui limitent de manière adéquate l'accès aux données par des tiers non autorisés, tels que, le cas échéant, des autorités étrangères.

Le secteur public, quant à lui, connaît la notion de « secret de fonction » au sens de l'art- 320 CP. La notion d'auxiliaire a été ajoutée à l'art. 320 CP à compter du 1er janvier 2023 et le Conseil fédéral a précisé « qu'il n'y avait pas de violation du secret de fonction lorsque des informations protégées sont communiquées à un auxiliaire en Suisse ou à l'étranger (BO 2022 N 353 s). A noter toutefois que certaines autorités cantonales de protection des données adoptent des positions plus strictes sur ce point et imposent aux administrations publiques sous leur compétence des exigences élevées en cas de transfert à l'étranger de données soumises au secret de fonction.

E. Perspectives d'avenir

Après l'agitation générée par la décision Schrems II, l'on assiste aujourd'hui, au niveau des tribunaux, à un retour vers une approche plus raisonnable s'agissant des transferts transatlantiques de données personnelles. Des décisions allemandes (cf. par exemple LG Passau, Endurteil v. 17.06.2024 – 1 O 121/24) relatives à Facebook constatent que les transferts d'un data exporter en Allemagne vers l'entité irlandaise du Groupe Facebook, avec ensuite un onward transfer vers la maison-mère du Groupe aux États-Unis, sont acceptables en cas de mise en place des EU SCC et eu égard au nouveau mécanisme de protection juridique (aux États-Unis) introduit en lien avec le Swiss-U.S. DPF.

Si l'on continue ce raisonnement, le transfert depuis un responsable de traitement situé dans l'Union européenne (ou en Suisse) vers un prestataire de services basé dans l'Union européenne (mais potentiellement soumis à l'effet extraterritorial de US Cloud Act) devrait, comme discuté ci-dessus (scénario 1), être acceptable dans la perspective du RGPD (et de la LPD). A nos yeux, il est même possible d'aller encore un pas plus loin : dans le cas d'un transfert effectif de données personnelles à un prestataire américain non-certifié, mais éligible à la certification (scénario 2), les nouvelles dispositions du mécanisme de protection juridique américain adoptées dans la perspective des Data Privacy Frameworks au niveau de l'Union européenne et de la Suisse s'appliquent même en-dehors du Data Privacy Framework et peuvent donc être prises en considération lors de l'analyse du scénario 2, qui devrait donc également être admissible sous l'angle de la LPD.

L'on constate donc que le Swiss-US DPF a un effet indirect en ce sens qu'il peut être pris en compte même dans des scénarios qu'il ne couvre pas expressément, faute d'un transfert direct de données personnelles aux États-Unis (scénario 1) ou d'une certification du data importer américain (scénario 2).

Au niveau suisse, nous sommes d'avis que la décision de reconnaissance du Conseil fédéral devrait clore le débat sur la compatibilité du US CLOUD Act avec le droit suisse de la protection des données. Toutefois, bien que le Swiss-U.S. DPF soit conçu comme une solution à long terme, il convient de rester vigilant, car la question pourrait resurgir en cas de nouveaux développements juridiques, en particulier si une décision de type « Schrems III » venait à être rendue au niveau européen. En tout état de cause, la décision de reconnaissance du Conseil fédéral sera régulièrement réexaminée pour prendre en compte l'évolution du cadre juridique et les décisions susceptibles d'affecter son évaluation. Le premier réexamen est prévu dans le courant de l'année 2025.

F. Conclusion

L'approbation du Swiss-U.S. DPF par le Conseil fédéral marque une étape importante dans la clarification du cadre juridique applicable aux transferts de données personnelles entre la Suisse et les États-Unis. Elle offre une plus grande sécurité juridique aux entreprises et organismes publics suisses utilisant des services cloud américains. En effet, les préoccupations relatives à l'accès potentiel aux données par les autorités américaines, notamment en vertu du US CLOUD Act, ont longtemps soulevé des doutes quant à la conformité de tels fournisseurs avec les exigences légales suisses. La clarification qui découle de la reconnaissance, en Suisse, du Swiss-U.S. DPF, permettra désormais aux entreprises privées et aux institutions du secteur public de prendre des décisions plus éclairées, tout en veillant à ce que les risques liés à la protection des données soient correctement appréhendés.

Proposition de citation : Katharina Martin / Philipp Fischer, Swiss-US Data Privacy Framework : un premier pas vers une approche plus pragmatique ?, 17 janvier 2025 *in* www.swissprivacy.law/332