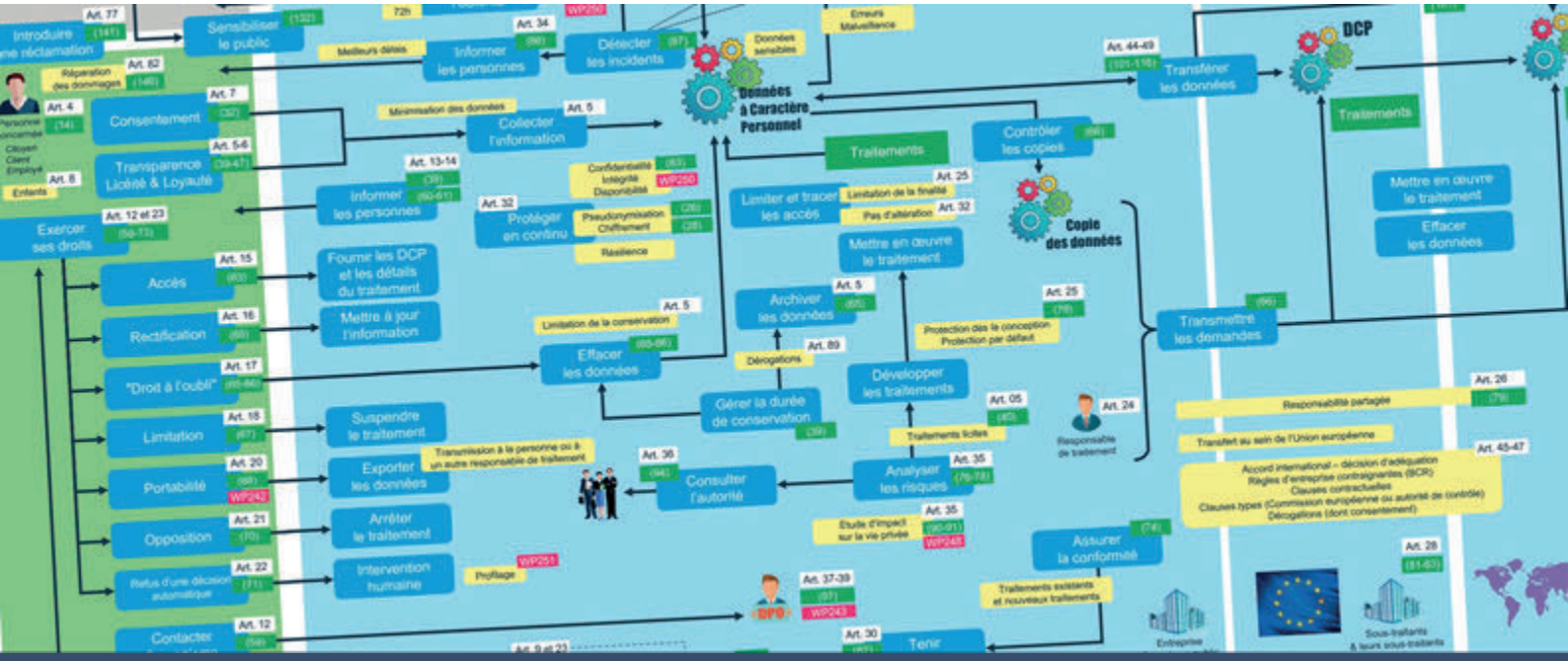
CLUSIF

LES GUIDES PRATIQUES DU CLUSIF - RGPD



TRANSFERT DE DONNÉES VERS LES ÉTATS-UNIS

1. RAPPEL HISTORIQUE

1.1 Le Safe Harbor et le Privacy Shield

Négocié entre les autorités américaines et la Commission européenne en 2001, le ***Safe Harbor*** était un ensemble de principes de protection des données personnelles. Ces règles publiées par le Département du Commerce américain, étaient essentiellement basées sur celles de la Directive 95/46 du 24 octobre 1995, c'est à dire l'information des personnes, la possibilité accordée à la personne concernée de s'opposer à un transfert ou à une utilisation des données pour des finalités différentes, le consentement explicite pour les données sensibles, le droit d'accès et de rectification, la sécurité des données.

M. Maximillian Schrems, ressortissant autrichien résidant en Autriche, a porté plainte auprès de l'autorité de contrôle irlandaise, visant, en substance, à faire interdire les transferts effectués par Facebook. Cette plainte a conduit à un arrêt du 6 octobre 2015 de la Cour de Justice de l'Union Européenne (CJUE), arrêt dit « Schrems I » qui s'est traduit par l'invalidation du Safe Harbor.

Après cette décision, la Commission européenne a pris une nouvelle décision d'adéquation le 8 juillet 2016. Le *Privacy Shield* (Bouclier de protection des données en français), est un mécanisme d'auto-certification pour les sociétés établies aux États-Unis, reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données personnelles transférées depuis une entité européenne vers des sociétés établies aux États-Unis. Le ***Privacy Shield***

UE-États-Unis est entré en vigueur le 1er août 2016[1].

La décision d'adéquation de la Commission européenne validant le *Privacy Shield* a cependant été annulée par la CJUE le 16 juillet 2020 à la suite d'une nouvelle procédure intentée par Max Schrems. Dans son arrêt, dit « Schrems II », la CJUE s'est prononcée sur l'interprétation et la validité du Privacy Shield et sur la validité des clauses contractuelles types (CCT) de la Commission européenne et sur leur utilisation en cas de transfert de données à caractère personnel vers un pays tiers.

1.2 Les motifs d'invalidation par la CJUE

La CJUE a estimé que le droit américain n'accorde pas une protection équivalente à celle du droit européen en matière de la protection des données personnelles. Selon elle, il existe en effet une surveillance excessive exercée par les services de renseignements américains sur les données des citoyens et résidents européens, insuffisamment encadrée et sans réelle possibilité de recours.

Plusieurs législations différentes encadrent les capacités de la justice et des services de renseignement américains. Sont notamment visés dans l'arrêt de la CJUE la collecte et l'accès aux données personnelles à des fins de sécurité nationale en vertu de l'article 702 de la loi américaine FISA (*Foreign Intelligence Surveillance Act*) et du décret (« Executive Order ») 12 333.

La CJUE a analysé la législation américaine en matière d'accès aux données des fournisseurs de services Internet et entreprises de télécommunications par les services de renseignement américains (Section 702 FISA et *Executive Order* 12 333). Ce texte autorise les forces de l'ordre ou les agences de renseignement américaines à obtenir des opérateurs télécoms et des fournisseurs de services de cloud computing des informations stockées sur leurs serveurs que ces données soient situées aux USA ou à l'étranger, y compris les données personnelles.

Il s'agit des données que les hébergeurs Cloud **contrôlent, stockent ou gèrent, ainsi que les clés de chiffrement permettant leur déchiffrement**, concernant les personnes à surveiller (non américaines et non résidentes aux États-Unis).

Le FISA section 702 n'a pas de visée extraterritoriale, c'est-à-dire qu'il n'est applicable qu'auprès d'entreprises opérant sur le territoire américain. En revanche, si ces entreprises ont la capacité d'accéder à distance à des serveurs hébergés dans l'EEE, alors les données qui y sont stockées peuvent être saisies au titre de FISA section 702. C'est pourquoi la définition de «transfert» couvre cette éventualité.

La Cour en a conclu que les atteintes portées à la vie privée des personnes dont les données sont traitées par les entreprises et opérateurs états-uniens soumis à cette législation sont disproportionnées au regard des exigences de la Charte des Droits Fondamentaux.

En particulier, la Cour a jugé que la collecte des données par les services de renseignement n'est pas proportionnée et que les voies de recours, y compris juridictionnelles, dont disposent les personnes à l'égard du traitement de leurs données sont insuffisantes. La CJUE a dès lors invalidé cette décision d'adéquation de la Commission européenne.

1.3 Affirmation de la validité des clauses contractuelles type (sous réserve d'adaptation au cas par cas)

La CJUE a consacré la validité de ces clauses, tout en indiquant que, pour les utiliser, il appartient au responsable de traitement, le cas échéant en collaboration avec le destinataire des données transférées, d'évaluer au cas par cas si, en pratique et pour le transfert envisagé, ces CCT permettent d'assurer aux données transférées un niveau de protection essentiellement équivalent à celui assuré en Union européenne.

Si l'effet de ces clauses est limité ou totalement écarté par la législation du pays tiers applicable aux transferts de ces données, le responsable de traitement doit également mettre en place des garanties supplémentaires pour assurer le

1 Décision 2016/1250 du 12 juillet 2016 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016D1250

niveau de protection des données requis ou notifier l'autorité de protection des données compétente son intention de continuer à transférer des données sans ces garanties.

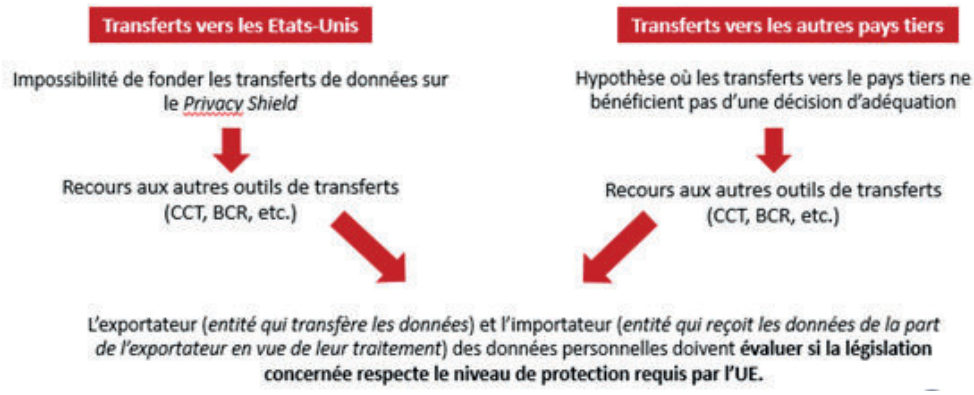
2. QUELS IMPACTS DE L'ARRÊT SCHREMS II ?

La décision de la CJUE n'a pas pour effet d'interdire de manière générale tous les transferts de données personnelles vers les États-Unis d'Amérique.

Pour procéder à de tels transferts, la décision de la CJUE implique en revanche de mener une analyse spécifique et de respecter de nouvelles conditions.

Outre l'encadrement de ces transferts (clauses contractuelles, BCR, etc.), des mesures supplémentaires doivent être mises en œuvre par l'exportateur de données afin d'empêcher tout accès par les autorités américaines de renseignement, lorsqu'elles sont stockées sur le territoire états-unien comme lors de leur transit à destination des États-Unis, ou de rendre les données inutilisables en cas d'accès.

Enfin, à titre exceptionnel, les transferts se fondant sur les dérogations prévues par le RGPD peuvent également se poursuivre à destination des États-Unis.



Comment évaluer la législation du pays tiers ?

Le Comité européen de la protection des données (CEPD) a publié des recommandations le 10 novembre 2020[2] sur **les garanties essentielles qui doivent être trouvées dans le cadre juridique d'un pays tiers** dans le cadre de la surveillance mise en œuvre par les autorités publiques de ce pays :

- L'ingérence dans la vie privée doit :
  - Reposer sur des règles claires, précises et accessibles ;
  - Être nécessaire et proportionnée au regard des objectifs légitimes poursuivis ;
- Un mécanisme de contrôle indépendant doit être mis en place ;
- Les personnes doivent bénéficier de voies de recours effectives.

Le CEPD a également précisé la notion de garanties supplémentaires :

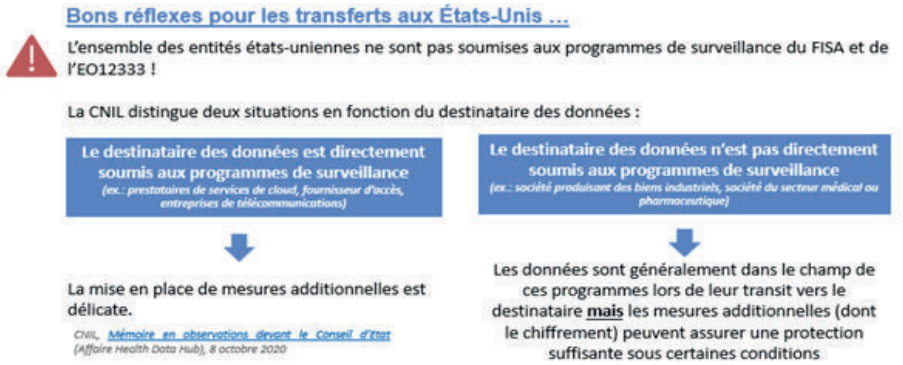
2 https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_fr.pdf

Quelles sont les actions à mettre en œuvre avant un transfert hors UE ?

Dans ses recommandations du 10 novembre 2020, le CEPD préconise la mise en place des étapes suivantes :

1. **Cartographier** les transferts vers des pays hors UE ;
2. **Vérifier les outils de transfert utilisés** pour encadrer ces transferts ;
3. **Evaluer le niveau de protection** offert par le pays vers lequel les données sont transférées (en l'absence d'une décision d'adéquation et hors l'hypothèse d'une dérogation particulière) ;
4. **En l'absence d'un niveau de protection adéquate, identifier les garanties supplémentaires** à intégrer dans les outils de transfert.

Source : CEPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, 10 novembre 2020



3. LE CLOUD ACT

Le *Cloud Act* (acronyme de *«Clarifying Lawful Overseas Use of Data Act»*) est une loi fédérale américaine promulguée le 23 mars 2018 qui modifie principalement le chapitre 121 du Titre 18 du *United States Code*, dénommé *Stored Communications Act*, en permettant aux forces de l'ordre ou aux agences de renseignement américaines d'obtenir des opérateurs télécoms et des fournisseurs de services de cloud computing des informations stockées sur leurs serveurs... Que ces données soient situées aux États-Unis ou à l'étranger.

Cette loi fédérale intervient notamment en réaction à un Per curiam de la Cour suprême des États-Unis du 17 avril 2018, dans l'affaire Microsoft Ireland, par lequel la Cour avait censuré le mandat délivré par un juge new-yorkais autorisant la police américaine à perquisitionner des serveurs situés en Irlande, et appartenant à la filiale irlandaise du groupe Microsoft.

Cette loi fédérale permet ainsi aux instances de justices américaines d'émettre un mandat de perquisition contraignant les fournisseurs de Cloud américains (y compris si ces données sont hébergées hors des États-Unis, par exemple, en France) **à fournir toutes les données d'un individu, sans qu'aucune autorisation ne soit demandée à la justice du pays dans lequel se situent l'individu ou les données**.

A la différence du FISA (*Foreign Intelligence Surveillance Act*), le champ d'application du Cloud act ne se limite pas simplement aux personnes morales de droit américain, ou « *US persons* », mais il s'étend aussi à des « *non US per-*

sons ». Le texte permet encore, à l'instar du RGPD, d'atteindre, via un critère de ciblage, les entreprises qualifiées de *« providers of electronic communications services or remote computing services »* dont le marché américain constitue la cible, c'est à dire, éventuellement certaines entreprises européennes, situées sur le territoire de l'Union — soit qu'elles soient des filiales européennes d'entreprise américaines, soit, au contraire, qu'elles ciblent un public américain, par exemple, via leurs filiales implantées aux États-Unis.

Cette loi fédérale étend donc la portée géographique des demandes éventuelles du gouvernement américain à pouvoir accéder aux données sur les serveurs, quelle que soit leur localisation :

- Les prestataires de service doivent communiquer les *«contenus de communications électroniques et tout enregistrement ou autre information relatifs à un client ou abonné, qui sont en leur possession ou dont ils ont la garde ou le contrôle, que ces communications, enregistrements ou autres informations soient localisés à l'intérieur ou à l'extérieur des États-Unis»*.
- Ces autorités américaines peuvent obtenir des données, notamment personnelles ou de contenu, sans que la personne «ciblée» ou que le pays où sont stockées ces données n'en soient informés.
- Le *Cloud Act* permet également au gouvernement américain de signer des accords bilatéraux avec d'autres Etats qui permettent de faciliter les demandes d'accès aux données (à savoir sans procédure judiciaire).

Le périmètre du *Cloud Act* est très large : il porte autant des enquêtes criminelles mais également permet d'accéder aux datas qui pourraient « menacer l'ordre public ». Une notion floue et large et sans réelle définition juridique.

De plus, le *Cloud Act* entre en contradiction avec l'article 48 du RGPD qui dispose que *«Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit* **fondée sur un accord international** *[…]»*. **Cet accord international est ainsi obligatoire pour qu'une juridiction ou une autorité issue d'une administration transfère ou divulgue des données à caractère personnel.**

Certes, le *Cloud Act* permet à un fournisseur de service recevant une réquisition de saisir l'autorité judiciaire américaine si son client visé n'est pas un citoyen, un résident permanent en situation régulière ou une entreprise installée aux États-Unis, et s'il estime que la divulgation d'informations serait contraire à la législation d'un État étranger. Cependant, l'on ne peut préjuger de ce que sera la décision judiciaire dans un pays où de nombreux programmes de surveillance généralisée ont été mis en œuvre soi-disant au nom de la lutte contre le terrorisme.

Les forces de l'ordre des États-Unis ne peuvent donc rechercher le contenu de fournisseurs de services que dans deux circonstances :

- Avec le consentement du client
- En l'absence d'accord bilatéral, avec un mandat délivré par un tribunal américain conformément aux procédures pénales en vigueur aux États-Unis. Et pour qu'un mandat soit émis, un tribunal américain doit être convaincu qu'il existe des motifs probables de croire qu'un crime a été commis et que les preuves demandées sont directement liées à ce crime et contrôlées par le fournisseur.

4. LE DATA PRIVACY FRAMEWORK

Après l'invalidation du *Privacy Shield*, la Commission Européenne a validé un nouvel accord d'adéquation avec les États-Unis, le *Data Privacy Framework*, entré en application le 10 juillet 2023.

Le *Data Privacy Framework* fait l'objet d'une fiche FAQ dédiée.

Campus Cyber
Tour Eria
5 rue Bellini
92821 Puteaux cedex
Tel : +33 1 53 25 08 80
clusif@clusif.fr
https://clusif.fr

L'intégralité de la FAQ RGPD et la liste des membres qui y ont contribué sont consultables sur le site du Clusif
https://clusif.fr/les-publications