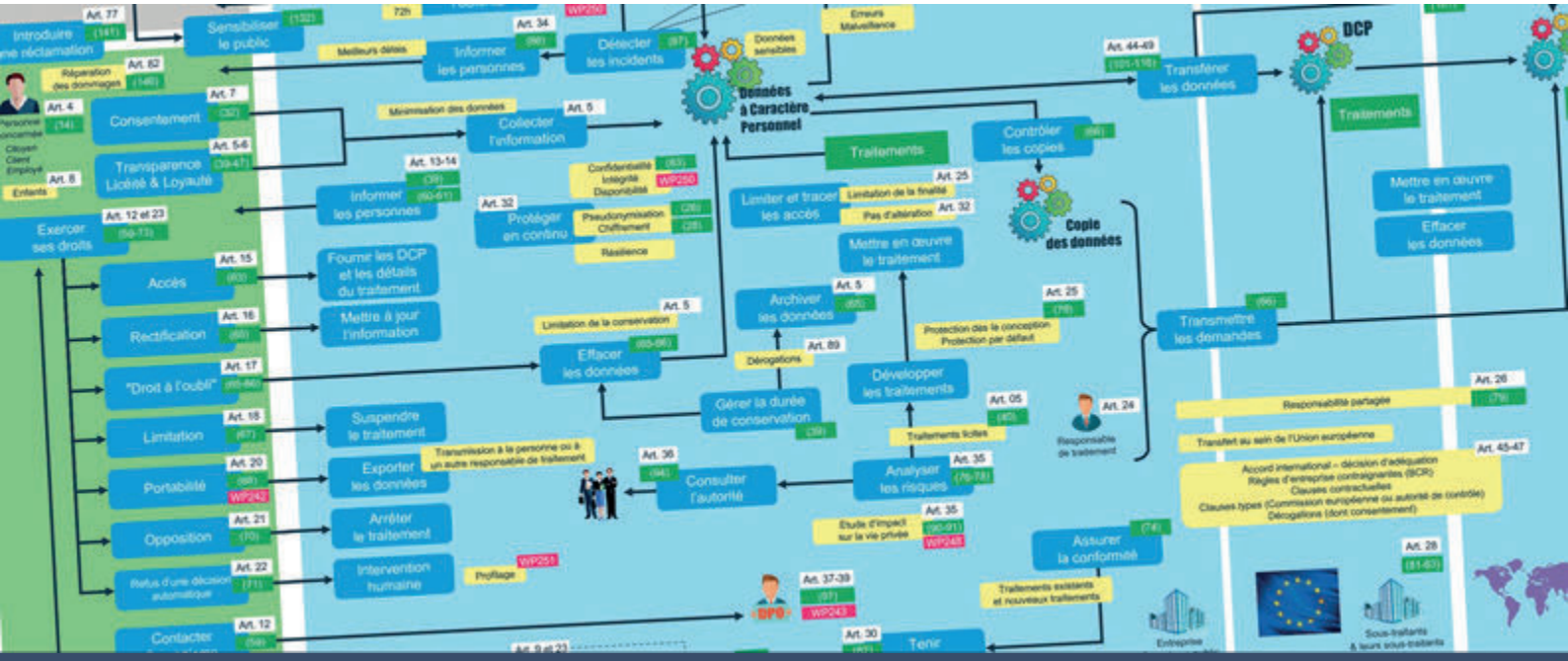
CLUSIF

LES GUIDES PRATIQUES DU CLUSIF - RGPD



LE DATA PRIVACY FRAMEWORK (DPF)

1. LE NOUVEAU DÉCRET EXÉCUTIF DU 7 OCTOBRE 2022

A la suite de l'arrêt Schrems II, un décret du 7 octobre 2022 signé par le président américain Joe Biden prévoit de nouvelles garanties afin de concilier les activités de surveillance américaines et le droit européen. Ce décret est destiné à mettre en œuvre l'accord de principe signé le 25 mars 2022 avec la Commission européenne. Il devrait mettre un terme à la période d'incertitude consécutive à l'invalidation du *Privacy Shield* en 2020 par la Cour de justice de l'Union européenne.

L'un des objectifs principaux de cet accord entre la Commission européenne et les États-Unis a été d'encadrer l'accès des services de renseignement américains aux données des citoyens de l'Union européenne et leur utilisation à des fins de sécurité nationale. Désormais, ces services pourront accéder aux données transférées si, et seulement si, les activités de surveillance sont « nécessaires » et « proportionnées » à la poursuite de leurs objectifs.

L'arrêt Schrems II a précisé les deux conditions nécessaires à garantir un niveau de protection équivalent au droit européen :

- La surveillance américaine doit être proportionnée et nécessaire au sens de l'article 52 de la Charte des droits fondamentaux[1]. A cette fin, le décret présidentiel prévoit :
    - Le renforcement du contrôle des agences de renseignement, exigeant notamment qu'elles soient menées de

1 https://fra.europa.eu/fr/eu-charter/article/52-portee-et-interpretation-des-droits-et-des-principes

manière « proportionnées et nécessaires[2] » en vue de la réalisation d'objectifs de sécurité nationale définis, et en prenant en considération la vie privée et les libertés civiles des personnes ;

- L'obligation de traiter les données personnelles collectées par les agences de renseignement de manière proportionnée après une évaluation des facteurs pertinents au regard des objectifs ;
- La mise en conformité des procédures et politiques des agences de renseignement afin de respecter les nouvelles règles introduites en matière de vie privée et de liberté civile ;
- L'examen par le *Privacy and Civil Liberties Oversight Board* des politiques et procédures des agences de renseignement américaines (afin de s'assurer de leur conformité aux mesures prévues par le décret) ainsi que la revue annuelle du mécanisme de recours ;

• L'accès à un recours indépendant et contraignant doté d'un double niveau juridictionnel, garantissant, conformément à l'article 47 de la charte de l'Union européenne, le droit à un recours effectif et à accéder à un tribunal impartial :

- Le premier niveau de recours est confié à un agent sous la direction du Director of National Intelligence, menant une première enquête sur plainte ;
- Le second à une *Data Protection Review Court* (DRPC) qui procèdera à un examen indépendant et contraignant des décisions prises par l'agent ;

Ce second point ne répond pas aux exigences de la Commission européenne. Il ne s'agit pas à proprement parler d'une juridiction (la DPRC s'apparentant davantage à un organe relevant du pouvoir exécutif américain).

Il appartient à la Commission européenne de constater par une décision d'adéquation, que le texte garantit bien un niveau de protection des données personnelles « adéquat ».

Maximilian Schrems, président de l'ONG NOYB (*None Of Your Business*) à l'origine des précédents recours contre les décisions d'adéquation US-UE, est déjà mobilisé et prévoit de saisir la CJUE d'un recours contre la future décision d'adéquation qui pourrait être adoptée à la suite de ce nouveau texte, la *Data protection Commission* (DPC) irlandaise devant s'attendre à une nouvelle plainte de l'activiste.

2. LE DATA PRIVACY FRAMEWORK (DPF)

La Commission européenne a publié le 14 décembre 2022 sa proposition de décision d'adéquation qui autorise à nouveau les transferts de données personnelles vers les États-Unis[3].

> Pour rappel, une décision d'adéquation est un instrument prévu par l'article 45 du RGPD. C'est une décision adoptée par la Commission européenne, qui dresse une équivalence théorique entre les niveaux de protection des données à caractère personnel, permettant ainsi de les transférer depuis l'Union européenne vers un autre pays. Ainsi, un pays tiers à l'UE ou une organisation internationale est considérée comme assurant un niveau de protection adéquat des données à caractère personnel.

La Commission européenne lance ainsi le processus en vue de l'adoption d'une décision d'adéquation concernant le cadre de protection des données UE-États-Unis. Cette décision d'adéquation devrait répondre aux préoccupations soulevées par la Cour de justice de l'Union européenne (CJUE) dans sa décision « Schrems II » du 16 juillet 2020 ayant conduit à l'invalidation du « Privacy Shield ».

C'est à la suite d'un **accord de principe**[4] entre l'Union européenne et les Etats-Unis du 25 mars 2022, puis de la signature du **décret exécutif américain** le 7 octobre 2022[5] (*Executive order*) visant à introduire des garanties pour les données personnelles des résidents de l'Union européenne (notamment en limitant l'accès des agences de renseignement américaines et en introduisant un mécanisme de recours indépendant), que cette troisième tentative de

2 A noter que si le décret mentionne bien les termes « proportionné » et « nécessaire » ; le système de surveillance de masse américain demeure possible dans certaines conditions...

3 https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en

4 Trans-Atlantic Data Privacy Framework, 25 mars 2022. En mars 2022, à la suite d'intenses négociations entre les principaux négociateurs, le commissaire Reynders et la secrétaire d'État Raimondo, la présidente von der Leyen et le président Biden ont annoncé un accord de principe sur un nouveau cadre pour le transfert transatlantique de données.

5 En octobre 2022, le président Biden a signé un décret présidentiel intitulé «Enhancing Safeguards for United States Signals Intelligence Activities», qui a été complété par des règlements adoptés par le procureur général des États-Unis. Ensemble, ces deux instruments ont mis en œuvre dans le droit américain les engagements pris par les États-Unis et ont complété les obligations des entreprises américaines.

décision d'adéquation a vu le jour. Ainsi, la Commission européenne a évalué le cadre juridique américain et a conclu que celui-ci offre des garanties comparables à celles de l'Union européenne, en ce qu'il assure un niveau de protection adéquat pour les données à caractère personnel transférées de l'Union européenne vers les entreprises américaines.

Le projet de décision a été publié et transmis au Comité européen de la protection des données (CEPD) et au Parlement européen pour avis. La Commission européenne a ensuite demandé l'approbation du comité des représentants des États membres de l'Union européenne. C'est à l'issue de cette procédure que la Commission a procédé à l'adoption de la décision finale d'adéquation.

2.1 Contenu de la décision

La décision d'adéquation, essentiellement fondée sur le contenu de l'*Executive order* signé en octobre 2022 par Joe Biden, est divisé en plusieurs parties :

- Cadre de confidentialité des données entre l'Union européenne et les Etats-Unis ;
- Accès et utilisation des données personnelles transférées de l'Union européenne par les autorités publiques des Etats-Unis ;
- Effets de la décision et action des autorités de protection des données ;
- Suivi et révision de la décision ;
- Suspension, abrogation ou modification de la décision ;
- Considérations finales.

Le projet repose sur un **système de certification annuelle** en vertu duquel les entreprises américaines s'engagent à respecter **un ensemble d'obligations en matière de confidentialité et les principes de protection de la vie privée des personnes** (transparence, responsabilité, minimisation, exactitude des données, sécurité, effacement des données...) et déclarer publiquement leur engagement à ces principes et que leur politique de confidentialité est en accord avec ces principes. Pour être certifiées, les entreprises devront se soumettre au pouvoir d'enquête de la FTC (*Federal Trade Commission*) ou du ministère américain des transports (*DoT*).

En outre, les résidents de l'Union européenne bénéficieront de plusieurs **voies de recours en cas de violation de leurs données à caractère personnel** dans le cadre prévu. Ce dernier point était essentiel pour la CJUE.

Le cadre juridique américain prévoit un certain nombre de limitations et de garanties en ce qui concerne l'accès des pouvoirs publics des États-Unis aux données, en particulier à des fins d'application du droit pénal et de sécurité nationale. Il s'agit notamment des nouvelles règles introduites par le décret présidentiel américain, qui répondait aux préoccupations soulevées par la Cour de justice de l'Union européenne dans l'arrêt Schrems II :

- L'accès des services de renseignement américains aux données européennes sera **limité à ce qui est nécessaire et proportionné** pour protéger la sécurité nationale ;
- Les citoyens de l'UE auront la possibilité d'obtenir réparation en ce qui concerne la collecte et l'utilisation de leurs données par les services de renseignement américains devant un mécanisme de **recours indépendant et impartial**, qui comprend
    - **L'Officier de Protection des Libertés Civiles** (*Civil Liberties Protection Officer*), voie de recours de niveau 1,
    - **Une Cour de révision de la protection des données** (*Data Protection Review Court*), voie de recours de niveau 2. Nouvellement créée, la Cour examinera et tranchera de manière indépendante les plaintes des Européens, y compris en adoptant des mesures correctives contraignantes.

Les **entreprises situées dans l'Union européenne pourront s'appuyer sur ces garanties pour les transferts de données transatlantiques**, et également lorsqu'elles utiliseront d'autres mécanismes de transfert, tels que des clauses contractuelles types et les règles d'entreprise contraignantes.

Le fonctionnement du cadre UE-États-Unis de protection des données fera l'objet d'examens périodiques effectués par la Commission européenne, les autorités européennes chargées de la protection des données et les autorités américaines compétentes. Le premier réexamen aura lieu dans un délai d'un an après l'entrée en vigueur de la décision d'adéquation, afin de vérifier si tous les éléments pertinents du cadre juridique américain ont été pleinement mis en œuvre et fonctionnent efficacement dans la pratique.

A noter que l'ONG autrichienne NOYB (*None Of Your Business*) et son président Max Schrems n'ont pas manqué de réagir à cette annonce. A l'origine de l'invalidation des deux précédents cadres, ils ont une nouvelle fois réitéré leurs critiques vis-à-vis du cadre juridique prévu. Bien que certains amendements, comme l'établissement d'une Cour,

semblent prometteurs, Max Schrems lui-même indique que « comme le projet de décision est basé sur le fameux décret exécutif américain, je ne vois pas comment il pourrait survivre à une contestation devant la Cour de justice. Il semble que la Commission européenne ne fait qu'émettre des décisions similaires encore et encore, en violation flagrante de nos droits fondamentaux ».

2.2 L'avis du comité européen de la protection des données et du Parlement Européen

Le 28 février, le Comité européen à la protection des données (CEPD[6]) a rendu son avis sur le projet de décision d'adéquation de la Commission européenne. Il relève les améliorations apportées par le nouveau cadre juridique américain, mais indique que des préoccupations subsistent[7].

De son côté, le Parlement européen a adopté le 11 mai 2023[8] une motion, engageant la Commission à ne pas adopter la décision d'adéquation tant que subsistent les inquiétudes émises par le CEPD. Le Parlement européen demande également à la Commission de ne pas prendre en compte, dans la décision, des intérêts politiques ou commerciaux. Le vote des parlementaires, largement favorable au refus de la décision d'adéquation, est justifié par l'insuffisance des efforts américains pour rendre le cadre des échanges transatlantiques de données suffisamment protecteur pour les européens. Le Parlement relève à ce sujet une dizaine de points qui pêchent par une insuffisance d'engagement des États-Unis. Il faut toutefois noter que l'avis du CEPD et du Parlement ne sont que consultatifs, et n'obligent pas la Commission à les suivre.

2.3 La décision du 10 juillet 2023

Par un communiqué du 10 juillet 2023, la Commission européenne a annoncé avoir adopté la décision d'adéquation portant sur les transferts de données personnelles des citoyens européens depuis l'Union Européenne vers certains organismes américains. Après une analyse globale de la législation américaine, et notamment du décret exécutif signé le 7 octobre 2022, la Commission européenne prend acte des nouveaux engagements inscrits au « *Data Privacy Framework* » et considère que les États-Unis assurent un niveau adéquat de protection des données personnelles. Conformément aux dispositions de l'article 45 du RGPD, les transferts de données personnelles entre l'Union européenne et les États-Unis sont présumés licites.

Le texte prévoit que :

- **Les données à caractère personnel pourront circuler librement et en toute sécurité vers les entreprises américaines inscrites sur une liste rendue publique par le Département du commerce américain** (*Federal Trade Commission*).

> **Les transferts de données personnelles depuis l'Union européenne vers les organismes figurant sur cette liste peuvent donc s'effectuer librement**, sans encadrement spécifique par des « clauses contractuelles types » ou un autre instrument de transfert.
>
> Pour les transferts de données vers des organismes **ne figurant pas** sur cette liste, il faudra :
>
> - **Utiliser un des autres mécanismes** mis à disposition : clauses contractuelles types conformes au RGPD, mécanisme alternatif (BCR, codes de conduite...).
> - **Procéder à une analyse d'impact du transfert** : intégration des évolutions légales américaines en conformité avec la solution de la CJUE, suivi des recommandations du CEPD.
> - **Mettre en place des garanties techniques** (en fonction des circonstances du traitement mis en œuvre), des garanties contractuelles (mesures techniques spécifiques, transparence et renforcement de l'exercice des droits des personnes concernées) et des garanties organisationnelles (politiques internes de transfert, minimisation des données, audits internes...).

- **De nouvelles règles et garanties contraignantes sont mises en place** pour limiter l'accès aux données par les autorités de renseignement américaines. Les agences de renseignement américaines adopteront des procédures

6 Organe qui regroupe l'ensemble des autorités de protection des données au niveau européen
7 https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en
8 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html

pour assurer un contrôle efficace des nouvelles normes en matière de protection de la vie privée et des libertés civiles ;

- **Les droits des personnes concernées sont renforcés**. Les entreprises certifiées devront mentionner dans leurs politiques de confidentialité un point de contact chargé des traitements des demandes d'exercice des droits ainsi qu'indiquer un organe indépendant de résolution (*independent dispute resolution body*) gratuit pour les utilisateurs et qui pourra prononcer les sanctions à l'égard des entreprises qui ne respectent pas les principes fondamentaux ;
- Les États-Unis vont créer un nouveau **système de recours à deux niveaux pour examiner et résoudre les plaintes des Européens** sur l'accès aux données par les autorités de renseignement américaines. Au premier niveau est créé un *Civil Liberties Protection Officier* qui veille au respect de la vie privée et des droits fondamentaux par les services de renseignement américains. Au second niveau, il sera désormais possible de faire appel devant la nouvelle Cour de contrôle de la protection des données (*Data Protection Review Court*) ;
- Une obligation pour les entreprises qui traitent des données transférées depuis l'UE de s'auto-certifier et de se déclarer auprès de la *Federal Trade Commission*.

2.4 Conséquences pratiques et limites du DPF

L'entrée en application du DPF est certainement une bonne nouvelle pour les organismes Européens qui doivent procéder à des transferts de données personnelles avec les États-Unis. Après plusieurs années d'incertitude, le DPF apporte un cadre juridique stabilisé. Toutefois, il faut bien noter qu'il ne s'agit pas d'une solution parfaite.

Les décisions d'adéquation de la Commission européenne assurent généralement que le pays concerné offre une protection correcte des données personnelles d'une manière générale. Ces décisions sont rappelées sur le site de la Commission[9] et concernent (à la date du 1er octobre 2023) les pays suivants : Andorre, Argentine, Canada (pour les organisations commerciales), Iles Féroé, Guernesey, Israël, Ile de Man, Japon, Jersey, Nouvelle Zélande, République de Corée, Suisse, Royaume Uni et Uruguay.

Or, en ce qui concerne les États-Unis, **la décision ne porte que sur les organismes qui ont suivi la démarche d'auto-certification** auprès du Département du commerce américain. Leur liste est accessible publiquement[10]. Il faut d'ailleurs noter que la procédure d'enregistrement est payante et relativement onéreuse, ce qui peut dissuader les organisations de petite taille.

La décision d'adéquation des États-Unis ne porte donc que sur les organismes auto-certifiés, qui ne peuvent être que des entreprises. **Elle ne couvre donc pas les organismes publics, ni les organisations associatives ou similaires**.

Le DPF comporte des précisions sur la prise en compte des transferts ultérieurs[11]. Les organisations qui transfèrent des données à un tiers doivent conclure un contrat avec ce tiers, prévoyant que les données seront traitées conformément aux principes de protection des données, et instituant des mesures pour s'assurer que le tiers traite effectivement les données conformément aux principes.

Pour les organismes qui ne sont pas couverts par la décision d'adéquation, les transferts de données ne peuvent s'effectuer qu'avec l'usage des autres outils proposés, comme les CCT ou les règles d'entreprise contraignantes (BCR) pour les transferts entre filiales.

La prudence est également conseillée en ce qui concerne la **pérennité de l'accord fondé sur le DPF**, qui pourrait être remis en question comme ses prédécesseurs Safe Harbor et Privacy Shield.

D'une part, Max Schrems et Noyb n'ont pas caché leur intention de lancer de nouvelles procédures visant l'annulation du DPF qui, si elles aboutissent, demanderons plusieurs années.

D'autre part, agissant à titre personnel, le député français Philippe Latombe a intenté une action devant la CJUE, dont il espère un résultat plus rapide, demandant l'annulation de la décision d'adéquation qui selon lui, porte atteinte à ses droits et n'est conforme ni au RGPD, ni à la Charte des Droits Fondamentaux de l'Union.

9 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_fr
10 https://www.dataprivacyframework.gov/s/participant-search
11 https://www.dataprivacyframework.gov/s/article/3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER-dpf

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