# L'AVIS DE L'EXPERT EUROPEEN

DBF Bruxelles
Délégation des Barreaux de France

## LE DATA PRIVACY FRAMEWORK ENTRE L´UE ET LES ETATS-UNIS : HISTORIQUE, FONCTIONNEMENT ET PERSPECTIVES

N°52

MARS 2025

**3**

C'EST LE NOMBRE DE CADRES JURIDIQUES INSTITUÉS ENTRE LES ETATS-UNIS ET L'UNION EUROPÉENNE AFIN D'ENCADRER LES TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL.

**SEBASTIAN CORDING**
PRÉSIDENT DU COMITÉ SURVEILLANCE AU SEIN DU CCBE
EXPERT ALLEMAND AU SEIN DU COMITÉ IT
AVOCAT SPÉCIALISÉ DANS LE DROIT DES TECHNOLOGIES DE L'INFORMATION, DES MÉDIAS ET DU DROIT D'AUTEUR AU SEIN DU CABINET CMS À HAMBOURG

**LIENS COMPLEMENTAIRES**

- Décision d'adéquation concernant la circulation sécurisée de données entre l'UE et les Etats-Unis
- Trump Fires Democrats from Privacy Oversight Board (Correct)
- Executive Order 14086
- Le cloud américain bientôt illégal ? Trump fait un premier trou dans l'accord UE-USA sur les données personnelles
- La Commission européenne soumet les transferts de données entre l'UE et les Etats-Unis à un troisième examen par la CJUE
- Décision d'exécution instaurant le *Data Protection Framework*
- Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, dit « E-evidence »).

### A. Historique

Le *Data Privacy Framework* (« DPF ») constitue la 3ème tentative de la Commission européenne de créer un cadre juridique sécurisé pour les transferts de données de l'UE vers les Etats-Unis. En effet, le transfert de données à caractère personnel vers des pays tiers en dehors de l'Espace économique européen nécessite une base juridique spécifique. La solution la plus simple pour les entreprises est l'adoption par la Commission européenne d'une décision dite d'adéquation, par laquelle elle constate qu'un niveau de protection des données personnelles comparable à celui de l'UE existe dans le pays tiers concerné. Le DPF est un accord intergouvernemental qui vise à créer les conditions d'un niveau de protection adéquat aux Etats-Unis et qui sert de base à la décision d'adéquation de la Commission.

L'accord dit « *Safe Harbor* », une décision d'adéquation de la Commission européenne datant de l'année 2000, reposait sur une auto-certification des entreprises auprès de la *Federal Trade Commission* et été annulé par la Cour de justice de l'Union européenne (« CJUE ») en 2016 (« Schrems I »). La décision d'adéquation suivante, datant de 2016, reposait quant à elle sur le « *Privacy Shield* ». Là encore, le principe restait celui de l'auto-certification. A ce titre, un médiateur a été nommé pour assurer la protection juridique et il était prévu que les mesures de surveillance des services secrets seraient limitées. Cette décision d'adéquation a également été annulée par la CJUE en 2020 (« Schrems II »). Les pouvoirs étendus des services secrets ainsi que les mécanismes de protection juridique insuffisants pour les citoyens de l'UE ont été déterminants dans cette décision.

### B. Fonctionnement du Data Privacy Framework

Le DPF de 2023 repose également sur une auto-certification des entreprises, mais est également complété par un nouveau mécanisme de protection juridique. Désormais, les personnes concernées peuvent s'adresser à l'autorité de protection des données de leur pays d'origine, qui transmettra ensuite la plainte aux Etats-Unis. Là-bas, le *Civil Liberties and Privacy Office* (« CLPO ») est compétent en première instance et le *Data Protection Review Court* (« DPRC ») en deuxième instance. En outre, le *Privacy and Civil Liberties Oversight Board* (« PCLOB ») est un organe de contrôle indépendant et non partisan au sein de l'exécutif. Il est composé de 5 membres et est habilité à examiner les stratégies de l'exécutif, ainsi que leur mise en œuvre en ce qui concerne la protection de la vie privée et des libertés civiles.

Avant même l'entrée en fonction de Donald Trump, des doutes ont été émis quant à la compatibilité du DPF avec le RGPD. La collecte et l'utilisation massives de données par les services secrets américains sur la base de l'*Executive Order* (EO) 12333 et surtout de la section 702 du *Foreign Intelligence Surveillance Act* se poursuivirent. La disposition de l'EO 14086 selon laquelle ces mesures de surveillance doivent être « proportionnées » à l'égard des citoyens de l'UE, ne peut dissiper complètement les préoccupations qui en découlent, compte tenu d'une compréhension complètement différente de la notion de « proportionnalité ».

Par ailleurs, le CLPO n'est pas un organisme indépendant, mais fait partie des services secrets américains. Le DPRC est certes indépendant sur le plan formel, mais les procédures qui s'y déroulent ne correspondent pas non plus aux conceptions européennes de l'état de droit. Ainsi, la personne concernée ne peut pas se présenter elle-même devant cet organisme, mais est représentée par un envoyé spécial. En outre, ni la décision elle-même ni les motifs de celle-ci ne sont par la suite communiqués à la personne concernée. Au vu de ces faiblesses, il est permis de douter que la CJUE considère ces procédures comme se déroulant devant un tribunal au sens de l'article 47 de la Charte des droits fondamentaux de l'Union européenne, ce qui est pourtant une condition préalable pour que la CJUE considère qu'un niveau de protection adéquat est assuré.

### C. Perspectives : le DPF sous l'administration Trump

Dès les premières semaines ayant suivi son entrée en fonction, l'administration Trump a attaqué les fondements essentiels du DPF. Ainsi, les 3 membres du PCLOB appartenant au parti démocrate ont été licenciés, de sorte qu'il ne reste plus que 2 membres de cet organe, lequel n'est donc plus en mesure de prendre des décisions. On peut également se demander si cet organisme peut être indépendant, alors que le président est en mesure d'exercer une influence aussi forte sur lui. Il est également possible que l'administration Trump abroge l'EO 14086, ce qui pourrait être réalisé à tout moment, sans l'accord du Congrès.

Si l'on ajoute à cela les doutes déjà exprimés quant à la légalité de la décision d'adéquation, il n'est pas impossible qu'une décision « Schrems III » soit rendue. Compte tenu de l'importance pratique considérable des transferts de données de l'UE vers les Etats-Unis, la recherche d'une nouvelle base juridique pour ces transferts devrait alors commencer très rapidement. Il reste toutefois à voir si l'administration américaine, sous la présidence Trump, lancera d'autres attaques contre le DPF dans le cadre de sa restructuration.

Cela pourrait également entraîner des répercussions sur un autre accord prévu entre l'UE et les Etats-Unis, à savoir le règlement « E-Evidence », entré en vigueur le 28 juillet 2023. Celui-ci prévoit l'échange numérique transfrontalier obligatoire de preuves électroniques entre les tribunaux, les autorités et les fournisseurs de services de télécommunication (fournisseurs de services) au sein de l'UE. Un accord similaire avec les Etats-Unis est en cours de négociation et devrait permettre un tel échange numérique avec ce pays. Il semble difficile d'imaginer qu'un tel accord puisse être conclu alors même que le respect des exigences fondamentales en matière de protection des données n'est pas en pratique garanti aux Etats-Unis.