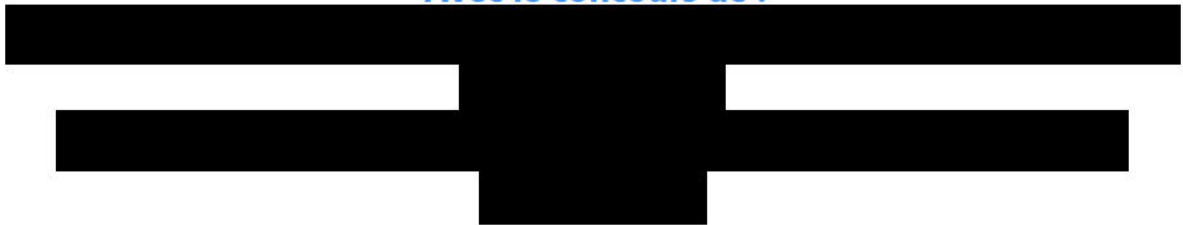


Communication présentée en séance plénière le 28 septembre 2023

COMMUNICATION SUR LES REGLES APPLICABLES AU  
REGARD DES TRANSFERTS DE DONNEES HORS UNION  
EUROPEENNE

Rapporteur : M. **François PELLEGRINI**

Avec le concours de :



## Table des matières

1. Rappel des principes généraux en matière de transferts de données hors de l'Union européenne.....	2
2. Les décisions d'adéquation .....	6
A. Focus sur l'adéquation des États-Unis.....	6
a) Rappel du contexte .....	6
b) Éléments clés du nouveau cadre.....	7
c) Conséquences pour les organismes souhaitant transférer des données vers les États-Unis.....	8
B. Application de l'article 48 du RGPD à des fournisseurs soumis à des lois extra-européennes autorisant les demandes d'accès par des autorités publiques de pays tiers...	9
3. Les garanties appropriées .....	13
A. Présentation des garanties .....	13
B. Analyse d'impact sur les transferts .....	15
4. Les dérogations .....	16
5. Possibilités liées à l'article 9.4 du RGPD .....	17

## 1. Rappel des principes généraux en matière de transferts de données hors de l'Union européenne

Le chapitre V du RGPD (articles 44 à 49) fixe les règles en matière de transfert de données hors de l'Union européenne, de sorte que le niveau de protection des personnes physiques garanti par le RGPD ne soit pas compromis lorsque des données à caractère personnel sont transférées vers un pays tiers ou une organisation internationale. Les responsables de traitement et les sous-traitants peuvent transférer des données hors de l'Union européenne et de l'espace économique européen à condition d'assurer un niveau de protection des données suffisant et approprié c'est-à-dire en transférant vers un pays considéré comme assurant un niveau de protection adéquat (section 2.) ou si des garanties appropriées sont mises en place (section 3.). À défaut, il existe également des dérogations permettant d'effectuer des transferts dans certains cas particuliers (section 4.).

L'article 4 du RGPD ne contient pas de définition de **la notion de transfert**. Le CEPD a adopté le 14 février 2023 des lignes directrices sur l'articulation entre le champ d'application territorial du RGPD (article 3) et les dispositions relatives aux transferts énoncées au chapitre V<sup>1</sup>. Ces lignes directrices visent à aider les organismes à déterminer si une opération de traitement constitue un transfert et à fournir une interprétation commune de cette notion. Les trois **critères cumulatifs pour considérer qu'un traitement constitue un transfert** sont :

1. le responsable de traitement ou le sous-traitant exportateur de données est soumis au RGPD pour le traitement donné ;
2. l'exportateur transmet ou met les données à caractère personnel à la disposition de l'importateur de données (une autre responsable du traitement, responsable conjoint ou sous-traitant) et
3. l'importateur est dans un pays tiers ou est une organisation internationale, qu'il soit soumis ou non au RGPD.

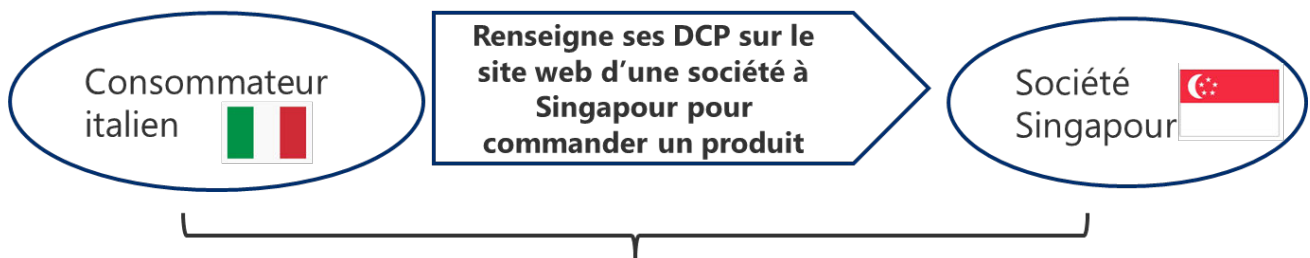
À titre d'exemple, la transmission de données par un organisme responsable de traitement soumis au RGPD vers un sous-traitant fournisseur de services de *cloud* à des fins d'hébergement sur des serveurs dans un pays tiers constitue un transfert de données hors Union européenne. Si l'hébergement est réalisé sur des serveurs situés en Europe, il peut tout de même y avoir des transferts vers des serveurs hors UE gérés par des entités situées dans des pays tiers à des fins de réplication ou de sauvegarde ou vers des équipes localisées dans des pays tiers à des fins de support ou de maintenance.

En revanche, le recours par un responsable de traitement soumis au RGPD à un fournisseur de services de *cloud* soumis à une législation d'un pays tiers qui héberge les données sur le territoire de l'Union européenne ne constitue pas en tant que tel un transfert et le chapitre V du RGPD n'est pas applicable. Toutefois, si le fournisseur communique des données à caractère personnel en réponse à une demande d'accès des autorités du pays tiers en vertu de la législation à laquelle il est soumis, une telle divulgation constitue un transfert en vertu du chapitre V du RGPD.

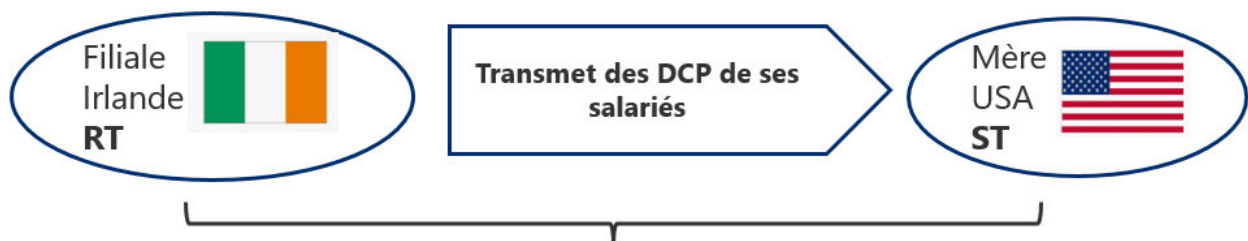
<sup>1</sup> [https://edpb.europa.eu/system/files/2023-02/edpb\\_guidelines\\_05-2021\\_interplay\\_between\\_the\\_application\\_of\\_art3-chapter\\_v\\_of\\_the\\_gdpr\\_v2\\_en\\_o.pdf](https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_o.pdf)

Un autre cas ne constituant pas un transfert est celui d'un salarié qui, à l'occasion d'un déplacement professionnel temporaire hors de l'Union européenne, accède à distance à ses documents professionnels stockés dans le *cloud*. Le CEPD a considéré qu'il ne s'agissait pas ici d'un transfert dans la mesure où le salarié n'est pas une entité distincte de son employeur responsable de traitement.

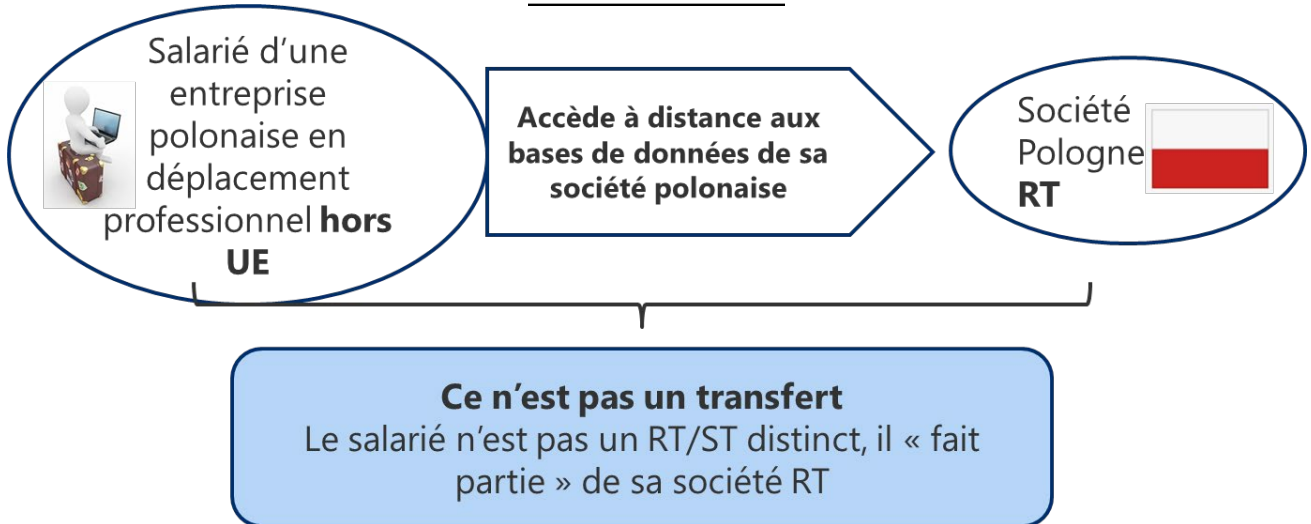
Les schémas ci-dessous présentent différentes situations permettant d'illustrer des situations de transfert ou d'absence de transfert.



**Ce n'est pas un transfert**  
Pas de RT/ST exportateur (données divulguées directement et de sa propre initiative par la personne concernée).  
Attention, la société singapourienne peut être soumise au RGPD en vertu de l'art 3.2



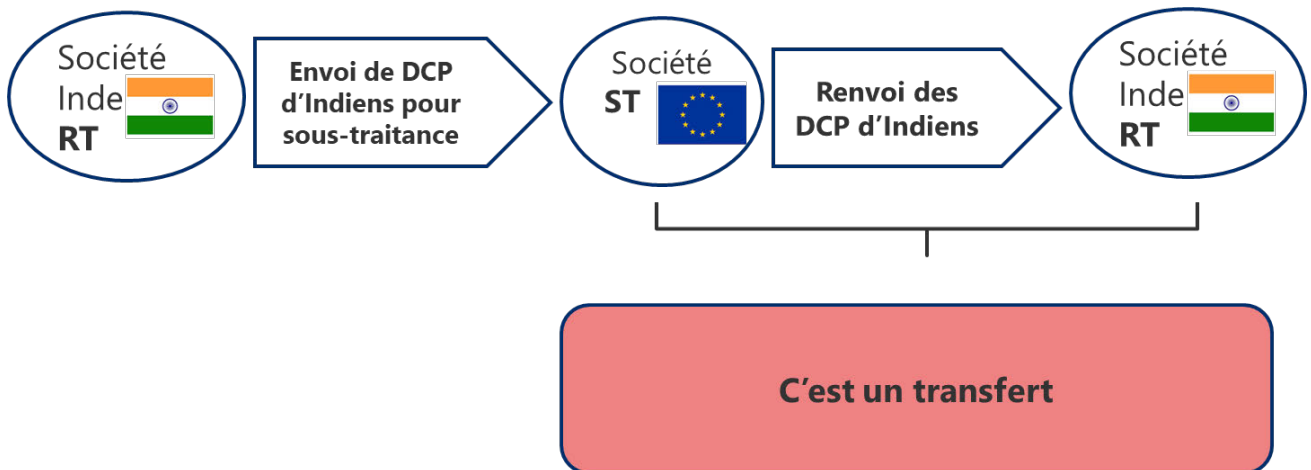
**C'est un transfert**



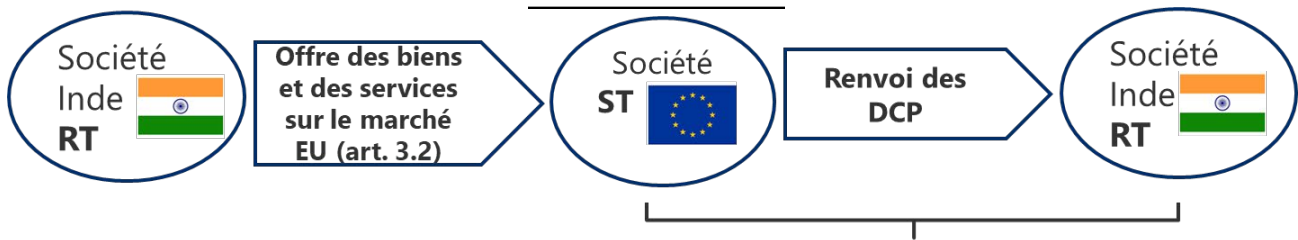
76  
77



78  
79



80  
81



**C'est un transfert**

Les deux entités sont toutes deux soumises au RGPD, la société indienne en vertu de l'art. 3.2 et la société EU en vertu de l'art 3.1

82  
83

## 2. Les décisions d'adéquation

Une décision d'adéquation est une décision adoptée par la Commission européenne fondée sur l'article 45 du RGPD, qui établit qu'un pays tiers ou une organisation internationale assure un niveau de protection adéquat des données à caractère personnel.

Le RGPD prévoit une liste non exhaustive d'éléments qui, cumulés, permettent à la Commission d'évaluer le caractère adéquat du niveau de protection des données du pays tiers. Ces éléments incluent notamment la législation interne du pays, l'existence d'une ou de plusieurs autorités de contrôle indépendantes en matière de protection des données et les engagements internationaux pris par le pays.

Une décision d'adéquation a pour effet de permettre le transfert, sans exigence supplémentaire, de données à caractère personnel par des organismes soumis au RGPD vers le pays tiers concerné. **À ce jour, 15 pays bénéficient d'une décision d'adéquation<sup>2</sup> :** Andorre, Argentine, Canada (volet commercial)<sup>3</sup>, Îles Féroé, Guernesey, Israël, Île de Man, Jersey, Nouvelle-Zélande, Suisse et Uruguay et, depuis l'entrée en application du RGPD, Japon, République de Corée, Royaume-Uni et États-Unis (organismes auto-certifiés).

La Commission est actuellement en phase de **revue des 11 décisions d'adéquation adoptées avant l'entrée en application du RGPD**. Cette revue prendra la forme d'un rapport adressé au Parlement et au Conseil qui contiendra une synthèse des modifications internes (réformes législatives, jurisprudence) depuis l'adoption de la décision d'adéquation. Pour la première fois, les règles en matière d'accès aux données par les gouvernements seront évaluées. Pour chaque pays, le rapport présentera et évaluera les modifications puis conclura sur l'adéquation. Si la conclusion est positive, l'adéquation restera en place. Si elle est négative, une procédure sera alors initiée pour modifier ou retirer la décision. Pour certains pays (par exemple Israël), la Commission a indiqué que des préoccupations ont été identifiées mais des solutions portant sur des garanties additionnelles ont été négociées.

### A. Focus sur l'adéquation des États-Unis

#### a) Rappel du contexte

Le 16 juillet 2020, la CJUE dans son arrêt « Schrems II » a invalidé la précédente décision d'adéquation de la Commission européenne à l'égard des États-Unis (le « Privacy Shield »).

La CJUE a analysé la législation étasunienne alors en vigueur en matière d'accès aux données des fournisseurs de services web et entreprises de télécommunications par les services de renseignement étasuniens (Section 702 FISA et Executive Order n°12333). Elle en a conclu que les atteintes portées à la vie privée des personnes dont les données étaient traitées par les entreprises et opérateurs étasuniens soumis à cette législation étaient disproportionnées au

<sup>2</sup> [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en#adequacy-decisions-latest](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#adequacy-decisions-latest)

<sup>3</sup> Décision d'adéquation applicable uniquement aux traitements couverts par la loi PIPEDA (« *Personal Information Protection and Electronic Documents* ») régissant le traitement des informations personnelles par les organisations sur secteur privé à des fins commerciales.



regard des exigences de la Charte des Droits Fondamentaux européenne. 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 étaient insuffisantes. La CJUE a dès lors invalidé cette décision d'adéquation de la Commission européenne.

En réaction à cette invalidation, le président des États-Unis, Joe Biden, a adopté le 7 octobre 2022, un décret présidentiel (Executive Order n°14086) pour renforcer les garanties concernant la collecte et l'utilisation des données à caractère personnel par les services de renseignement étasuniens.

Sur cette base, le Département du Commerce étasunien a adopté un nouveau cadre transatlantique pour la protection des données à caractère personnel (le « EU-U.S. Data Privacy Framework »).

Ce nouveau cadre transatlantique a été soumis à la Commission européenne afin qu'elle évalue s'il permet d'assurer un niveau de protection adéquat des données des Européens. Avant d'adopter définitivement sa décision reconnaissant le caractère adéquat de ce nouveau dispositif, la Commission a soumis le 13 décembre 2022 un projet de décision pour avis au CEPD.

Le 28 février 2023, le CEPD a adopté et publié son avis sur ce projet d'adéquation. Le CEPD y relève les améliorations apportées par le gouvernement des États-Unis, tout en faisant part de ses préoccupations sur un certain nombre de points dont il dresse la liste.

#### **b) Éléments clés du nouveau cadre**

Le cadre de protection des données UE-États-Unis est composé d'un nouvel ensemble de règles et de garanties contraignantes pour limiter l'accès aux données à caractère personnel par les autorités de renseignement étasuniennes à ce qui est nécessaire et proportionné pour protéger la sécurité nationale.

#### **Le système d'auto-certification des entités important des données**

Comme dans le précédent cadre de protection des données UE-États-Unis (le « Privacy Shield »), **un système d'auto-certification des entités étasuniennes** est mis en place. Une fois inscrites sur la liste des organismes certifiés, ces dernières s'engagent annuellement et publiquement à adhérer à ce cadre légal et à en respecter l'ensemble des principes. Des garanties similaires à celles de l'UE sont prévues, telle que la limitation de la finalité, c'est-à-dire l'obligation de supprimer les données qui ne seraient plus nécessaires à la finalité de collecte. En cas de partage des données européennes à un tiers, la continuité de leur protection devra également être assurée.

**Seuls les transferts vers les entités étasuniennes certifiées ne nécessitent pas l'utilisation d'outils d'encadrement des transferts prévus par l'article 46 du RGPD.** Pour les transferts de données vers d'autres entités que celles certifiées, des garanties appropriées doivent être fournies et ces transferts ne sont possibles qu'à condition de garantir des droits opposables aux personnes concernées ainsi que des voies de recours effectives.



## Le décret présidentiel n°14086

**Un des éléments clés de ce cadre** est le décret présidentiel étasunien n°14086 qui a pour objet de renforcer la protection des données à caractère personnel traitées par les services de renseignement étasuniens, en :

- consacrant les principes de nécessité et de proportionnalité dans le cadre de l'accès des autorités étasuniennes aux données ; et
- introduisant un nouveau mécanisme de recours indépendant et impartial auprès d'une Cour de contrôle de la protection des données.

### c) Conséquences pour les organismes souhaitant transférer des données vers les États-Unis

La Commission européenne ayant constaté que les États-Unis assurent un niveau de protection substantiellement équivalent à celui de l'UE, les organismes soumis au RGPD (qu'ils soient responsables de traitement ou sous-traitants) peuvent désormais transférer des données à caractère personnel vers les organismes certifiés qui se sont engagés, annuellement et publiquement, à adhérer à ce cadre légal. Ils n'ont pas l'obligation de mettre en place un outil de transfert au titre de l'article 46 du RGPD ou de se prévaloir d'une dérogation au titre de l'article 49 du RGPD.

Avant de procéder au transfert, les organismes doivent s'assurer que l'organisme destinataire figure sur une liste mise à disposition sur le site du Département du Commerce des États-Unis<sup>4</sup>.

Les organismes certifiés sur la base du Privacy Shield et qui avaient maintenu cette certification même après l'invalidation de la décision d'adéquation ont été automatiquement inscrits sur la nouvelle liste. Ils ont trois mois pour mettre à jour leur Politique de Confidentialité (jusqu'au 10 octobre 2023)<sup>5</sup>. Néanmoins, les transferts vers ces organismes peuvent bénéficier immédiatement de la décision d'adéquation, dans la mesure où les principes de protection des données à caractère personnel sont restés les mêmes que précédemment, combinés au cadre de protection renforcé offert par le décret présidentiel.

Les responsables du traitement et les sous-traitants réalisant des transferts vers des organismes auto-certifiés au titre de la décision d'adéquation doivent par ailleurs se conformer à d'autres obligations découlant du RGPD, notamment en ce qui concerne la nécessité de mettre à jour leurs registres de traitement et l'information des personnes concernées des transferts vers les États-Unis.

Les transferts vers des entités étasuniennes ne figurant pas sur la liste du Département du Commerce ne peuvent pas être fondés sur la décision d'adéquation et nécessitent des garanties appropriées prévues par l'article 46 du RGPD. Il est cependant important de souligner que les garanties mises en place par le gouvernement étasunien via le décret présidentiel dans le domaine de la sécurité nationale (y compris le mécanisme de recours) s'appliquent à tous les transferts de données effectués par des entités publiques ou privées

<sup>4</sup> <https://www.dataprivacyframework.gov/s/participant-search>

<sup>5</sup> Annex I, Section III (Supplemental Principles), 6.e de la décision d'adéquation de la Commission européenne.

soumises au RGPD vers des entreprises situées aux États-Unis. Elles sont donc applicables quel que soit l'outil de transfert utilisé (clauses contractuelles types ou règles d'entreprise contraignantes, notamment).

## **B. Application de l'article 48 du RGPD à des fournisseurs soumis à des lois extra-européennes autorisant les demandes d'accès par des autorités publiques de pays tiers**

Des lignes directrices sur l'article 48 sont actuellement en cours d'élaboration par le CEPD

[REDACTED] dont l'objectif est de clarifier son champ d'application dans le cadre de demandes d'accès adressées à des destinataires dans l'UE à des fins répressives et de sécurité nationale.

Même en l'absence de transfert de données à caractère personnel hors UE, une société soumise à la législation d'un pays tiers peut faire l'objet d'injonctions des autorités publiques de ce pays l'obligeant à leur transférer des données stockées et traitées sur le territoire de l'Union européenne.

Cette situation a été spécifiquement couverte par l'article 48 du RGPD qui prévoit 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, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre* ». Une demande d'un juge ou d'une autorité administrative d'un pays tiers ne peut donc être exécutoire que s'il existe un cadre juridique spécifique en place convenu entre les deux pays (comme un traité d'entraide judiciaire).

De telles demandes de transmission d'information peuvent ainsi être fondées sur :

- des traités d'entraide judiciaire, une juridiction étrangère demandant communication d'information ou de document et pouvant être revêtue d'un exequatur en Europe ;
- des traités de coopération pénale ; on peut également signaler le deuxième protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest<sup>7</sup>) mais qui n'est pas encore applicable car en cours de ratification ;
- des traités de coopération fiscale qui prévoient la communication de renseignements d'une administration fiscale à une autre : si la décision est « reconnue » par

<sup>6</sup> [REDACTED]

<sup>7</sup> Ce protocole a pour objectif d'améliorer l'accès transfrontière aux preuves électroniques à utiliser dans le cadre des procédures pénales. Il contribuera à la lutte contre la cybercriminalité et d'autres formes de criminalité au niveau mondial en facilitant la coopération entre les États membres et les pays tiers, tout en assurant un niveau élevé de protection des personnes et en veillant au respect des normes de l'UE en matière de protection des données. Le protocole prévoit des procédures visant à améliorer la coopération internationale entre autorités ainsi qu'à renforcer la coopération directe avec les fournisseurs de services et les entités situés dans d'autres pays. Il définit également des procédures relatives à la demande d'entraide judiciaire urgente.

l'administration européenne, dans le cadre du traité, elle communique les données demandées.

De tels traités doivent d'ailleurs eux-mêmes être conformes aux exigences du RGPD et de la jurisprudence de la CJUE.

En revanche, en dehors d'actions de coopération entre États (telles que visées ci-dessus), il n'existe évidemment pas de traités prévoyant que des services de renseignement d'États étrangers puissent demander aux sociétés relevant de leurs lois nationales ayant des établissements en Europe de leur communiquer des données personnelles d'Européens (d'ailleurs généralement sans en informer les autorités européennes). Et il n'en existera probablement jamais.

Ce risque de divulgation non autorisé par le droit de l'Union a d'ailleurs été confirmé par le Conseil d'État dans son ordonnance du 13 octobre 2020 concernant le dossier HDH précisant qu'« (...) il résulte de l'instruction que les mesures techniques mises en œuvre par Microsoft ou susceptibles de l'être à brève échéance n'écartent pas toute possibilité pour cette entreprise d'accéder aux données traitées sous la responsabilité de la Plateforme des données de santé, en dépit des précautions, limitant ce risque, qui entourent le chiffrement dont elles font l'objet et le stockage des clés de chiffrement utilisées. **Il ne peut ainsi être totalement exclu, sur le plan technique, que Microsoft soit amenée à faire droit à une demande des autorités américaines fondée sur l'article 702 du FISA, ce qui méconnaîtrait alors les articles 28 et 48 du règlement général sur la protection des données (...)** ».

La question se pose de savoir quelles sont les conséquences de la récente adéquation des États-Unis sur l'application de cet article 48. Plus précisément, les nouvelles garanties apportées par le droit étasunien permettent-elles de conclure à la conformité des réponses aux demandes d'accès des autorités étasuniennes aux données situées dans l'UE sur le fondement de l'article 48 ? Si tel n'est pas le cas, comment appliquer l'article 48 sans toutefois empêcher tout recours à des opérateurs non soumis à une législation d'un pays tiers ?

[REDACTED]

[REDACTED]

303

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

346

[REDACTED]

[REDACTED]

[REDACTED]

368

[REDACTED]

386

387

388

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



### 3. Les garanties appropriées

#### A. Présentation des garanties

L'article 46 prévoit différents outils pour encadrer les transferts de données vers des entités situées dans des pays non adéquats.

- **Clauses contractuelles types (CCT) de la Commission européenne**

Les clauses contractuelles types sont des modèles de clauses encadrant le transfert de données à caractère personnel et adoptés par la Commission européenne. Leur conclusion ne nécessite pas d'autorisation d'une autorité de contrôle.

Les modèles de clauses contractuelles ont été mis à jour par la Commission européenne le 4 juin 2021. Elles combinent des clauses générales avec une approche « par modules » pour répondre à divers scénarios de transfert.

- module 1 : transfert de responsable de traitement à responsable de traitement ;
- module 2 : transfert de responsable de traitement à sous-traitant ;
- module 3 : transfert de sous-traitant à sous-traitant ;
- module 4 : transfert de sous-traitant à responsable de traitement

Les clauses contractuelles types intègrent la jurisprudence « Schrems II » de la CJUE en imposant à l'exportateur de tenir compte de la législation applicable à l'importateur pour déterminer si les clauses contractuelles types pourront produire tous leurs effets.

Il convient de noter qu'elles ne peuvent pas être utilisées si l'importateur dans le pays tiers est soumis au RGPD en vertu de l'article 3.2 du RGPD. La Commission a annoncé travailler à l'élaboration de clauses « allégées » pour couvrir cette situation afin de tenir compte des exigences qui s'appliquent déjà directement à ces organismes soumis au RGPD.

- **Règles internes d'entreprises (BCR)**

Il existe des BCR « responsable du traitement » et « sous-traitant ». Le nouveau référentiel BCR « responsable du traitement » mis à jour a été approuvé par le CEPD le 20 juin 2023. Les travaux de mise à jour du référentiel BCR « sous-traitant » ont démarré au sein du CEPD. *Pour plus d'informations, il est renvoyé au le point d'actualité relatif aux dossiers BCR présenté en séance plénière le 12 janvier 2023*

- **Clauses contractuelles types adoptées par une autorité de contrôle et approuvées par la Commission européenne** (*pas de clauses adoptées à ce jour*)
- **Code de conduite** approuvé comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE (importateurs) d'appliquer les garanties appropriées

Le 22 février 2022, le CEPD a adopté des lignes directrices sur les codes de conduite en tant qu'outils de transfert<sup>11</sup>. Le principal objectif des lignes directrices est de clarifier l'application de l'article 40, paragraphe 3, et de l'article 46, paragraphe 2, point e), du RGPD. Ces dispositions prévoient qu'une fois approuvé par une autorité de contrôle compétente et après

<sup>11</sup> [https://edpb.europa.eu/system/files/2022/10/edpb\\_guidelines\\_codes\\_conduct\\_transfers\\_after\\_public\\_consultation\\_fr.pdf](https://edpb.europa.eu/system/files/2022/10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_fr.pdf)

s'être vu accorder une validité générale au sein de l'EEE par la Commission, un code de conduite peut être adopté et utilisé par les responsables du traitement et les sous-traitants qui ne sont pas soumis au RGPD afin de fournir des garanties appropriées pour les transferts de données en dehors de l'UE.

À ce jour, aucun code de conduite en tant qu'outil de transfert n'a été approuvé<sup>12</sup>.

Il convient de noter qu'un code de conduite en tant qu'outil de transfert est différent d'un code de conduite « RGPD » au sens de l'article 40.2 du RGPD dont l'objectif est de démontrer la conformité de ses adhérents au RGPD<sup>13</sup>. Même si le code de conduite « RGPD » contient des éléments sur la conformité des transferts de données effectués par ses adhérents en tant qu'exportateurs, il ne constitue pas pour autant un outil de transfert.

- **Mécanisme de certification approuvé** comportant l'engagement contraignant et exécutoire pris par les importateurs hors UE d'appliquer les garanties appropriées

Le 14 février 2023, le CEPD a adopté des lignes directrices sur la certification en tant qu'outil de transfert<sup>14</sup>. L'article 46, paragraphe 2, point f), du RGPD introduit des mécanismes de certification approuvés en tant que nouvel outil permettant de transférer des données à caractère personnel vers des pays tiers en l'absence d'accord d'adéquation. L'objectif principal de ces lignes directrices est de fournir des précisions sur l'utilisation pratique de cet outil de transfert.

À ce jour, aucune certification n'a été approuvée en tant qu'outil de transfert. Toutefois, un organisme a soumis un projet à l'autorité luxembourgeoise.

De la même manière que pour les codes de conduite, les certifications outil de transfert sont à distinguer des certifications « RGPD » au sens de l'article 42.1 du RGPD dont l'objectif est de démontrer la conformité des organismes certifiés au RGPD, y compris pour les transferts pour lesquels ils sont exportateurs<sup>15</sup>. En revanche, et conformément à l'article 42.2 du RGPD, les certifications outil de transfert sont destinées aux **organismes qui ne sont pas soumis au RGPD** et donc aux importateurs de données hors UE qui peuvent ainsi être certifiées pour les données qu'ils reçoivent dans le cadre de transferts de leurs clients soumis au RGPD.

<sup>12</sup> À ce jour, un organisme a contacté la CNIL pour un projet de code de conduite comme outil de transfert mais les échanges sont à ce stade préliminaire et aucun projet n'a été adressé formellement à la CNIL.

<sup>13</sup> En 2021, la CNIL a approuvé son premier code de conduite, le code européen porté par CISPE (Cloud Infrastructure Service Providers Europe) à destination des fournisseurs de services d'infrastructures informatiques en nuage (« cloud ») situés sur le territoire de l'Union européenne, de façon quasi simultanée avec l'approbation par l'autorité belge du Code européen « EU CLOUD CoC ». Au niveau européen, quatre codes nationaux et deux codes européens ont été approuvés à ce jour depuis l'entrée en vigueur du RGPD. Actuellement, les services de la CNIL accompagnent les porteurs de trois projets de codes de conduite européens et quatre projets nationaux dans différents secteurs d'activités.

<sup>14</sup> [https://edpb.europa.eu/system/files/2023-05/edpb\\_guidelines\\_07-2022\\_on\\_certification\\_as\\_a\\_tool\\_for\\_transfers\\_v2\\_fr\\_0.pdf](https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_fr_0.pdf)

<sup>15</sup> A ce jour, trois certifications « RGPD » ont été approuvées dont une seule s'applique en France car européenne (EuroPrivacy). Ces certifications sont toutes « généralistes », c'est-à-dire non spécifiques au secteur du *cloud* mais rien n'empêche un fournisseur de services de *cloud* d'y candidater. Huit projets de certifications sont en cours d'examen.



- **Arrangement administratif** entre les autorités ou les organismes publics qui prévoit des droits opposables et effectifs pour les personnes concernées

Le 21 mars 2019, la CNIL a autorisé la mise en œuvre d'un arrangement administratif visant à encadrer les transferts des données à caractère personnel entre l'autorité des marchés financiers (AMF) et ses homologues en dehors de l'EEE.

Le 18 mars 2021, la CNIL a autorisé la mise en œuvre d'un arrangement administratif visant à encadrer les transferts des données à caractère personnel entre le Haut Conseil du Commissariat aux comptes (H3C) et son homologue étasunien, le *Public Company Accounting Oversight Board* (PCAOB).

## B. Analyse d'impact sur les transferts

Dans son arrêt dit « Schrems II », la CJUE a souligné la responsabilité des exportateurs et importateurs de garantir que le traitement des données à caractère personnel se fait, et continue à se faire, dans le respect du niveau de protection fixé par la législation européenne. Selon la Cour, les exportateurs ont également la responsabilité de suspendre le transfert, et/ou de résilier le contrat si l'importateur n'est pas, ou n'est plus en mesure de respecter ses engagements en matière de protection des données à caractère personnel. Ainsi, les exportateurs s'appuyant sur les instruments de l'article 46 du RGPD pour leurs transferts de données à caractère personnel ont l'obligation d'évaluer le niveau de protection dans les pays tiers de destination. Une telle évaluation est communément appelée « *Transfer Impact Assessment* » ou « TIA » (« analyse d'impact des transferts » en français).

*Pour plus d'éléments sur ce sujet, votre rapporteur renvoie au guide d'analyse d'impact sur les transferts présenté en séance plénière le 14 septembre 2023.*

## 4. Les dérogations

Lorsqu'un pays tiers n'est pas reconnu comme offrant un niveau de protection adéquat et en l'absence de garanties appropriées encadrant ce transfert, le transfert peut néanmoins, par exception, être opéré dans les conditions prévues par l'article 49.1 du RGPD. Cet article prévoit notamment le cas dans lequel la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle ou lorsque le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale. Ces dérogations sont soumises à des conditions particulières, d'interprétation stricte, détaillées à l'article 49 du RGPD.

Le RGPD prévoit enfin, lorsqu'aucune de ces dérogations n'est applicable, la possibilité de procéder au transfert s'il ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. Le 25 mai 2018, le CEPD a adopté des lignes directrices sur l'interprétation de l'article 49 du RGPD qui établissent sa doctrine sur ces dérogations réservées à des situations particulières<sup>16</sup>.

<sup>16</sup> [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_2\\_2018\\_derogations\\_fr.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf)

538 **5. Possibilités liées à l'article 9.4 du RGPD**

539 Cet article permet aux États membres de maintenir ou d'introduire des conditions  
540 supplémentaires, y compris des limitations, en ce qui concerne le traitement des données  
541 génétiques, des données biométriques ou des données concernant la santé.  
542

546  
547