GUIDE PRATIQUE

ANALYSE D'IMPACT DES TRANSFERTS DE DONNÉES

Version finale

Janvier 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

1. Introduction

1.1 Contexte

Quels que soient leur statut (public ou privé, à but lucratif ou non lucratif) et leur taille (entreprises multinationales ou petites et moyennes entreprises, collectivités territoriales, administrations centrales, artisans ou professions libérales), un très grand nombre de responsables de traitement et sous-traitants est concerné par la question des transferts de données hors de l'Espace économique européen[1] (EEE). En effet, l'interpénétration des réseaux et le développement de services transfrontaliers, en particulier avec l'informatique en nuage, ont multiplié les situations dans lesquelles des données à caractère personnel (parfois désignées ci-après simplement par « données ») sont traitées en tout ou partie dans des pays tiers qui ne sont pas soumis au droit de l'Union européenne, en particulier au Règlement général sur la protection des données[2] (RGPD) et peuvent ainsi donner lieu à des transferts.

Le principe institué par le RGPD est qu'en cas de transfert, les données doivent continuer à bénéficier d'une protection substantiellement équivalente à celle offerte par ce texte. En effet, le considérant 101 du RGPD souligne qu' « il importe que, lorsque des données à caractère personnel sont transférées de l'Union à des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas compromis ». Le chapitre V du RGPD comporte des dispositions spécifiques concernant les transferts de données.

Dans son arrêt dit « Schrems II »[3], la Cour de justice de l'Union européenne (CJUE) a souligné la responsabilité des exportateurs et importateurs[4] 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 de l'Union européenne en matière de protection des données. 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 outils de transferts énumérés à 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 et la nécessité de mettre en place des mesures supplémentaires. **Une telle évaluation est appelée « *Analyse d'impact des transferts de données* » ou « AITD » en français.**

1.2 L'objectif de l'AITD

Une **AITD doit être réalisée par l'exportateur soumis au RGPD, qu'il soit responsable de traitement ou sous-traitant, avec l'assistance de l'importateur, avant de transférer les données vers un pays tiers hors de l'EEE lorsque ce transfert s'appuie sur un outil de l'article 46 du RGPD**. Si le pays de destination est couvert par une décision d'adéquation de la Commission européenne, l'exportateur n'est pas soumis à cette obligation. L'exportateur n'a pas non

---

[1] L'Espace économique européen (EEE) est constitué des États membres de l'Union européenne et de la Norvège, de l'Islande et du Liechtenstein dans lesquels le RGPD est devenu applicable par incorporation à l'Accord EEE.

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[3] Arrêt de la Cour de justice de l'Union européenne du 16 juillet 2020, « Schrems II », C-311/18 : https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=3086778

[4] Selon la définition du CEPD, un « **exportateur** » est un responsable de traitement, responsable conjoint de traitement ou sous-traitant soumis au RGPD pour un traitement, qui communique par transmission ou rend accessible par un autre moyen les données à caractère personnel en cause à un « **l'importateur** », responsable de traitement, responsable conjoint de traitement ou sous-traitant qui se trouve dans un pays tiers (hors Espace économique européen (EEE)), qu'il soit ou non soumis au RGPD pour le traitement en cause conformément à l'article 3, ou qu'il soit une organisation internationale. Voir CEPD, Lignes Directrices 05/2021 sur l'interaction entre l'application de l'article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD : https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_fr.pdf

plus à réaliser une AITD, si le transfert est effectué sur la base d'une des dérogations listées à l'article 49 du RGPD.

L'objectif d'une AITD est d'**évaluer si l'importateur pourra respecter ses obligations telles que prévues par l'outil choisi** compte tenu de la législation et des pratiques du pays tiers de destination - en particulier en ce qui concerne le potentiel accès aux données à caractère personnel par des autorités du pays tiers - et de documenter cette évaluation. À cette fin, l'exportateur doit évaluer le niveau de protection offert par la législation locale et tenir compte des pratiques des autorités dans le pays tiers au vu du transfert envisagé. En cas de nécessité, l'AITD doit également permettre d'évaluer si des mesures supplémentaires permettraient de combler les lacunes constatées dans la protection des données et d'assurer le niveau requis par la législation de l'Union européenne.

1.3 L'objectif du présent guide

Dans la continuité des recommandations du Comité européen de la protection des données (CEPD) sur les mesures supplémentaires complétant les outils de transferts[5], la CNIL a élaboré le présent guide pour les exportateurs, afin de les aider à réaliser leur AITD.

Ce guide constitue une méthodologie qui identifie les étapes préalables à la réalisation d'une AITD et les différents éléments à prendre en compte lors de la réalisation d'une AITD. Il donne des indications sur la manière dont l'analyse peut être menée en suivant les étapes établies dans les recommandations du CEPD et renvoie vers la documentation pertinente. Il ne constitue pas une évaluation des législations et pratiques des pays tiers.

L'utilisation de ce guide n'est pas obligatoire, d'autres éléments peuvent également être pris en compte et d'autres méthodologies appliquées.

Pour ce qui est des étapes préalables à la réalisation d'une AITD (section 2), ce guide s'organise autour des questions suivantes :

i. Existence d'un transfert de données à caractère personnel
ii. Nécessité de réaliser une AITD
iii. Responsabilité de réaliser l'AITD
iv. Périmètre de l'AITD, en particulier prise en compte des transferts ultérieurs
v. Conformité aux principes du RGPD

Pour ce qui est de la réalisation de l'AITD (section 3), ce guide s'organise suivant les six différentes étapes à suivre pour mener une AITD telles que recommandées par le CEPD :

1. Connaître son transfert
2. Identifier l'outil de transfert utilisé
3. Évaluer la législation et les pratiques du pays de destination des données et l'efficacité de l'outil de transfert
4. Recenser et adopter des mesures supplémentaires
5. Mettre en œuvre les mesures supplémentaires
6. Réévaluer à intervalles appropriés le niveau de protection et suivre les développements potentiels qui pourraient l'affecter

[5] 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 (version 2.0) (PDF, 658 ko), CEPD : https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_fr.pdf

L'**étape 1** permet à l'exportateur de **décrire le transfert**.

L'**étape 2** consiste à **documenter l'outil qui sera utilisé pour encadrer le transfert** décrit et l'analyse concluant à la nécessité ou non de réaliser une AITD.

L'**étape 3** permet à l'exportateur d'**évaluer la législation et les pratiques en vigueur dans le pays de destination** des données et d'identifier si des éléments sont susceptibles de porter atteinte à l'efficacité des garanties apportées via l'outil de transfert utilisé (documenté à l'étape 2).

L'**étape 4** consiste à **recenser les mesures de sécurité** (techniques, contractuelles et organisationnelles) existantes qui permettent d'assurer un niveau de protection des données suffisant dans le pays tiers, en tenant compte du transfert (décrit à l'étape 1) et de l'évaluation de la législation et des pratiques du pays tiers (étape 3). Si ces mesures ne sont pas satisfaisantes, l'exportateur **identifie les mesures supplémentaires qui doivent être mises en œuvre** pour assurer que les données transférées jouissent dans le pays tiers d'un niveau de protection essentiellement équivalent à celui au sein de l'EEE.

L'**étape 5** contient un modèle de **plan d'action** pour la mise en œuvre opérationnelle des mesures supplémentaires identifiées et des éventuelles étapes procédurales dans l'étape 4.

Enfin, l'**étape 6** permet d'anticiper les **futures réévaluations** du transfert par l'exportateur.

La description du transfert (dans l'étape 1) et l'identification de l'outil de transfert (dans l'étape 2) permettent la prise en compte des caractéristiques et de la sensibilité du transfert dans l'évaluation de la législation et des pratiques du pays de destination des données et de l'efficacité de l'outil de transfert (à l'étape 3) en vue de la mise en place d'éventuelles mesures supplémentaires (à l'étape 4).

2. Avant de réaliser une analyse d'impact des transferts de données

Avant de réaliser une AITD, plusieurs éléments doivent être vérifiés. Il est préconisé de documenter l'analyse.

2.1 Existence d'un transfert de données à caractère personnel

Avant toute autre chose, il est nécessaire de s'assurer que :

- **Les données en cause sont des données à caractère personnel**

L'article 4(1) du RGPD définit comme donnée à caractère personnel *« toute information se rapportant à une personne physique identifiée ou identifiable »*, une personne physique identifiable étant « *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » [6].

- **Un transfert de données à caractère personnel est réalisé**

Dans ses lignes directrices[7], le CEPD a identifié les trois critères cumulatifs suivants pour établir si un traitement peut être qualifié de transfert :

1) Un responsable de traitement, responsable conjoint de traitement ou un sous-traitant (« l'exportateur ») est soumis au RGPD pour le traitement en cause ;

[6] Voir par exemple les différentes ressources du site de la CNIL :
- « Donnée personnelle » : https://www.cnil.fr/fr/definition/donnee-personnelle
- « Identifier les données personnelles » : https://www.cnil.fr/fr/identifier-les-donnees-personnelles

[7] Voir lignes directrices 05/2021 du CEPD sur l'interaction entre l'application de l'article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD, CEPD : https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_fr.pdf

2) L'exportateur divulgue par transmission ou met d'une autre manière les données à caractère personnel en cause à disposition d'une autre entité (« l'importateur »), qu'elle soit responsable de traitement, responsable conjoint de traitement ou sous-traitant ;

3) L'importateur est dans un pays tiers (hors EEE), qu'il soit ou non soumis au RGPD pour le traitement en cause conformément à l'Article 3, ou qu'il soit une organisation internationale.

Comme le rappelle le CEPD[8], la notion de « transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale » ne s'applique qu'à la divulgation de données à caractère personnel faisant intervenir deux entités juridiquement distinctes (chacune d'elles étant un responsable du traitement, un responsable conjoint du traitement ou un sous-traitant). Le chapitre V du RGPD ne s'applique donc pas aux transmissions ou mises à disposition de données à l'intérieur d'une même entité. Cela signifie que lorsqu'un employé d'un responsable de traitement dans l'UE accède à distance à une base de données de son employeur depuis un pays tiers, durant un voyage d'affaires par exemple, cela ne constitue pas un transfert au sens du RGPD.

En revanche, la transmission ou mise à disposition de données entre deux entités distinctes appartenant à un même groupe peut constituer un transfert[9].

L'accès à distance depuis un pays tiers à des données stockées dans l'EEE et le stockage en nuage de données hors de l'EEE constituent un transfert lorsque ces activités sont réalisées par une entité juridiquement différente de celle de l'exportateur.

2.2 Nécessité de réaliser une AITD

Une AITD doit être réalisée avant de transférer les données vers un pays tiers lorsque ce transfert s'appuie sur un outil de l'article 46 du RGPD. Par exemple, cela concerne les données transférées sur la base de clauses contractuelles types de la Commission européenne[10] ou des règles d'entreprise contraignantes (ou *Binding Corporate Rules* (*BCR*) en anglais)[11].

A contrario, il n'est pas nécessaire de réaliser une AITD quand :

➢ Le transfert est vers un pays qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat

Les transferts de données à caractère personnel vers des pays qui ont été reconnus par la Commission européenne comme offrant un niveau de protection adéquat[12] ne nécessitent pas de mettre en place des outils de transfert des données du chapitre V du RGPD ou des mesures supplémentaires. Si le transfert de données à caractère personnel s'effectue vers un tel pays, un niveau de protection adéquat pour les données en cause est assuré. **Dans ce cas, il n'est pas nécessaire de réaliser une AITD**.

Comme le rappelle le CEPD dans son avis 22/2024, pour ces pays adéquats, la Commission a déjà pris en compte : les règles relatives aux transferts ultérieurs de données vers un autre pays tiers ou une organisation internationale, la jurisprudence, ainsi que les droits effectifs et exécutoires des personnes concernées et les voies de recours administratives et judiciaires effectives pour les personnes concernées[13].

---

[8] *ibid.*, §20.
[9] *ibid.*, §21.
[10] « Transfert de données : les clauses contractuelles types (CCT) de la Commission européenne », 8 février 2016, CNIL : https://www.cnil.fr/fr/transfert-de-donnees-les-clauses-contractuelles-types-cct-de-la-commission-europeenne
[11] « Les règles d'entreprise contraignantes (BCR) », CNIL : https://www.cnil.fr/fr/les-outils-de-la-conformite/les-regles-dentreprise-contraignantes-bcr
[12] Pour la liste complète des pays ayant fait l'objet de telles décisions, voir « *Adequacy decisions* » [en anglais], Commission européenne : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[13] *Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)*, §92-93, [en anglais] (PDF, 653 ko), CEPD : https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf

Les décisions d'adéquation peuvent avoir un champ d'application limité (par exemple, la décision d'adéquation du Canada vise uniquement les organisations du secteur privé qui traitent des données à caractère personnel dans le cadre d'activités commerciales[14] et la décision d'adéquation du Japon ne concerne pas les données à caractère personnel transférées aux organismes de radiodiffusion, aux éditeurs de journaux, aux agences de communication ou à d'autres organes de presse, aux personnes exerçant une activité de rédaction professionnelle, aux universités, aux institutions religieuses et aux organismes politiques[15]) ou ne concernent que certaines entités certifiées dans le pays concerné (par exemple, les entités certifiées dans le cadre de la décision d'adéquation visant les États-Unis[16]). Lorsque le transfert de données n'entre pas dans le champ d'application d'une décision d'adéquation, il est nécessaire de recourir à l'un des outils de l'article 46 ou de s'appuyer sur une dérogation de l'article 49. Dans le premier cas, il est nécessaire de faire une AITD.

Les décisions d'adéquation sont soumises à des examens périodiques. Il est donc recommandé de vérifier régulièrement la liste des pays ayant fait l'objet d'une décision d'adéquation au cas où de nouvelles décisions auraient été adoptées ou que des pays aient été retirés de la liste.

➢ Le transfert est basé sur une des dérogations de l'article 49

La réalisation d'une AITD ne sera nécessaire que lorsque l'un des outils de l'article 46 est utilisé. Par conséquent, les transferts fondés sur une des dérogations de l'article 49 peuvent être effectués sans formalité autre que le respect des conditions de leur application prévues par cet article.

Comme le souligne le CEPD dans ses recommandations sur les mesures supplémentaires/sur les dérogations, « ce n'est que dans certains cas que l'exportateur peut invoquer l'une des dérogations prévues à l'article 49 du RGPD, pour autant qu'il remplisse les conditions requises. Les dérogations ne peuvent pas devenir « la règle » dans la pratique, mais doivent être limitées à des situations particulières »[17].

2.3 Qualification des parties et responsabilité de réaliser une AITD

La qualification (responsable de traitement, responsable conjoint de traitement ou sous-traitant[18]) des différentes entités impliquées dans le transfert doit être identifiée, car elle détermine l'allocation des responsabilités et entraine des obligations différentes pour les parties. Le CEPD a produit des lignes directrices[19] dédiées à ces concepts. Des éléments sont également disponibles sur le site de la CNIL[20].

L'AITD doit être réalisée par l'exportateur, qu'il agisse en tant que responsable de traitement ou sous-traitant, avec l'assistance de l'importateur. En effet, il incombe en premier lieu à l'exportateur de veiller à ce que les données transférées bénéficient dans le pays tiers d'un niveau de protection essentiellement équivalent à celui garanti au sein de l'EEE et par conséquent de réaliser l'AITD. Néanmoins, l'importateur disposant de nombreuses informations nécessaires à cette évaluation et, en particulier,

---

[14] Commission européenne, Décision 2002/2/CE du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32002D0002

[15] Commission européenne, Décision d'exécution 2019/419 du 23 janvier 2019 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu de la loi sur la protection des informations à caractère personnel, article premier, EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32019D0419

[16] Commission européenne, Décision d'exécution (UE) 2023/1795 du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis, EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023D1795.
Pour le cas particulier des Etats-Unis, il est recommandé de consulter la page dédiée « Adéquation des États-Unis : les premières questions-réponses de la CNIL », CNIL : https://www.cnil.fr/fr/adequation-des-etats-unis-les-premieres-questions-reponses.

[17] CEPD, Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, p.4

[18] Responsable du traitement (ou responsable conjoint) : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (voir article 4(7) & (8) du RGPD).

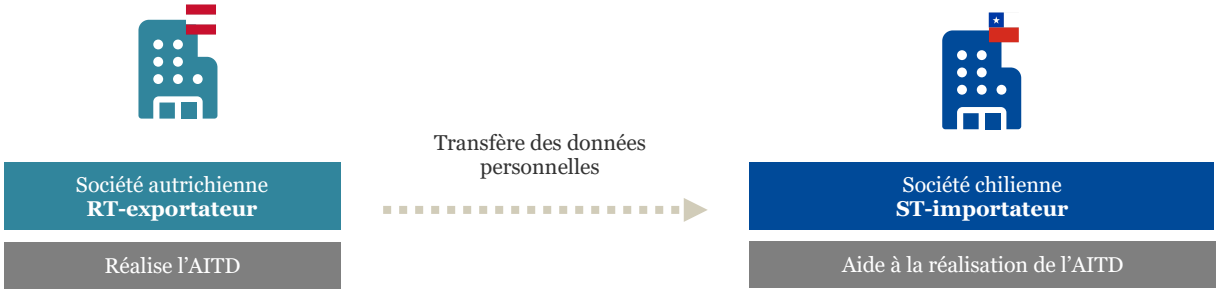
[19] Voir *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD* (PDF, 1, 58 Mo), CEPD :
https://www.edpb.europa.eu/system/files_en?file=2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf

[20] Voir par exemple « Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles », 8 juillet 2020, CNIL, : https://www.cnil.fr/fr/responsable-de-traitement-et-sous-traitant-6-bonnes-pratiques-pour-respecter-les-donnees.

d'une connaissance de la législation du pays où il est localisé, sa coopération est indispensable à la réalisation de l'AITD.

On peut distinguer plusieurs cas en fonction du rôle des parties dans le traitement et de leur qualification :

Cas 1 - Responsable de traitement dans l'EEE agissant en tant qu'exportateur transférant des données vers un sous-traitant agissant en tant qu'importateur dans un pays tiers :



Le responsable de traitement est tenu de réaliser l'AITD avec la collaboration du sous-traitant. En effet, dans le cadre d'une relation de sous-traitance, en vertu de l'article 28(3)(h) du RGPD, le sous-traitant est tenu de transmettre au responsable de traitement les informations permettant de démontrer le respect des obligations qui lui incombent[21]. Ces informations pourront contenir toute information utile permettant au responsable de traitement de réaliser l'analyse de la législation locale et des pratiques, notamment des autorités publiques en matière d'accès.

Les éléments concrets sur la législation et les pratiques des autorités peuvent inclure, selon le cas, des rapports sur l'accès aux données transférées depuis l'EEE par les autorités du pays tiers, des rapports sur les demandes d'accès reçues par le passé par l'importateur des données ou par son sous-traitant ou par des acteurs du même secteur d'activité, des informations sur la législation du pays tiers avec des traductions dans la langue de travail des parties ou bien des informations par les autorités compétentes sur le traitement des recours lorsque ces recours sont exercés par des ressortissants des États membres de l'EEE[22].

Cas 2 - Sous-traitant soumis au RGPD agissant en tant qu'exportateur transférant, pour le compte d'un RT soumis au RGPD, des données vers un sous-traitant ultérieur agissant en tant qu'importateur dans un pays tiers :

Dans le cas où le transfert des données en dehors de l'EEE (en Inde dans le schéma ci-après) n'est pas effectué par le responsable de traitement (la société allemande dans le schéma), mais par son sous-traitant (la société française), ce dernier agissant ainsi en tant qu'exportateur, il lui incombe de s'assurer de la conformité de son transfert et de réaliser l'AITD.

---

[21] Le CEPD précise dans ses lignes directrices 07/2020 : « [*L]e contrat [de sous-traitance] doit préciser la fréquence et la manière dont le flux d'informations entre le sous-traitant et le responsable du traitement devrait avoir lieu, de sorte que le second soit pleinement informé des détails du traitement qui sont pertinents pour démontrer le respect des obligations énoncées à l'article 28 du RGPD ; [c]es informations devraient comprendre des données sur […] la localisation des données, les transferts de données, les personnes qui ont accès aux données et les destinataires des données, les sous-traitants ultérieurs utilisés, etc.* ». https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr

[22] Il est possible de s'appuyer sur toute source fiable comme celles citées dans l'annexe 3 des Recommandations 01/2020 sur les mesures qui complètent les outils de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE du CEPD (« Sources d'information possibles aux fins d'évaluation d'un pays tiers » en §144) : https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_fr

En vertu de l'article 28(3)(h) du RGPD, le sous-traitant (la société française) est tenu de transmettre au responsable de traitement (la société allemande) les informations permettant de démontrer le respect des obligations qui incombent à ce dernier, y compris l'AITD réalisée. Il faut noter que la transmission par le sous-traitant exportateur (la société française) d'une simple conclusion ou d'un résumé exécutif de son AITD ou de son évaluation sur la législation du pays tiers, sans la fourniture d'éléments concrets, ne lui permet pas de satisfaire à ses obligations[23].

Par ailleurs, la décision finale d'engager ou non ce sous-traitant et son sous-traitant ultérieur (les sociétés française et indienne) ou de maintenir la relation contractuelle avec ceux-ci appartient au responsable de traitement (la société allemande) qui a l'obligation de vérifier les garanties proposées au titre de l'article 28(1) du RGPD. Plus le traitement présente un risque élevé pour les droits et libertés des personnes concernées, plus les vérifications effectuées devraient être importantes[24]. Pour ce faire, il peut s'appuyer sur les informations reçues de son sous-traitant – dont son AITD - et les compléter si nécessaire (par exemple si elles sont incomplètes, inexactes ou soulèvent des questions).

Cas 3 - Responsable de traitement soumis au RGPD agissant en tant qu'exportateur transférant des données vers un responsable de traitement dans un pays tiers

Dans le cadre d'un transfert de données entre un responsable de traitement soumis au RGPD agissant en tant qu'exportateur et un responsable de traitement basé dans un pays-tiers agissant en tant qu'importateur, il incombe à l'exportateur de veiller à ce que les données transférées bénéficient dans le pays tiers d'un niveau de protection essentiellement équivalent à celui garanti au sein de l'EEE et par conséquent de réaliser l'AITD avec l'aide de l'importateur.

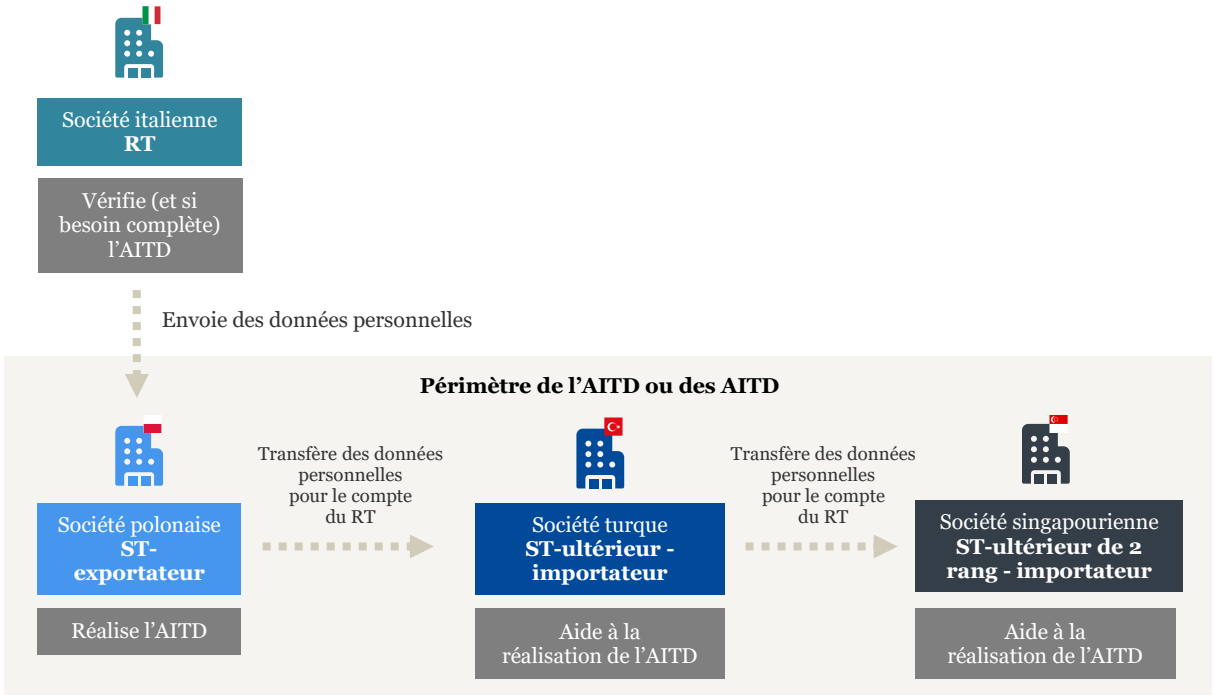
---

[23] Le CEPD précise en §96 de son avis 22/2024, *op.cit.*, (traduction en français par la CNIL) : « Le responsable du traitement doit évaluer les garanties appropriées mises en place et être attentif à toute législation problématique qui pourrait empêcher le sous-traitant de respecter les obligations établies dans son contrat avec le sous-traitant initial. Plus précisément, le responsable du traitement doit veiller à ce qu'une « analyse d'impact du transfert » soit effectuée, conformément à la jurisprudence et comme expliqué dans les recommandations 01/2020 du CEPD. La documentation relative aux garanties appropriées mises en place, à l'« analyse d'impact du transfert » et aux éventuelles mesures supplémentaires doit être produite par le sous-traitant/exportateur (le cas échéant en collaboration avec le sous-traitant/importateur). Le responsable du traitement peut s'appuyer sur l'évaluation préparée par le sous-traitant et, si nécessaire, la compléter. Par exemple, lorsque l'évaluation reçue par le responsable du traitement semble incomplète, inexacte ou soulève des questions, le responsable du traitement doit demander des informations supplémentaires, vérifier les informations et les compléter/corriger si nécessaire, en gardant à l'esprit que l'évaluation doit être conforme aux recommandations 01/2020 du CEPD et aux étapes qui y sont décrites. Il s'agit notamment d'identifier les lois et pratiques pertinentes à la lumière de toutes les circonstances du transfert et d'identifier les mesures supplémentaires appropriées si nécessaire ».

[24] Voir le résumé exécutif et le §60 de l'avis 22/2024 du CEPD, *op. cit.*, (traduction en français par la CNIL) : « Lorsque des transferts de données à caractère personnel en dehors de l'EEE ont lieu entre deux sous-traitants, conformément aux instructions du responsable du traitement, ce dernier reste soumis aux obligations découlant de l'article 28, paragraphe 1, du RGPD concernant les « garanties suffisantes », en plus de celles prévues à l'article 44 pour veiller à ce que le niveau de protection garanti par le RGPD ne soit pas remis en question par les transferts de données à caractère personnel. Le sous-traitant-exportateur doit préparer la documentation pertinente, conformément à la jurisprudence et comme expliqué dans les recommandations 01/2020 du CEPD. Le responsable du traitement doit évaluer cette documentation et être en mesure de la présenter à l'autorité de protection des données compétente. Le responsable du traitement peut s'appuyer sur la documentation ou les informations reçues du sous-traitant-exportateur et, si nécessaire, les compléter. L'étendue et la nature de l'obligation du responsable du traitement d'évaluer cette documentation peuvent dépendre de l'outil utilisé pour le transfert et du fait que le transfert constitue un transfert initial ou un transfert ultérieur ». Le CEPD précise aussi que « les autorités de protection des données devraient évaluer si le responsable du traitement est en mesure de démontrer que la vérification du caractère suffisant des garanties fournies par ses traitants (et sous-traitants ultérieurs) a eu lieu à la satisfaction du responsable du traitement. Le responsable du traitement peut choisir de s'appuyer sur les informations reçues de son sous-traitant et de les compléter si nécessaire (par exemple, lorsqu'elles semblent incomplètes, inexactes ou qu'elles soulèvent des questions). Plus spécifiquement, pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement devrait augmenter son niveau de vérification en termes de contrôle des informations fournies ».

2.4 Périmètre de l'AITD et prise en compte des transferts ultérieurs

La première étape dans la réalisation de l'AITD est de cartographier les transferts des données (voir étape 1 du présent guide). Cette cartographie consiste à bien identifier l'importateur des données et le pays tiers d'importation. Elle permet à l'exportateur des données (et *in fine* au responsable de traitement, si le transfert n'est pas effectué par lui-même) d'identifier les mesures supplémentaires à mettre en place (voir étapes 4 et 5 du présent guide).



L'exportateur doit prendre en considération dans son analyse l'ensemble du flux des données, y compris les transferts ultérieurs, afin que le responsable du traitement (qu'il soit l'exportateur ou non) puisse évaluer les risques liés à tous les transferts des données en dehors de l'EEE[25].

Une AITD peut concerner un seul transfert ou un ensemble de transferts. Par conséquent, l'exportateur a le choix de documenter son analyse au sein du même ou de plusieurs documents. En cas de changement dans la chaine de transferts, il pourra modifier l'analyse existante ou faire une nouvelle

[25] Au §97 de son avis 22/2024, le CEPD précise que « *les responsables du traitement doivent être en mesure de présenter la documentation relative [aux] transferts ultérieurs. Cela signifie que le responsable du traitement doit recevoir ces informations de la part des sous-traitants-exportateurs ou des sous-traitants ultérieurs exportateurs, montrant que les importateurs respectent effectivement les exigences relatives aux transferts ultérieurs tels qu'elles sont prévues dans l'outil du transfert* ».

analyse qu'il rattacher aux analyses préexistantes qu'il a déjà menées. Si l'exportateur est sous-traitant, il doit partager ces informations avec le responsable de traitement.

Par ailleurs, tout transfert ultérieur est soumis au respect, par l'importateur, des obligations qui sont prévues dans l'outil de transfert utilisé. Si des clauses contractuelles types de la Commission (CCT)[26] ont été conclues, l'importateur de données s'engage à ne pas divulguer les données à caractère personnel à un tiers situé en dehors de l'Union européenne dans le même pays que l'importateur de données ou dans un autre pays tiers non-adéquat (ci-après « transfert ultérieur »), sauf si le tiers est lié par les CCT ou accepte de l'être, en vertu du module approprié. Dans le cas contraire, un transfert ultérieur par l'importateur de données ne peut avoir lieu que si les conditions prévues par les CCT sont respectées (module 1, article 8.7 et 8.8 ; modules 2 et 3 – article 8.8) et à condition de respecter ses obligations en matière de tenue de la documentation nécessaire pour démontrer sa conformité (modules 1 et 3, article 8.9 ; module 2 – article 8.8).

2.5 Conformité du transfert aux principes du RGPD

Un transfert de données, comme tout autre traitement, doit être conforme à l'ensemble des principes du RGPD. Conformément à l'article 5 du RGPD, le responsable de traitement doit (directement s'il est lui-même exportateur ou par l'intermédiaire de son sous-traitant si c'est lui l'exportateur) notamment s'assurer que le transfert est licite et repose sur l'une des bases légales de l'article 6 et, le cas échéant, de l'article 9 du RGPD. Les données doivent également être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Il est donc nécessaire de s'assurer que les données transférées sont limitées à ce qui est strictement nécessaire en vue des finalités poursuivies par le transfert. Il est également nécessaire de s'assurer que les personnes concernées sont informées conformément aux articles 13 et 14 RGPD. Il est préférable, lorsque cela est possible, de divulguer ou transmettre des données anonymisées à la place de données à caractère personnel, tout en veillant à ce que le processus d'anonymisation soit mis en œuvre conformément aux lignes directrices du CEPD[27]. Dans ce cas, le RGPD ne s'applique pas.

3. Les différentes étapes de l'AITD

Pour réaliser une AITD, il est recommandé de suivre les 6 étapes suivantes :

3.1 Connaître son transfert (étape 1)

Afin d'assurer un niveau de protection essentiellement équivalent aux données transférées, et ce, où qu'elles soient traitées, il est nécessaire en premier lieu de décrire le transfert. La description du transfert (dans l'étape 1) permet la prise en compte de ses caractéristiques et de sa sensibilité dans l'évaluation de la législation et des pratiques du pays de destination des données et de l'efficacité de l'outil de transfert (à l'étape 3) en vue de mettre en place d'éventuelles mesures supplémentaires (à l'étape 4).

Pour compléter le tableau ci-après, il est possible d'utiliser la documentation interne préexistante, telle que le registre des activités de traitement ou le contrat encadrant le transfert.

Il est également possible de se rapprocher de l'importateur des données.

[26] Voir les clauses contractuelles types publiées par la Commission européenne : https://commission.europa.eu/system/files/2021-06/1_fr_annexe_acte_autonome_cp_part1_v4.pdf

[27] Pour plus de détails sur l'anonymisation, voir Groupe de travail de l'article 29 (G29), avis 05/2014 sur les Techniques d'anonymisation : https://www.cnil.fr/sites/cnil/files/atoms/files/wp216_fr.pdf, ainsi que les articles dédiés sur le site de la CNIL, notamment « L'anonymisation de données personnelles » : https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles ; Des travaux sont actuellement en cours au sein du CEPD afin de publier de nouvelles Lignes directrices sur l'anonymisation.

Exportateur	
Nom de l'exportateur	
Point de contact et coordonnées (service ou personne responsable en interne pour le transfert)	
Pays d'exportation des données	
Qualification de l'exportateur dans le contexte du transfert de données[28]	☐ Responsable de traitement ☐ Responsable conjoint de traitement ☐ Sous-traitant *Si « **Sous-traitant** » ou **« Responsable conjoint »**, préciser le nom du responsable de traitement ou des autres responsables conjoints :*
Toute autre information utile	

Importateur	
Nom de l'importateur	
Point de contact et coordonnées (service ou personne responsable en interne pour le transfert)	
Pays d'importation des données	
Qualification de l'importateur dans le contexte du transfert de données	☐ Responsable de traitement ☐ Responsable conjoint de traitement ☐ Sous-traitant *Si « **Sous-traitant** » ou **« Responsable conjoint »**, préciser le nom du responsable de traitement :*
Nature des activités de l'importateur[29]	*Préciser la nature :*

[28] Voir CEPD, Lignes directrices 07/2020, op.cit.
[29] Information facilitant l'identification de la législation applicable dans le pays tiers.

Importateur	
	Est-ce que c'est un importateur des données spécifiquement protégé par la législation du pays de destination des données [30] ?
Toute autre information utile	

Transfert	
Activités de traitement de l'importateur sur les données transférées (*ex. support informatique, marketing, fourniture d'un logiciel en nuage, hébergement des données*)	
Type de transfert (*manière dont sont rendues disponibles les données auprès de l'importateur*)	☐ **Accès à distance sans possibilité de téléchargement/stockage local** - Les données à caractère personnel sont hébergées par l'exportateur au sein de l'EEE. L'importateur n'a pas la possibilité de télécharger des copies des données, mais il peut y accéder à distance depuis un pays hors de l'EEE non adéquat. ☐ **Accès à distance avec possibilité de téléchargement/stockage local** - Les données à caractère personnel sont hébergées par l'exportateur au sein de l'EEE. L'importateur a la possibilité d'accéder aux données depuis un pays tiers et si nécessaire de télécharger et de stocker des copies des données dans un pays tiers à l'EEE non adéquat. ☐ **Transmission et hébergement / stockage local** - L'importateur héberge ou stocke les données à caractère personnel dans un pays tiers à l'EEE non adéquat. ☐ **Autre**
Méthode de transfert (*ex. transmission par protocole de transfert de fichier sécurisé (SFTP), transmission par email, connexion via une interface de programmation (API), connexion à un serveur à distance, stockage des données dans un support physique et envoi, etc.*)	
Format des données transférées	☐ En clair ☐ Chiffrées

[30] Un importateur de données dans un pays tiers peut-être spécifiquement protégé par le droit national, par exemple dans le but de fournir un traitement médical à un patient ou des services juridiques à un client. Voir §91, 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.

Transfert	
	☐ Pseudonymisées ☐ Autre *Si « **Autre** », préciser :*
Fréquence des transferts	☐ Transfert unique ☐ Transfert ponctuel / occasionnel (*récurrence à préciser*) : ☐ Transfert régulier (*récurrence à préciser*) :
Possibilité d'effectuer des transferts ultérieurs pour l'importateur *(cf. ci-dessus section 2.4)*	☐ Oui ☐ Non *Si **oui**, préciser :*
Catégories de données à caractère personnel transférées	☐ Données d'identification (*à préciser*) : ☐ Coordonnées de contact (*à préciser*) : ☐ Données relatives à la vie familiale (*à préciser*) : ☐ Données relatives à la vie professionnelle (*à préciser*) : ☐ Données d'utilisation d'un service (*à préciser*) : ☐ Autres (*à préciser*) :
Catégories particulières de données à caractère personnel transférées (« données sensibles »)	☐ Données révélant l'origine raciale ou ethnique (*à préciser*) : ☐ Données révélant les opinions politiques (*à préciser*) : ☐ Données révélant les croyances religieuses ou philosophiques (*à préciser)* : ☐ Données révélant l'appartenance syndicale (*à préciser*) : ☐ Données génétiques ou données biométriques aux fins d'identifier une personne physique de manière unique (*à préciser*) : ☐ Données concernant la santé (*à préciser*) : ☐ Données concernant la vie sexuelle d'une personne physique (*à préciser*) : ☐ Aucune des catégories ci-dessus
Autres données hautement personnelles transférées	☐ Données relatives aux condamnations pénales, aux infractions[31] (*à préciser*) :

[31] Article 10 du RGPD

Transfert	
	☐ Numéro national d'identification[32] (*à préciser*) : ☐ Données de géolocalisation[33] (*à préciser*) : ☐ Données financières susceptibles d'être utilisées pour des paiements frauduleux[34] (*à préciser*) : ☐ Autres (*à préciser*) : ☐ Aucune des catégories ci-dessus
Catégories de personnes concernées	
Personnes vulnérables parmi les personnes concernées (*ex. mineurs, personnes dépendantes)*	☐ Oui ☐ Non *Si « **Oui** », préciser :*
Caractère total ou partiel du transfert[35] (si pertinent)	☐ Total ☐ Partiel *Si « **partiel** », préciser le pourcentage (si possible) :*
Volume des données transférées (si possible)	
Nombre des personnes concernées (si possible)	
Date envisagée de début du transfert (si possible)	
Date envisagée de fin ou durée du transfert (si possible)	

[32] Article 87 du RGPD
[33] Voir Groupe de travail de l'article 29 (G29), Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, p.11 : https://www.cnil.fr/sites/cnil/files/atoms/files/wp248_rev.01_fr.pdf
[34] Idem
[35] Les données transférées représentant la totalité des données traitées ou seulement une partie.

3.2 Identifier l'outil de transfert utilisé (étape 2)

L'identification de l'outil de transfert utilisé vient compléter la description du transfert (à l'étape 1). Elle est nécessaire à l'évaluation de son efficacité (à l'étape 3).

Outil de transfert de l'article 46 RGPD	
Outil de transfert de l'article 46 utilisé pour encadrer le transfert	☐ Clauses Contractuelles Types (CCT)[36] (Module utilisé à préciser) : ☐ Règles d'entreprise contraignantes (BCR) « responsable de traitement »[37] ☐ Règles d'entreprise contraignantes (BCR) « sous-traitant »[38] ☐ Code de conduite[39] ☐ Mécanisme de certification[40] ☐ Clauses contractuelles ad hoc
Éléments et documentation attestant de l'outil de transfert en place (ex. contrat signé avec l'importateur des données, attestation de certification de l'importateur des données, copie des BCR avec la liste d'entités faisant partie des BCR dont l'importateur des données)	

Si le transfert s'appuie sur un des outils de transfert de l'article 46 du RGPD, il est nécessaire de procéder à une AITD et il convient de passer à l'étape 3.

S'il n'est pas nécessaire de réaliser une AITD (voir section 2.2), il est recommandé de documenter la décision de ne pas réaliser une AITD.

[36] Voir les clauses contractuelles types publiées par la Commission européenne : https://commission.europa.eu/system/files/2021-06/1_fr_annexe_acte_autonome_cp_part1_v4.pdf. Dans sa FAQ sur les CCT, la Commission européenne indique qu'un jeu supplémentaire de CCT, dédié aux transferts vers les importateurs soumis au RGPD est en cours d'élaboration. Une fois que ce nouveau jeu sera adopté, il sera possible de l'utiliser pour encadrer les transferts vers des importateurs soumis au RGPD. Voir §25 de la FAQ de la Commission européenne sur les CCT (en anglais) : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en#scope-of-application-and-transfer-scenarios

[37] Pour les BCR-Responsable de traitement, voir CEPD, Recommandations 1/2022 concernant la demande d'approbation et les éléments et principes des règles d'entreprises contraignantes pour les responsables de traitement (article 47 du RGPD) : https://www.edpb.europa.eu/system/files/2024-05/edpb_recommendations_20221_bcr-c_v2_fr.pdf

[38] Pour les BCR-Sous-traitant, voir G29, formulaire d'instruction WP265 : https://www.cnil.fr/sites/cnil/files/atoms/files/wp_265-bcr-st-formulaire-en.doc ; et référentiel d'approbation WP257 : https://www.cnil.fr/sites/cnil/files/atoms/files/wp-257_bcr-st-referentiel_fr.pdf.

[39] Voir CEPD, Lignes directrices 04/2021 sur les codes de conduite en tant qu'outils pour les transferts : https://www.edpb.europa.eu/system/files/2022-10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_fr.pdf

[40] Voir CEPD, Lignes directrices 07/2022 sur la certification en tant qu'outil au service des transferts (version 2.0) : https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_fr_0.pdf

3.3 Évaluer la législation et la pratique du pays de destination des données et l'efficacité de l'outil de transfert (étape 3)

Une fois obtenue une vision claire du transfert et de l'outil utilisé pour l'encadrer, la troisième étape est de déterminer s'il existe des éléments dans la législation ou les pratiques du pays tiers importateur qui pourraient porter atteinte à l'efficacité des garanties de l'outil utilisé, dans le contexte spécifique du transfert, ou empêcher l'exportateur ou l'importateur de remplir leurs obligations[41]. La description du transfert (dans l'étape 1) permet la prise en compte de ses caractéristiques et de sa sensibilité dans l'évaluation de la législation et des pratiques du pays de destination des données et de l'efficacité de l'outil de transfert (à l'étape 3).

La coopération de l'importateur est indispensable pour cet exercice : il revient à l'exportateur de lui demander de fournir une analyse de sa législation, notamment en matière d'accès des autorités aux données ou *a minima* de fournir la liste des lois applicables. Il est donc important d'impliquer l'importateur dans la réalisation de l'AITD dans la mesure où l'importateur doit respecter les instructions de l'exportateur et du responsable de traitement (si l'exportateur est sous-traitant).

Pour compléter cette étape, il est recommandé de consulter l'Annexe 3 des recommandations du CEPD sur les mesures supplémentaires[42] qui énumère, de manière non exhaustive, des sources d'information qui peuvent être utilisées. Ces sources doivent être pertinentes, objectives, fiables, vérifiables et publiquement disponibles ou accessibles d'une autre manière.

Il est possible de s'appuyer sur la carte du monde de la CNIL qui contient des informations relatives au cadre de protection des données dans le pays tiers (existence d'une loi sur la protection des données et d'une autorité de protection des données).

Pour l'analyse de la législation en matière d'accès aux données par les autorités publiques, il ne faut pas hésiter à s'appuyer aussi sur des rapports d'organisations internationales et des analyses d'experts telles que les analyses commandées par le CEPD pour certains pays[43]. Ces analyses doivent être complétées et mises à jour en tant que de besoin.

Il est recommandé de partager les analyses à travers des réseaux des DPO, des fédérations professionnelles ainsi que des groupes d'entreprises ou d'administrations.

Législation en matière de protection des données	
Quel est le cadre **applicable à l'importateur** en matière de protection des données ?	*Référence du/des textes :*

[41] Pour plus d'informations sur comment évaluer ceci, il est possible de se référer au §43.3 des recommandations 01/2020 du CEPD sur les mesures qui complètent les outils de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE : https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_fr.pdf

[42] Voir les mesures qui complètent les outils de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE dans les .

[43] Le CEPD a commandé des rapports d'experts en ce qui concerne :

- la Russie, l'Inde, la Chine (https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf) ;
- le Brésil (https://www.edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_brazil_final_report_milieu_redacted.pdf) ;
- le Mexique et la Turquie (https://www.edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_mexico_and_turkiye_final_report_milieu_redacted.pdf).

Législation en matière de protection des données		
Quel est son champ d'application ?	☐ Cadre général ☐ Application sectorielle	*Si application sectorielle, préciser :*
Adhésion du pays tiers à des traités internationaux en matière de protection des données	☐ Oui ☐ Non	*Si oui, préciser :*
Existe-t-il une autorité de protection des données compétente (ou une entité administrative disposant de prérogatives comparables) dans le pays tiers ?	☐ Oui ☐ Non	*Nom de l'autorité :*
Cette autorité/entité est-elle indépendante[44] ?	☐ Oui ☐ Non	*Justifier :*
Quels sont les droits des personnes concernées ?	**Droits des personnes concernées**	
	Droit d'accès ☐ Oui ☐ Non	*Si oui, référence :*
	Droit de rectification ☐ Oui ☐ Non	*Si oui, référence :*
	Droit de suppression	*Si oui, référence :*

[44] Afin de déterminer si l'autorité est indépendante, il est possible de s'appuyer sur les articles 52 à 54 du RGPD, sur l'article 15 de la Convention 108+ du Conseil de l'Europe (https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726), ainsi que sur les travaux de l'Assemblée mondiale pour la protection de la vie privée (GPA), disponibles tous les trois en anglais :

- Article 5.1 de ses règles de procédure : https://globalprivacyassembly.org/wp-content/uploads/2020/10/GPA-Rules-and-Procedures-October-2020.pdf ;
- Principe B.2 de ses principes d'accréditation : http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Accreditation-Features-of-Data-Protection-Authorities.pdf ; et
- le document du Groupe de travail sur l'avenir de la Conférence « Interprétation des critères d'autonomie et d'indépendance » : https://globalprivacyassembly.org/wp-content/uploads/2019/12/ICDPPC-Background-document-on-independence-criteria_post-Coe-comment.pdf.

Il est aussi possible de s'appuyer sur les travaux plus généraux de l'Organisation de coopération et de développement économiques (OCDE) » :

- « Being an Independent Regulator, The Governance of Regulators » (disponible en anglais) : https://www.oecd.org/en/publications/being-an-independent-regulator_9789264255401-en.html ;
- « Créer une culture d'indépendance : Lignes directrices pour contrer l'influence indue » : https://www.oecd.org/fr/publications/creer-une-culture-d-independance_9789264287884-fr.html

Législation en matière de protection des données		
	☐ Oui ☐ Non	
	Droit d'opposition pour des situations particulières ☐ Oui ☐ Non	*Si oui, référence :*
	Droit d'opposition à la prise de décision automatisée ☐ Oui ☐ Non	*Si oui, référence :*
	Autres droits ☐ Oui ☐ Non	*Si oui, préciser :*
	Est-ce que les restrictions à ces droits prévues par la loi sont nécessaires et proportionnées dans une société démocratique ? ☐ Oui ☐ Non	*Si oui, préciser :*
Voies de recours et sanctions	Existe-t-il des voies de recours effectives ? ☐ Oui ☐ Non	*Justifier :*
	Existe-t-il des sanctions effectives et dissuasives ? ☐ Oui ☐ Non	*Justifier :*
	Est-ce que ces droits et ces voies de recours peuvent être exercés par des ressortissants des Etats-membres de l'EEE ? ☐ Oui ☐ Non	*Justifier :*

Lois et/ou pratiques permettant l'accès aux données		
	Si oui, lister :	
	Références	*Description (champ d'application, autorité publique concernée, nature de l'obligation, etc.)*
Existe-t-il des lois de surveillance **applicables à l'importateur** établissant des obligations de divulguer les données à caractère personnel transférées ou d'octroyer l'accès à ces données à des autorités publiques[45] ? ☐ Oui ☐ Non		
Existe-t-il des pratiques de surveillance **applicables à l'importateur** entrainant des obligations de divulguer les données à caractère personnel transférées ou d'octroyer l'accès à ces données à des autorités publiques[46] ? ☐ Oui ☐ Non		

[45] Ces lois peuvent avoir une portée générale, concerner l'application du droit pénal ou bien la protection de la sécurité nationale. Elles peuvent concerner des autorités telles que des organismes gouvernementaux, des régulateurs, des autorités en charge des impôts, la police, des agences de renseignement, etc.
[46] *Idem*.

Garanties essentielles[47]	
L'accès aux données est-il encadré par des règles claires, précises et accessibles ? ☐ Oui ☐ Non	*Justifier :*
L'accès aux données est-il nécessaire et proportionné dans une société démocratique pour sauvegarder un des objectifs listés à l'article 23(1) du RGPD[48] ? ☐ Oui ☐ Non	*Justifier :*
L'accès aux données est-il contrôlé par un mécanisme de surveillance indépendant ? ☐ Oui ☐ Non	*Justifier :*
L'autorité publique concernée est-elle soumise à des obligations de transparence et de contrôle régulier ? ☐ Oui ☐ Non	*Justifier :*
La personne concernée dispose-t-elle de voies de recours générales (non soumises à des conditions de nationalité) et effectives devant un organe indépendant et impartial ? ☐ Oui ☐ Non	*Justifier :*

[47] Voir CEPD Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance : https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_fr.pdf

[48] Ces objectifs sont : (a) la sécurité nationale ; (b) la défense nationale ; (c) la sécurité publique ; (d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; (e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ; (f) la protection de l'indépendance de la justice et des procédures judiciaires ; (g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière ; (h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g) ; (i) la protection de la personne concernée ou des droits et libertés d'autrui; (j) l'exécution des demandes de droit civil.

Etat de droit		
Existe-t-il des problèmes d'État de droit affectant la capacité des personnes concernées par les données transférées à exercer un recours contre des accès illégaux aux données à caractère personnel ? ☐ Oui ☐ Non	*Si oui, lister :*	
	Problème	*Manière dont il affecte l'exercice des droits pour les personnes concernées*

Demandes reçues	
L'importateur peut-il démontrer qu'il n'a pas reçu de demande d'accès ou fait l'objet d'un accès direct par les autorités du pays tiers à des données à caractère personnel des ressortissants d'un Etat-membre de l'EEE (au moins sur les dernières années) ? ☐ Oui ☐ Non	*Si **oui**, préciser ici comment il peut le démontrer[49] :* *Si **non**, préciser ici le type de demandes reçues, la quantité et la manière dont elles ont été traitées et/ou les raisons pour lesquelles il pense pouvoir en faire l'objet dans le futur :*
Peut-il être démontré qu'il n'y a aucune raison de croire que l'importateur fera l'objet d'une demande d'accès ou d'un accès direct par les autorités du pays tiers, notamment parce que la législation ou les problèmes identifiés ne s'appliqueront pas en pratique aux données transférées et à l'importateur (compte tenu de son secteur d'activité et de l'historique des demandes d'accès des autorités du pays tiers)[50] ? ☐ Oui ☐ Non Dans ce cas, il est possible de décider de procéder au transfert sans mettre en œuvre de mesures supplémentaires.	*Si **oui**, préciser ici comment il peut le démontrer[51] :*

[49] Par exemple, par son rapport de transparence sur les demandes d'accès par les autorités aux données de l'exportateur ou d'autres exportateurs.
[50] Dans certains cas où l'outil de transfert n'est pas efficace à la lumière de l'évaluation menée mais qu'il n'y a pas lieu de croire que la législation problématique sera appliquée en pratique aux données transférées et/ou à l'importateur, il est possible de décider de procéder tout de même au transfert sans mettre en œuvre de mesures supplémentaires. Il est alors nécessaire de démontrer et documenter cette évaluation le cas échéant en collaboration avec l'importateur, compte tenu également de l'expérience d'autres acteurs opérant dans le même secteur et/ou dans des secteurs liés à des données personnelles transférées similaires et d'autres sources d'information. Voir CEPD, Lignes directrices 01/2020, §43.3
[51] Par exemple, par des éléments publiés par d'autres acteurs opérant dans le même secteur et/ou dans des secteurs liés.

Conclusion
☐ L'outil de transfert est efficace à la lumière de l'évaluation de la législation et des pratiques locales et il est possible de procéder au transfert sans mettre en place de mesures supplémentaires (1). ☐ L'outil de transfert n'est pas efficace à la lumière de l'évaluation de la législation et des pratiques locales et il est nécessaire de mettre en place des mesures supplémentaires (2). ☐ L'outil de transfert n'est pas efficace à la lumière de l'évaluation menée mais il n'y a pas lieu de croire que la législation problématique sera appliquée en pratique et il est décidé de procéder au transfert sans mettre en œuvre de mesures supplémentaires (3). Justifier :

Si la conclusion est (1) l'effectivité de l'outil de transfert à la lumière de l'évaluation menée ou (3) le fait que, malgré l'ineffectivité de l'outil, il est possible de procéder au transfert sans mettre en place de mesures supplémentaires, il est possible de procéder au transfert. Il est recommandé de réaliser l'étape 6.

Si la conclusion est que (2) l'outil de transfert n'est pas efficace à la lumière de l'évaluation menée, il est nécessaire d'aller à l'étape 4 afin de recenser des mesures supplémentaires.

3.4 Recenser et adopter des mesures supplémentaires (étape 4)

Il est nécessaire d'identifier au cas par cas quelles mesures supplémentaires pourraient être efficaces pour le transfert vers un pays tiers donné. La description du transfert dans l'étape 1 permet, en particulier, que ses caractéristiques et sa sensibilité soient prises en compte pour l'évaluation des mesures supplémentaires à mettre en place. Plus le traitement présente un risque élevé pour les droits et libertés des personnes concernées, plus les vérifications effectuées et les mesures supplémentaires à mettre en place doivent être importantes[52].

Ces mesures sont dites « supplémentaires » car elles complètent l'outil de transfert destiné à garantir le respect du niveau de protection des données à caractère personnel de l'EEE. Il est donc nécessaire de recenser dans le tableau ci-dessous à la fois des mesures déjà mises en œuvre, le cas échéant, ainsi que des mesures nouvellement identifiées.

[52] Dans son avis 22/2024, le CEPD indique que « *pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement devrait augmenter son niveau de vérification en termes de contrôle des informations fournies.* ». En ce qui concerne les transferts spécifiquement, il indique : « *l'obligation pour le responsable du traitement de vérifier si les sous-traitants ([y compris] ultérieurs) présentent des garanties suffisantes pour mettre en œuvre les mesures [qu'il a) déterminées en vertu de l'article 28, paragraphe 1, du RGPD devrait s'appliquer quel que soit le risque pour les droits et libertés des personnes concernées. Néanmoins, l'étendue de cette vérification variera en pratique en fonction de la nature des mesures organisationnelles et techniques déterminées par le responsable du traitement sur la base, entre autres critères, du risque associé au traitement* ». Voir CEPD, Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), résumé exécutif, §60 et 83.

L'Annexe 2 des recommandations du CEPD sur les mesures supplémentaires fournit une liste non exhaustive de mesures techniques, contractuelles et organisationnelles qui peuvent être mises en œuvre sous forme de cas d'usage. Elle présente aussi des cas d'usage pour lesquels le CEPD n'est pas en mesure d'identifier de mesures efficaces[53].

Il peut s'avérer nécessaire de combiner plusieurs mesures supplémentaires. Dans la plupart des cas, les mesures contractuelles et organisationnelles ne sont pas suffisantes pour empêcher un éventuel accès aux données par les autorités du pays tiers et doivent être complétées par des mesures techniques dûment mises en œuvre[54].

L'efficacité des mesures supplémentaires peut varier en fonction du transfert décrit à l'étape 1 et selon le pays tiers, d'où l'importance de mener une analyse détaillée dans l'étape 3. **Dans certains cas, la conclusion sera qu'aucune mesure supplémentaire ne permet d'assurer un niveau de protection essentiellement équivalent au droit européen pour le transfert en cause, ce qui devrait conduire à renoncer au transfert de données en cause.**

Ce processus d'identification de mesures supplémentaires devrait être entrepris avec la diligence requise, en collaboration avec l'importateur et devrait être documenté. L'implication du responsable des systèmes d'information est essentielle. Il est recommandé d'annexer à l'AITD les avis ou analyses des personnes ou entités qui ont été consultées (ex. DPO, conseil juridique et technique, responsable des systèmes d'information, autorité de protection des données).

[53] Voir CEPD, Recommandations 01/2020, cas d'usage 6 et 7, §93 à 97.
[54] Voir CEPD, Recommandations 01/2020 , §53 : « *Des mesures contractuelles et organisationnelles ne permettront pas généralement, à elles seules, de surmonter l'accès des autorités publiques du pays tiers à des données à caractère personnel sur la base d'une législation et/ou de pratiques problématiques. En effet, dans certaines situations, seules des mesures techniques dûment mises en œuvre pourraient empêcher ou rendre inopérant l'accès des autorités publiques de pays tiers à des données à caractère personnel, notamment à des fins de surveillance* ».

Mesures supplémentaires déjà existantes			
Description (Pour chaque mesure, fournir une description, préciser si elle est mise en œuvre par l'importateur ou l'exportateur et dans quelle mesure elle se conforme aux recommandations du CEPD)			**Impact des mesures** (Pour chaque mesure, préciser quel(s) risque(s) est/sont atténué(s)
Mesures techniques	☐ Pseudonymisation[55] ☐ Chiffrement[56] ☐ Autre (préciser) :		

[55] Voir Recommandations 01/2020 du CEPD, cas d'usage 2, §85 :

1. *Un exportateur de données transfère des données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise ni être utilisées pour distinguer la personne concernée au sein d'un groupe plus vaste, sans avoir recours à des informations supplémentaires*
2. *les informations supplémentaires sont détenues exclusivement par l'exportateur de données et conservées séparément dans un État membre ou dans un pays tiers par une entité qui a la confiance de l'exportateur dans l'EEE ou dans une juridiction offrant un niveau de protection essentiellement équivalent à celui garanti dans l'EEE,*
3. *la divulgation ou l'utilisation non autorisée de ces informations supplémentaires est empêchée par des garanties techniques et organisationnelles appropriées, et il est garanti que l'exportateur conserve le contrôle exclusif de l'algorithme ou du répertoire permettant une réidentification à l'aide des informations supplémentaires, et*
4. *le responsable du traitement a établi, au moyen d'une analyse approfondie des données en question, en tenant compte de toutes les informations dont les autorités publiques du pays destinataire pourraient disposer et qu'elles pourraient utiliser, que les données à caractère personnel pseudonymisées ne peuvent pas être attribuées à une personne physique identifiée ou identifiable même en procédant à des recoupements avec ces informations*

[56] Voir Recommandations 01/2020 du CEPD, cas d'usage 3, §90 :

1. *Un exportateur de données transfère des données à caractère personnel à un importateur de données dans une juridiction où la législation et/ou la pratique autorisent les autorités publiques à accéder aux données alors qu'elles sont transmises par internet vers ce pays tiers sans les garanties essentielles européennes relatives à cet accès, le chiffrement de la transmission est utilisé, garantissant ainsi que les protocoles de chiffrement employés sont à la pointe de la technologie et offrent une protection efficace contre les attaques actives et passives au moyen de ressources dont disposent notoirement les autorités publiques du pays tiers,*
2. *les parties concernées par la communication conviennent d'une autorité ou d'une infrastructure de certification à clé publique digne de confiance,*
3. *des mesures de protection spécifiques et de pointe sont utilisées contre les attaques actives et passives dirigées contre les systèmes d'envoi et de réception qui assurent le chiffrement de la transmission, y compris des tests de vulnérabilité des logiciels et d'éventuelles portes dérobées,*
4. *au cas où le chiffrement du transfert ne permet pas en lui-même une sécurité suffisante en raison de la vulnérabilité de l'infrastructure ou du logiciel utilisé, les données à caractère personnel sont également chiffrées de bout en bout sur la couche application grâce à des méthodes de chiffrement de pointe,*
5. *l'algorithme de chiffrement et son paramétrage (par exemple la longueur de clé ou le mode opératoire, le cas échéant) sont conformes à l'état de la technique et peuvent être considérés comme résistants à une cryptanalyse réalisée par les autorités publiques lorsque les données transitent vers ce pays tiers, compte tenu des ressources et des capacités techniques (par exemple la puissance de calcul pour les attaques par force brute) dont elles disposent (voir note de bas de page n°80 ci-dessus),*
6. *la solidité du chiffrement tient compte de la durée spécifique pendant laquelle la confidentialité des données à caractère personnel chiffrées doit être préservée,*
7. *l'algorithme de chiffrement est correctement exécuté par un logiciel dûment mis à jour, sans vulnérabilités connues, et dont la conformité par rapport à la spécification de l'algorithme choisi a été vérifiée, par exemple par une certification,*
8. *les clés sont gérées de manière fiable (générées, administrées, stockées, le cas échéant, liées à l'identité du destinataire prévu et supprimées) par l'exportateur ou par une entité en laquelle l'exportateur a confiance située sur un territoire offrant un niveau de protection essentiellement équivalent*

Mesures supplémentaires déjà existantes			
Mesures organisationnelles [57]	☐ Documentation des demandes d'accès (demandes reçues, réponse, raisonnement juridique, acteurs impliqués) ☐ Minimisation des données (accès strict et granulaire, politiques de confidentialité, accès basé sur le principe du besoin de savoir, contrôle par le biais d'audits, mesures disciplinaires ☐ Gouvernance (information et implication du délégué à la protection des données ou du référent RGPD pour toutes les demandes d'accès) ☐ Adoption de normes de sécurité et de protection des données (certification et respect des normes de sécurité) ☐ Politiques et procédures internes pour le traitement des demandes d'accès ☐ Répartition des responsabilités entre les entités d'un même groupe, désignation d'équipes spécifiques pour traiter les demandes d'accès, formation du personnel chargé de la gestion de ces demandes ☐ Autres (préciser) :		
Mesures contractuelles[58]	☐ Inclusion de mesures techniques ou organisationnelles supplémentaires dans un contrat contraignant ☐ Obligation de transparence ☐ Obligation pour l'importateur d'énumérer les lois, les pratiques, les mesures visant à empêcher l'accès, les demandes d'accès, et d'indiquer s'il lui est légalement interdit de fournir les informations susmentionnées		

[57] Voir Recommandations 01/2020 du CEPD, Section 2.3 Mesures organisationnelles, § 128 à 143 :
[58] Voir Recommandations 01/2020 du CEPD, Section 2.2 Mesures contractuelles supplémentaires, §98 à 127.

Mesures supplémentaires déjà existantes			
	☐ Interdiction d'utiliser des portes dérobées ou des procédés qui facilitent l'accès aux données ☐ Possibilité de procéder à un audit afin de vérifier la conformité ☐ Notification à l'exportateur (et aux personnes concernées) en cas d'accès aux données par les autorités publiques ☐ Engagement à contester les demandes d'accès ☐ Engagement par l'importateur d'examiner la légalité de toute ordonnance de divulgation et la contester s'il y a des raisons de le faire ☐ Engagement à demander des mesures provisoires pour suspendre les effets de l'ordonnance jusqu'à ce que le tribunal se prononce sur le fond ☐ Engagement à informer en cas d'incapacité à respecter ses engagements contractuels ☐ Sanctions en cas de violation, y compris l'indemnisation des personnes concernées ☐ Résiliation du contrat en cas de manquement aux obligations relatives aux transferts de données ☐ Engagement de l'importateur à ne fournir aux autorités du pays tiers que le minimum d'informations lorsqu'il répond à une demande d'accès ☐ Engagement de l'importateur à informer l'autorité du pays tiers de l'incompatibilité avec les lois sur la protection des données et à notifier simultanément l'exportateur ☐ Les données en clair ne peuvent être consultées qu'avec le		

Mesures supplémentaires déjà existantes			
	consentement explicite ou implicite de l'exportateur ☐ Autres (préciser) :		
Conclusion		☐ L'outil de transfert, combiné à ces mesures existantes, **est efficace** à la lumière de l'évaluation menée. ☐ L'outil de transfert, combiné à ces mesures existantes, **n'est pas efficace** à la lumière de l'évaluation menée. Dans les cas, il est nécessaire d'envisager d'autres mesures supplémentaires.	

Nouvelles mesures supplémentaires		
Description (Pour chaque mesure, fournir une description, préciser si elle est mise en œuvre par l'importateur ou l'exportateur et dans quelle mesure elle se conforme aux recommandations du CEPD)		**Impact des mesures** (préciser quel(s) risque(s) est/ sont atténué(s) grâce aux mesures supplémentaires)
Mesures techniques (cf. exemples ci-dessus)		
Mesures organisationnelles (cf. exemples ci-dessus)		
Mesures contractuelles (cf. exemples ci-dessus)		
Conclusion	☐ L'outil de transfert, combiné aux mesures existantes et à ces autres mesures supplémentaires, **est efficace** à la lumière de l'évaluation menée. ☐ L'outil de transfert, combiné aux mesures existantes et à ces autres mesures supplémentaires, **n'est pas efficace** à la lumière de l'évaluation menée.	

Si la conclusion est que l'outil de transfert, combiné à ces mesures, **est efficace** à la lumière de l'évaluation menée, il est possible de transférer sous réserve de la mise en œuvre effective de l'ensemble des mesures supplémentaires nécessaires. Dans le cas où des mesures déjà existantes suffisent, il est possible d'aller directement à l'étape 6. Dans le cas où d'autres mesures supplémentaires seraient nécessaires (en plus des mesures déjà existantes), il est recommandé d'aller à l'étape 5.

À la suite de la réalisation de l'AITD ou lors d'une réévaluation, si la conclusion est qu'il n'est pas possible de mettre en place les mesures nécessaires afin d'assurer l'efficacité de l'outil de transfert, **il ne faut pas mettre en œuvre le transfert prévu. Si le transfert est déjà en cours, il est nécessaire de l'arrêter.** Dans ce dernier cas, l'importateur devra effacer toutes les données et en apporter la preuve à l'exportateur ou lui restituer toutes les données et effacer les copies existantes.

3.5 Mettre en œuvre les mesures supplémentaires (étape 5)

Une fois les mesures supplémentaires adéquates pour s'assurer que les données transférées jouissent d'un niveau de protection essentiellement équivalent identifiées, il est recommandé de lister dans le tableau ci-après les actions à mener concernant les mesures supplémentaires restant à mettre en place et le respect des éventuelles étapes procédurales à suivre. Cela permet de s'assurer de leur effectivité et d'anticiper les obstacles éventuels (ex. difficulté financière, indisponibilité des équipes compétentes, etc.).

Les étapes procédurales à respecter peuvent varier selon l'outil de transfert sur lequel est basé le transfert. Les recommandations du CEPD sur les mesures supplémentaires listent certaines de ces étapes[59].

Plan d'actions	
Action 1 *Nom :*	*Description :*
	Coût estimé en jours/personne (optionnel) :
	Personne(s) en charge (ex. expert juridique, expert technique, service métier) :
	Date prévue de réalisation :
Action 2 *Nom :*	*Description :*
	Coût estimé en jours/personne (optionnel) :
	Personne(s) en charge (ex. expert juridique, expert technique, service métier) :
	Date prévue de réalisation :
…	…

[59] Voir, CEPD, Recommandations 01/2020, section 2.5 Etape 5, §59 à 68. Par exemple, la nécessité pour l'exportateur de demander une autorisation à l'autorité compétente dans le cas où les CCT ont été modifiées et que cela restreint les droits et obligations qu'elles contiennent ou lorsque les mesures supplémentaires contredisent les CCT.

Avis
Avis de la personne en charge de la protection des données (ou du délégué à la protection des données, le cas échéant)
Avis de la personne en charge de sécurité du système d'information (ou du responsable de la sécurité des systèmes d'information, le cas échéant)

Validation par la personne responsable du transfert en fonction de la gouvernance interne

3.6 Réévaluer à intervalles appropriés (étape 6)

Il est recommandé de réévaluer à intervalles appropriés l'outil de transfert et, le cas échéant, les mesures supplémentaires qui ont été mises en œuvre pour le transfert. Ceci est essentiel pour s'assurer que le transfert sera suspendu ou cessera si l'outil de transfert ou les mesures supplémentaires ne sont plus efficaces dans le pays tiers. À cette fin, il est recommandé de prévoir dans le tableau ci-dessous une revue périodique du transfert.

Ces intervalles appropriés sont à déterminer au cas par cas en fonction du pays de destination des données et du niveau de risque pour les droits et libertés des personnes concernées impliquées par le transfert. Dans diverses circonstances, il peut être nécessaire de réévaluer la protection du transfert avant la date initiale de la prochaine revue, par exemple en cas de changement dans la législation ou les pratiques du pays tiers, d'incapacité de l'importateur à respecter ses engagements ou de changement dans l'appréciation par la Commission européenne du droit applicable dans le pays tiers. À cette fin, il est recommandé de suivre les actualités législatives dans ce pays, afin de pouvoir anticiper si la réévaluation de la protection des données dans ce pays s'avère nécessaire.

Réévaluer la protection	
Intervalle entre les revues (ex. tous les 2 ans)	
Date de la prochaine revue	
Revue anticipée, le cas échéant, et justification de l'anticipation	