Consultation publique sur le guide pratique

« Analyse d'impact des transferts de données »

Synthèse des contributions

Janvier 2025

De décembre 2023 à février 2024, la CNIL a soumis à consultation publique son guide pratique pour la réalisation d'analyses d'impact du transfert de données (AITD).

Les contributions reçues ont permis d'enrichir la version définitive du guide pratique AITD.

Cette synthèse présente les principales observations reçues, ainsi que les éléments de réponse que la CNIL a décidé de leur apporter.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Synthèse des contributions à la consultation publique sur le guide pratique « Analyse d'impact des transferts de données »

Cette consultation publique a fait l'objet de contributions, principalement de professionnels du secteur (délégués à la protection des données, avocats, consultants, têtes de réseaux professionnels), concernés par le sujet des transferts. La CNIL propose ici une synthèse des contributions.

À propos de la consultation publique de la CNIL sur son projet de guide AITD

Un très grand nombre de responsables de traitement et sous-traitants est concerné par la question des transferts. Dans son arrêt dit « Schrems II », la Cour de justice de l'Union européenne (CJUE) a souligné la responsabilité des exportateurs et importateurs des données de garantir que les traitements de données à caractère personnel se font, et continuent à se faire, dans le respect du niveau de protection fixé par la législation de l'Union européenne en matière de protection des données. 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 garanties supplémentaires. Une telle évaluation est communément appelée « Analyse d'impact des transferts de données » ou « AITD » en français (« Transfer Impact Assessment » ou « TIA » en anglais).

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

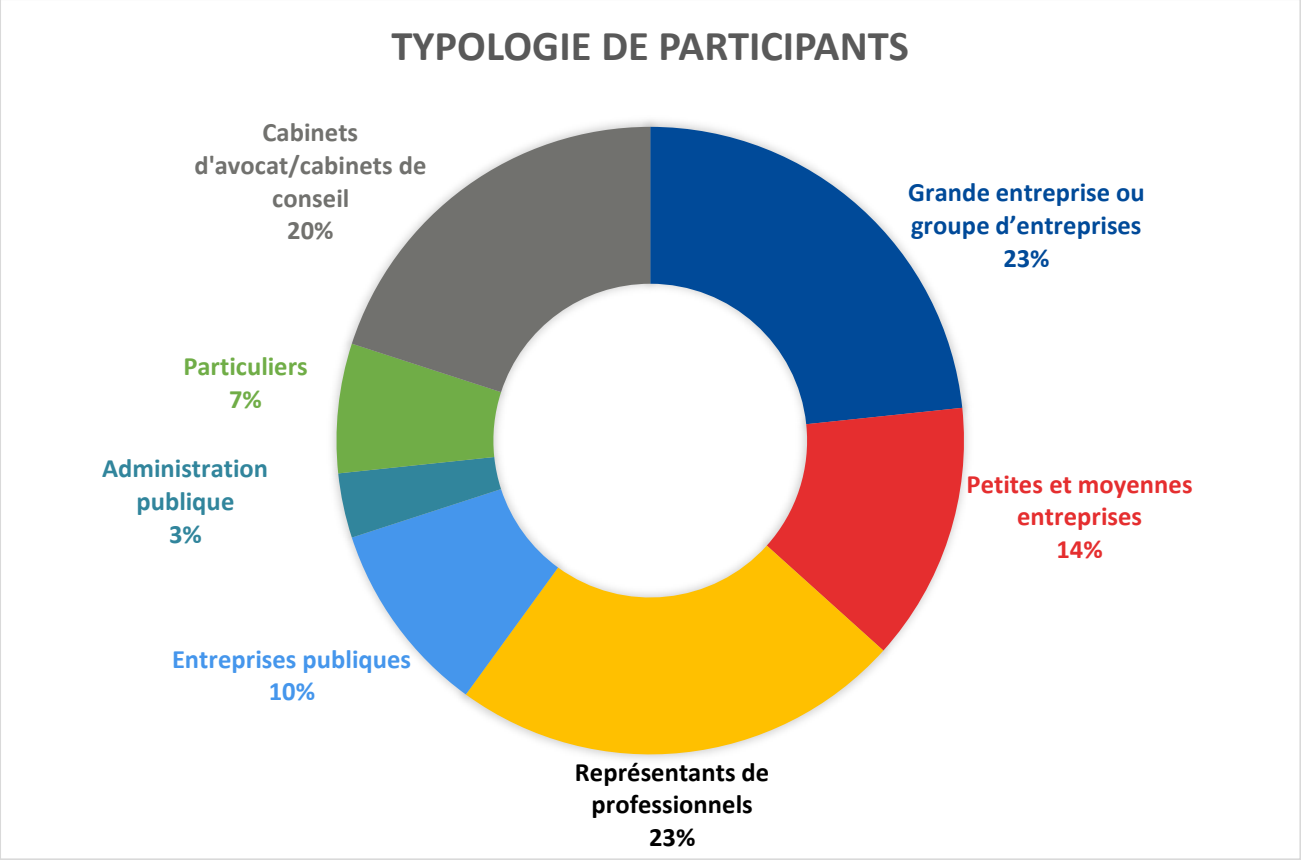
Le guide AITD constitue une méthodologie, qui identifie les étapes préalables à la réalisation d'une AITD et différents éléments à prendre en compte lors de la réalisation d'une AITD. Il donne des indications sur la manière dont l'analyse peut être menée en suivant les six étapes établies dans les recommandations du CEPD, et renvoie vers la documentation pertinente. Il ne constitue pas une évaluation des législations et pratiques des pays tiers, et des risques afférents. Son utilisation n'est pas obligatoire, d'autres éléments peuvent également être pris en compte et d'autres méthodologies appliquées.

Le projet de guide a fait l'objet d'une consultation publique entre décembre 2023 et février 2024 en vue de la préparation de sa version définitive.

Quelques chiffres

La consultation a reçu 34 contributions émanant principalement de professionnels du secteur (délégués à la protection des données, avocats, consultants, têtes de réseaux professionnels). Ceux-ci représentent des acteurs de toutes tailles (groupes français et internationaux, petites et moyennes entreprises, réseaux professionnels/fédérations d'entreprises, etc.) et de secteurs divers (banque/finance, assurance, transport, industrie, numérique/IT, cosmétique/santé, , administrations et collectivités territoriales, etc.).

- 75 % des participants à la consultation sont des experts (délégués à la protection des données, juristes, avocats ou consultants en protection des données)
- 23 % des participants sont des représentants d'associations professionnelles
- 23 % des participants sont de représentants de grandes entreprises



Ces contributions ont permis à la CNIL de faire évoluer, sur la forme comme sur le fond, son guide afin d'y apporter un certain nombre de clarifications et précisions sur son contenu et de consolider, ou ajuster, certaines réflexions et analyses, afin de prendre en compte notamment les derniers avis du Comité européen sur la protection des données.

Principales remarques reçues et réponses de la CNIL

Nous présentons ci-dessous une synthèse des principales remarques que nous avons reçues et traitées. De nombreuses propositions de modification ont été incorporées dans la version finale du guide, mais nous ne les analysons pas ici car elles ne soulèvent pas des points structurants du guide.

Sur les difficultés des acteurs de petite et moyenne taille à réaliser des AITD

Remarque : Plusieurs organismes ont partagé leur regret que le guide prévoie la même approche indépendamment de la taille de l'organisme : que les petites et moyennes entreprises, les artisans ou les professions libérales soient mis sur le même pied d'égalité avec les entreprises multinationales. D'autres, même de grande taille, ont évoqué la grande difficulté à laquelle font face les entreprises européennes et les administrations à analyser le cadre juridique et les pratiques dans les pays tiers.

Réponse CNIL : Le RGPD prévoit une approche homogène indépendamment de la taille des acteurs. La CJUE qui a instauré l'exercice de l'analyse d'impact des transferts de données et le Comité européen de protection des données (CEPD) qui a fourni une méthodologie à travers ses Recommandations 01/2020, prévoient une approche homogène peu importe la taille de l'organisme. Ceci dit, le degré des vérifications effectuées dans une AITD dépendra des moyens dont dispose l'exportateur et de l'aide fournie par l'importateur.

Ce guide contient une proposition de méthodologie afin de mener une AITD complète, y compris quelques sections optionnelles, avec des informations qui peuvent aider l'exportateur dans son évaluation.

Le guide s'organise autour des 6 étapes recommandées par le CEPD : 1) Connaître son transfert ; 2) Recenser l'outil de transfert utilisé ; 3) Evaluer la législation et les pratiques du pays de destination des données et l'efficacité de l'outil de transfert ; 4) Identifier et adopter des mesures supplémentaires ; 5) Mettre en œuvre les mesures supplémentaires et les étapes procédurales nécessaires et 6) Réévaluer à intervalles réguliers. La description du transfert (dans l'étape 1) permet, en particulier, que ses caractéristiques et sa sensibilité soient prises en compte pour évaluer la législation et les pratiques du pays de destination des données et l'efficacité de l'outil de transfert (à l'étape 3) et pour évaluer les mesures supplémentaires à mettre en place (à l'étape 4).

Nous sommes aussi conscients des difficultés dont font face les organismes de petite ou moyenne taille notamment dans leur évaluation des législations et des pratiques des pays tiers. Lorsqu'ils agissent en tant qu'exportateurs, nous les incitons à solliciter l'aide de l'importateur des données et à lui demander de fournir toute information utile permettant au responsable de traitement de réaliser l'analyse de la législation locale et des pratiques des autorités publiques en matière d'accès (cf. également la question suivante). Nous les invitons aussi à s'appuyer sur des analyses existantes telles que « la carte du monde de la protection des données » sur le site de la CNIL, des rapports d'organisations internationales réputées, des analyses d'experts telles que les analyses commandées par le CEPD pour certains pays (Russie, Inde, Chine, Brésil, Mexique, Turquie). Nous les invitons enfin à partager leurs analyses à travers des associations professionnelles, des réseaux de délégués à la protection des données, ainsi que des groupes d'entreprises ou d'administrations.

Sur la responsabilité pour la réalisation de l'AITD

Remarque : La plupart des organismes ont soulevé la question de savoir quelle entité dans une chaine de traitement est responsable de la réalisation d'une AITD. Plusieurs ont évoqué l'absence de coopération active de l'importateur qui constitue le frein principal à la réalisation de l'AITD vu la difficulté et le cout élevé associé à l'évaluation de la législation et des pratiques du pays tiers.

Réponse CNIL : La question de la responsabilité pour la réalisation de l'AITD dépend du rôle des acteurs dans le transfert (exportateur/importateur) et dans le traitement (responsable de traitement/sous-traitant). Nous avons inclus 3 scénarii afin d'adresser les cas les plus habituels rencontrés dans la pratique. Ces scénarii sont alignés avec l'avis 22/2024 du CEPD concernant la responsabilité des responsables de traitement dans une longue chaine de sous-traitance.

En principe, 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.

- **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** : Dans ce cas, le responsable de traitement est tenu de réaliser l'AITD avec la collaboration du sous-traitant.

- **Cas 2 - Sous-traitant dans l'EEE agissant en tant qu'exportateur transférant des données vers un sous-traitant ultérieur agissant en tant qu'importateur dans un pays tiers :** Dans ce cas, il incombe au sous-traitant de s'assurer de la conformité de son transfert et de réaliser l'AITD. 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, y compris l'AITD réalisée. En vertu de l'article 28(1) du RGPD, le responsable de traitement est tenu de vérifier les garanties proposées par le sous-traitant exportateur. Il peut s'appui sur les informations reçues du sous-traitant, y compris l'AITD.

- **Cas 3 : Responsable de traitement dans l'EEE agissant en tant qu'exportateur transférant des données vers un responsable de traitement dans un pays tiers :** Dans ce cas, le responsable de traitement – exportateur est tenu de réaliser l'AITD avec la collaboration du responsable de traitement – importateur.

Sur la définition de la notion de transfert

Remarque : Plusieurs organismes ont demandé que le guide définisse la notion de transfert, ainsi que les notions d'importateur et d'exportateur des données en citant des exemples de transferts. Les organismes ont soulevé plusieurs cas complexes : (i) le cas des transferts d'un responsable de traitement vers un sous-traitant dans l'EEE qui effectuent une transmission ultérieure de données à nouveau vers le même ou un autre pays tiers ; (ii) le cas des transferts intragroupes ; (iii) le cas des salariés qui télétravaillent depuis des pays tiers et (iv) le cas de collecte directe des données par un responsable de traitement dans un pays tiers.

Réponse CNIL : Nous avons fait le choix de nous référer aux travaux du Comité européen de protection de données (CEPD) qui a élaboré ces définitions dans ses 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. Au-delà des définitions, ces Lignes directrices contiennent 11 exemples qui clarifient les cas les plus récurrents de transferts des données. La CNIL publiera aussi, dans les mois à venir, un guide général sur les transferts des données.

Sur le périmètre de l'AITD

Remarque : Un nombre important d'organismes ont soulevé la question de savoir jusqu'où va l'obligation de réaliser une AITD dans le cadre d'une chaine de sous-traitance longue. Plusieurs ont évoqué le fait que les responsables de traitement ne disposent pas des moyens de mener une AITD pour chacun des transferts ultérieurs de données envisagés par chacun de leurs prestataires.

Réponse CNIL : Nous avons ajouté au guide une nouvelle section (2.4) qui répond à cette question. Dans son avis 22/2024, le CEPD précise que l'exportateur doit prendre en considération dans son analyse l'ensemble du cycle de vie des données, y compris les transferts ultérieurs, afin que le responsable du traitement (qu'il soit lui-même l'exportateur ou pas) puisse évaluer les risques liés à tous les transferts de données en dehors de l'UE.

Une AITD peut concerner un seul transfert ou un ensemble de transferts. L'exportateur a donc le choix de documenter son analyse au sein du même ou de plusieurs documents. En cas de changement dans la chaine de transfert, il pourra rattacher sa nouvelle analyse aux analyses préexistantes qu'il a déjà menées. Si l'exportateur est sous-traitant, il doit partager ces informations avec le responsable de traitement.

Sur la description du transfert (étape 3.1)

Remarque : Plusieurs organismes ont fait des propositions de reformulation des sections dans cette partie du guide.

Réponse CNIL : Nous avons accepté la grande majorité de ces propositions. La nouvelle section est plus simple sur certains aspects (ex. suppression de la « nature des activités de l'exportateur ») et plus précise sur d'autres (ex. ajout d'exemples sur la méthode de transfert, ajout d'une liste de catégories de données transférées). Nous avons fait le choix de ne pas préciser certains éléments malgré les demandes comme par exemples les catégories de personnes concernées car très aléatoire d'un organisme à l'autre. D'autres informations ont été ajoutées, mais restent optionnelles : caractère total ou partiel du transfert, volume des données et nombre de personnes concernées.

Sur le choix de l'outil du transfert (étape 3.2)

Remarque : Plusieurs organismes ont soulevé le fait que le choix d'outil vient en amont de la réalisation de l'AITD, puisque cette dernière n'est pas obligatoire en cas de transfert vers un pays adéquat ou en cas d'utilisation des dérogations de l'article 49

Réponse CNIL : Nous avons simplifié cette partie qui ne liste désormais que les outils de transfert de l'article 46 du RGPD. Les éléments relatifs à l'adéquation et aux dérogations sont développés dans la partie introductive 2.2. et feront l'objet des travaux ultérieurs (cf. ci-dessus sur un guide général sur les transferts).

Sur l'évaluation de la législation et des pratiques du pays de destination des données et l'efficacité de l'outil de transfert (étape 3.3)

Remarque : Plusieurs organismes ont informé la CNIL qu'ils font face à un grand nombre de difficultés pour évaluer la législation et la pratique du pays de destination des données. Ces difficultés commencent dès la collecte d'informations, et l'assurance de trouver des informations fiables, et se poursuivent également lorsqu'il s'agit de suivre l'évolution de la législation comme de la pratique du pays de destination. L'analyse de l'État de droit dans les pays tiers s'avère particulièrement complexe et couteuse nécessitant une connaissance approfondie du droit local et des pratiques. Si certaines grandes entreprises peuvent disposer de services juridiques compétents en interne, il n'en va pas de même des artisans, des professionnels libéraux et des petites ou moyennes entreprises. Par ailleurs, le sujet étant complexe et en fonction du pays concerné, même les entreprises bénéficiant d'un service juridique compétent en interne sont susceptibles de devoir faire appel à des conseils externes spécialisés.

D'ailleurs, certains soulèvent que la notion de « problème d'État de droit » n'est pas claire en ce qu'elle ne renvoie pas à des critères juridiques précis.

D'autres nous invitent à prendre position sur ces points qui vont être communs à tous les exportateurs ou réclament que cette analyse soit faite au niveau de l'EEE. Ils invitent la CNIL ou le CEPD à mettre à disposition de ces exportateurs un référentiel des législations et des pratiques applicables aux pays non couverts par une décision d'adéquation.

Certains ajoutent que l'appréciation des législations nationales relève d'enjeux politiques et économiques qui échappent à la simple relation contractuelle entre un exportateur et un importateur de données.

Plusieurs organismes évoquent enfin le côté subjectif de l'évaluation et du risque de fragmentation dans l'application du Chapitre V du RGPD.

Réponse CNIL : Nous sommes conscients des difficultés liées à l'analyse de la législation et des pratiques des pays tiers. Pour répondre autant que possible à ces problèmes, nous avons modifié l'étape 3.3 du guide afin de mettre en avant (i) la nécessité de la collaboration de l'importateur des données qui est censé connaître sa législation locale et les pratiques des autorités compétentes dans son pays ou a minima qui est mieux placé pour obtenir ces informations ; (ii) les ressources sur lesquels peuvent s'appuyer les exportateurs pour mener leur évaluation.

Ces ressources incluent « la carte du monde de la protection des données » sur le site de la CNIL (régulièrement mise à jour), les rapports des organisations internationales réputées et les analyses d'experts telles que les analyses commandées par le CEPD pour certains pays (Russie, Inde, Chine, Brésil, Mexique, Turquie). Nous invitons aussi les exportateurs à partager leurs analyses à travers des associations professionnelles, des réseaux de délégués à la protection des données, ainsi que des groupes d'entreprises ou d'administrations.

De manière générale, l'analyse de la législation et des pratiques des pays tiers ne relève pas des compétences de la CNIL. Une telle analyse est effectuée par la Commission européenne dans ses décisions d'adéquation conformément à l'article 45 du RGPD, mais il ne revient pas aux autorités nationales de protection des données d'effectuer une telle évaluation. Par ailleurs, cette analyse ne peut pas être dissociée de l'analyse des conditions spécifiques à chaque transfert et des particularités du traitement que seuls l'exportateur et l'importateur maitrisent.

Sur l'évaluation de l'indépendance des autorités de protection des données des pays tiers (étape 3.3)

Remarque : Certains organismes évoquent leur difficulté à analyser le degré d'indépendance des autorités de protection des données des pays tiers et invitent la CNIL à fournir une appréciation du degré d'indépendance des diverses autorités de protection des données ou à minima de préciser des critères d'évaluation de l'indépendance de l'autorité.

Réponse CNIL : Comme pour l'analyse des législations et des pratiques dans les pays tiers, l'appréciation du degré d'indépendance des diverses autorités de protection des données dans le monde ne relève pas de la compétence de la CNIL. Afin d'aider les exportateurs dans leur appréciation, nous avons ajouté quelques éléments qu'ils peuvent prendre en compte : les articles 52 à 54 du RGPD ; l'article 15 de la Convention 108+ du Conseil de l'Europe ; les travaux de l'Assemblée mondiale pour la protection de la vie privée (GPA) ; les travaux plus généraux de l'Organisation de coopération et de développement économiques (OCDE).

Sur la preuve à apporter d'absence d'accès par les autorités du pays tiers aux données transférées (étape 3.3)

Remarque : Certains organismes évoquent la difficulté de démontrer que l'importateur 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 État membre de l'EEE.

Réponse CNIL : Nous avons ajouté que les exportateurs peuvent s'appuyer sur le rapport de transparence de l'importateur sur les demandes d'accès par les autorités aux données et nous avons limité la vérification dans le temps en indiquant que l'importateur doit démontrer que *au moins sur les dernières années*, 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 État membre de l'EEE.

Conformément aux Recommandations 01/2020 du CEPD (§43.3), nous avons également prévu les cas où si, malgré le fait que l'outil de transfert n'est pas effectif à la lumière de l'évaluation menée, l'exportateur n'a pas lieu de croire que la législation problématique sera appliquée en pratique aux données transférées, il peut décider de procéder au transfert sans mettre en œuvre de mesures supplémentaires. Dans ces cas exceptionnels, l'exportateur devra démontrer et documenter cette évaluation, le cas échéant en collaboration avec l'importateur et en tenant compte également de l'expérience d'autres acteurs opérant dans le même secteur et/ou dans des secteurs liés à des transferts similaires.

Sur l'évaluation des mesures existantes et des mesures supplémentaires (étape 3.4)

Remarque : Certains organismes ont demandé à la CNIL qu'elle oriente les organismes sur la démarche et la méthodologie à adopter pour procéder à l'évaluation des mesures existantes et des mesures supplémentaires et que la CNIL fournisse des exemples.

Réponse CNIL : Nous avons précisé en note de bas de page les points de contrôle que les exportateurs doivent vérifier avec l'aide des importateurs afin de s'assurer que les mesures de sécurité sont efficaces pour empêcher l'accès aux données par les autorités des pays tiers. Ces points de contrôle reprennent les cas d'usages développés par le CEPD dans ses Recommandations 01/2020.

Sur le caractère suffisant des mesures contractuelles et organisationnelles (étape 3.4)

Remarque : Plusieurs organismes ont noté que dans sa version initiale, le guide était plus strict que les Recommandations 01/2020 du CEPD en ce qu'il précise que « *les mesures contractuelles et organisationnelles ne sont pas suffisantes en elles-mêmes pour empêcher un éventuel accès aux données par les autorités du pays tiers et qu'ils doivent être complétés par des mesures techniques* ».

Réponse CNIL : Nous avons aligné la formulation de notre guide avec les Recommandations 01/2020. En tout état de cause, conformément à ces recommandations : « *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. En pareil cas, des mesures contractuelles ou organisationnelles peuvent compléter des mesures techniques et renforcer le niveau global de protection des données (par exemple, en introduisant des contrôles et en éliminant des automatismes pour contrer les tentatives des autorités publiques d'accéder aux données en violation des normes de l'Union).* »

Sur la mise en œuvre des mesures supplémentaires (étape 3.4)

Remarque : Certains organismes évoquent la difficulté à mettre en place ces mesures, notamment pour des professionnels libéraux et des petites et moyennes entreprises.

Pour d'autres acteurs de plus grande taille, le gain de la mise en conformité par rapport au besoin métier ne justifie parfois pas de dépenser du temps sur cet exercice. Les mesures de sécurité proposées par le CEPD et reprises dans le guide ne sont pas adaptées à un grand nombre de services, notamment l'hébergement de données en nuage et la mise à disposition de ressources techniques (requêtes SQL, HPC, etc.), ce qui rend impossible la mise en conformité de ces transferts de données.

Réponse CNIL : L'objectif même de l'AITD est de permettre à l'exportateur d'identifier des mesures qui permettraient d'empêcher un accès aux données transférées par des autorités de pays tiers qui agissent selon un cadre juridique qui ne prévoit pas de garanties appropriées pour les droits et libertés des personnes concernées. Dans les cas où aucune mesure de sécurité n'est adaptée au traitement envisagé ou que la mise en œuvre des mesures envisagées est trop couteuse, les responsables de traitement ou sous-traitants doivent s'abstenir du transfert envisagé.

Sur la cessation du transfert en cas de non-conformité (étape 3.4)

Remarque : Lorsque la réalisation de l'AITD mène à la conclusion qu'il n'est pas possible de mettre en place les mesures nécessaires afin d'assurer l'effectivité de l'outil de transfert, mais que le transfert est déjà en cours, certains organismes ont proposé d'adopter une approche par les risques en cessant immédiatement le transfert uniquement lorsque le traitement présente des risques élevés pour les droits et libertés des personnes concernées. Dans le cas contraire, c'est-à-dire en l'absence d'un tel risque élevé, certains organismes ont suggéré d'arrêter le transfert uniquement lorsque le contrat arrive à son échéance ou à l'expiration d'un certain délai.

De manière plus générale, plusieurs organismes évoquent l'impact considérable qu'une suspension de transfert peut avoir compte tenu du modèle des affaires actuelles de beaucoup d'entreprises qui hébergent leurs données chez des prestataires en dehors de l'UE.

Réponse CNIL : L'objectif même de l'AITD est de permettre à l'exportateur d'identifier des mesures qui permettraient d'empêcher un accès aux données transférées par des autorités de pays tiers, qui agissent selon un cadre juridique qui ne prévoit pas de garanties appropriées pour les droits et libertés des personnes concernées. Lorsque ceci n'est pas possible, le responsable du traitement ou sous-traitant doit s'abstenir du transfert ou l'arrêter s'il est déjà en cours. Les conditions nécessaires à la mise en œuvre de la décision d'arrêt doivent ensuite être déterminées au cas par cas.

Sur la réévaluation à intervalles appropriés de l'analyse (étape 3.6)

Remarque : Plusieurs acteurs ont soulevé les difficultés d'analyser régulièrement les lois et pratiques des pays tiers. Selon eux, ils ne peuvent pas être au courant de tout changement législatif et ils sont moins bien placés que les pouvoirs publics français et européens pour réaliser cet exercice de veille et d'évaluation, qui peut être mené au niveau institutionnel dans le cadre de relations interétatiques.

Réponse CNIL : Nous sommes conscients des difficultés des organismes dans l'anticipation de tels changements. Il est recommandé de suivre les actualités législatives sur la protection des données dans tous les pays dans lesquels l'exportateur transfère des données, afin de pouvoir mieux anticiper si la réévaluation de la protection des données dans ce pays s'avère nécessaire. En tout état de cause, ces intervalles appropriés sont à déterminer par l'exportateur 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 impliqué par le transfert.