



Les transferts de données à caractère personnel hors Union européenne

Avec la globalisation des échanges et l'utilisation croissante des nouvelles technologies tant dans la sphère privée que commerciale, le nombre de transferts de données à caractère personnel en dehors de la France ne cesse de croître.

Or, en principe, les transferts de données à caractère personnel hors du territoire de l'Union européenne sont interdits à moins que le pays ou le destinataire n'assure un niveau de protection suffisant.

Afin de suivre la lettre de la loi, la mention des « transferts hors de l'Union européenne » sera utilisée pour évoquer les transferts vers des pays tiers.

Il est à noter que cette interdiction de transferts ne concerne pas l'Islande, le Liechtenstein et la Norvège, puisque ces pays ont transposé les dispositions de la directive 95/46/CE dans leur législation nationale (ces pays et les 27 Etats membres de l'Union européenne constituent l'Espace économique européen).

De même, cette interdiction ne concerne pas les transferts vers les pays reconnus comme « adéquats » par la Commission européenne. A ce jour, c'est le cas d'Andorre, de l'Argentine, du Canada, des Iles Féroé, de l'Ile de Man, de Guernesey, de Jersey, d'Israël, de l'Uruguay et de la Suisse.

Pour les transferts hors de ces pays, plusieurs outils ont été développés pour permettre aux acteurs d'apporter un niveau de protection suffisant : les règles internes d'entreprise (ou BCR), les Clauses Contractuelles Types et l'adhésion aux principes du « Safe Harbor ».

La loi prévoit également des exceptions permettant de transférer des données vers des pays tiers sans qu'il n'existe pour autant un niveau de protection suffisant.

L'ensemble de ces mécanismes sont présentés dans ce guide afin de répondre aux interrogations du public sur les transferts de données personnelles hors de l'Union européenne.

Date de publication : novembre 2012

Sommaire

Les principes4

Les règles internes d'entreprise ou BCR (*binding corporate rules*)13

Les Clauses Contractuelles Types de la Commission européenne 19

Le Safe Harbor 33

Les exceptions36

Les principes

- Q1.** Qu'est-ce qu'un transfert de données à caractère personnel ?
- Q2.** Quelles dispositions régissent en France les transferts de données à caractère personnel ?
- Q3.** Dois-je respecter d'autres règles dans le cadre d'un transfert de données à caractère personnel ?
- Q4.** Quelles formalités dois-je accomplir auprès de la CNIL lorsque j'effectue un transfert hors de l'UE ?
- Q5.** Je suis CIL. Un transfert hors de l'UE est envisagé par mon organisme. Quelles formalités dois-je effectuer ?
- Q6.** Les transferts que j'effectue sont issus de traitements relevant du champ d'application d'une norme simplifiée¹ ou d'une autorisation unique². Suis-je dispensé de toute formalité concernant les transferts ?
- Q7.** Puis-je transférer des données personnelles pour une finalité différente que celle pour laquelle elles ont été initialement collectées ?
- Q8.** Dois-je informer les personnes concernées lorsque je transfère leurs données vers un pays tiers ?
- Q9.** Qu'est-ce que je risque en cas de non respect des règles en matière de transferts ?

Les parties au transfert

- Q10.** Qu'est-ce qu'un « responsable de traitement » ?
- Q11.** Qu'est-ce qu'un « sous-traitant » ?
- Q12.** Qu'est-ce qu'un « destinataire de données » ?
- Q13.** Pourquoi faut-il distinguer le responsable de traitement du sous-traitant dans le cadre de transferts de données à caractère personnel ?
- Q14.** Quels indices permettent de distinguer le responsable de traitement du sous-traitant ?

¹ Une norme simplifiée est une norme établie par la CNIL pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

² Une autorisation unique est une décision adoptée par la CNIL pour certains traitements qui relèvent de la demande d'autorisation (article 25 de la loi « Informatique et Libertés ») et qui répondent à une même finalité, qui portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Q1. Qu'est-ce qu'un transfert de données à caractère personnel ?

On parle de transfert de données à caractère personnel lorsque ces données sont transférées depuis le territoire européen vers un ou des pays qui n'appliquent pas les dispositions de la directive 95/46/CE (il s'agit des pays ni membres de l'Union européenne, ni membres de l'Espace économique européen). Le transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (ex : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex. d'un disque dur d'ordinateur à un serveur).

Exemples de transferts

Exemple 1 - Une entreprise souhaite sous-traiter la gestion des relances téléphoniques de ses clients à une société située au Maroc, pays situé hors de l'Union européenne.

Exemple 2 - Les données des salariés d'une multinationale sont centralisées par la maison mère située aux Etats-Unis. Les données personnelles des salariés français font donc l'objet d'un transfert vers les Etats-Unis.

Q2. Quelles dispositions régissent en France les transferts de données à caractère personnel ?

- **La loi Informatique et Libertés du 6 janvier 1978 modifiée³ et le décret du 20 octobre 2005 modifié pris pour l'application de la loi n°78-17 relative à l'informatique et aux libertés.**

Le principe est posé par l'article 68 de la loi⁴ : les transferts en dehors de l'Union européenne⁵ sont interdits.

Les exceptions sont prévues par l'article 69 de la loi⁶ :

Les transferts en dehors de l'Union européenne sont toutefois autorisés si le pays ou l'entreprise destinataire assure un niveau de protection suffisant aux données transférées.

Cette protection suffisante peut être apportée de plusieurs manières :

- **Légalement**, si le pays destinataire des données personnelles a une législation reconnue par une décision de la Commission européenne comme offrant une **protection suffisante**. C'est le cas d'Andorre, de l'Argentine, du Canada, des Iles Féroé, de l'Ile de Man, de Guernesey, de Jersey, d'Israël, de l'Uruguay et de la Suisse. Cette liste évolue et peut être consultée sur le site de la CNIL (www.cnil.fr).

³ Transposant la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

⁴ Transposant l'article 25 de la directive européenne 95/46/CE.

⁵ Plus précisément, ce sont les transferts en-dehors de l'Union européenne et de l'Espace économique européen qui sont interdits, dans la mesure où la Norvège, l'Islande et le Liechtenstein ont transposé la directive européenne 95/46/CE dans leur législation interne.

⁶ Transposant l'article 26 de la directive européenne 95/46/CE.

- **De manière contractuelle**, par la signature de **Clauses Contractuelles Types** adoptées par la Commission européenne entre l'entité exportatrice et l'entité importatrice de données personnelles, ou par l'adoption de **Règles internes d'entreprise** (ou **BCR**) qui constituent un code de conduite en matière de transferts de données personnelles depuis l'Union européenne vers des pays tiers.
- Lorsque l'entité importatrice est basée aux Etats-Unis et qu'elle adhère aux **principes du Safe Harbor**.
- **L'article 69** permet également d'opérer des transferts dans des **situations exceptionnelles**.

Q3. Dois-je respecter d'autres règles dans le cadre d'un transfert de données à caractère personnel ?

Un transfert de données hors Union européenne, comme une communication de données à un tiers sur le territoire français, constitue un traitement de données à caractère personnel. Il est soumis à ce titre à l'ensemble des dispositions de la loi du 6 janvier 1978 modifiée :

- Tout transfert de données doit avoir une **finalité déterminée, explicite et légitime** ;
- Les données transférées ne doivent **pas être traitées ultérieurement de manière incompatible** avec cette finalité ;
- Les données transférées doivent être adéquates, pertinentes et non **excessives** au regard de la ou des finalités pour lesquelles elles sont transférées ;
- Les **personnes** dont les données sont transférées doivent être **informées** de l'existence de ce transfert (Article 91 du décret de 2007) ;
- La **durée de conservation** par l'importateur des données transférées ne doit pas être excessive ;
- Les personnes concernées disposent d'un **droit d'accès** à leurs données qui sont transférées et d'un **droit de rectification**, ainsi que d'un **droit d'opposition**, pour des motifs légitimes, au transfert de leurs données ;
- Des **mesures techniques de sécurité** doivent être mises en place afin de protéger les données contre tout accès par un tiers non autorisé et contre toute destruction, altération ou diffusion non autorisées desdites données.

Q4. Quelles formalités dois-je accomplir auprès de la CNIL lorsque j'effectue un transfert hors de l'UE ?

Un transfert ne constitue pas un traitement autonome. En effet, il est nécessairement rattaché à un traitement principal, ayant une finalité plus globale que le simple fait de transférer des données à caractère personnel hors de l'UE.

Afin de déterminer la formalité à accomplir lorsqu'un transfert est envisagé, il convient donc d'analyser le transfert à la lumière du traitement principal auquel il est rattaché.

La formalité à accomplir dépend donc de la finalité du traitement principal auquel est rattaché le transfert.

Si le traitement principal relève du régime de la déclaration normale, il convient de remplir le formulaire « déclaration » et son onglet « transfert hors UE ». Vous recevrez donc deux courriers : un **récépissé** vous permettant de mettre en œuvre le traitement (pour la déclaration) et une **décision d'autorisation** pour transférer les données hors UE. Ce n'est qu'à la réception des deux courriers que vous pourrez mettre en œuvre le transfert.

Exemple

Le transfert à la maison-mère située au Japon de curriculum vitae et de lettres de motivation des candidats postulant aux offres d'emploi des différentes entités du groupe situées dans le monde entier dans le cadre de la centralisation du recrutement.

Le transfert n'est pas un traitement autonome, il relève d'un traitement principal : la gestion du recrutement. Le traitement principal relevant du régime de la déclaration normale, il incombera à l'organisme qui souhaite en transférer une partie vers le Japon de procéder à une déclaration en ligne et de remplir l'onglet « transfert » en précisant le pays (Japon).

Le fait de transférer n'est pas une finalité, ce n'est qu'une « fonctionnalité », un aspect du traitement.

CADRE JURIDIQUE DU TRANSFERT	REGIME DU TRAITEMENT PRINCIPAL	
	DECLARATION NORMALE	AUTRE FORMALITE APPLICABLE (DEMANDE D'AUTORISATION OU D'AVIS)
Pays dit de PROTECTION SUFFISANTE ou société américaine adhérente au « SAFE HARBOR »	DECLARATION NORMALE + ONGLET TRANSFERTS (POUR CIL : L'INSCRIPTION AU REGISTRE SUFFIT)	FORMALITE APPLICABLE + ONGLET TRANSFERTS
Recours aux EXCEPTIONS article 69 de la loi Informatique et Libertés (appréciation restrictive de la CNIL : limitation aux cas ponctuels et exceptionnels)	DECLARATION NORMALE + ONGLET TRANSFERTS (POUR CIL : L'INSCRIPTION AU REGISTRE SUFFIT)	FORMALITE APPLICABLE + ONGLET TRANSFERTS
CLAUSES CONTRACTUELLES TYPES ou « BINDING CORPORATE RULES » (règles internes au sein d'un même groupe)	DECLARATION NORMALE + ONGLET TRANSFERTS ➔ LE TRANSFERT FERA L'OBJET D'UNE DECISION DE LA CNIL L'AUTORISANT	FORMALITE APPLICABLE + ONGLET TRANSFERTS

Les formalités sont à effectuer en ligne sur le site Internet de la CNIL : <http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil/>.

Q5. Je suis CIL. Un transfert hors de l'UE est envisagé par mon organisme. Quelles formalités dois-je effectuer ?

Si les transferts hors UE sont effectués à destination de pays reconnus comme offrant un niveau de protection suffisant, à destination de sociétés américaines ayant adhéré aux principes du Safe Harbor, ou reposent sur une exception de l'article 69, l'inscription de ces transferts dans le registre du CIL est suffisante.

En revanche, vous devrez quand même obtenir une décision d'autorisation de la CNIL pour les transferts hors UE encadrés par la signature de Clauses Contractuelles Types adoptées par la Commission européenne ou par des règles internes d'entreprise (BCR). Si le traitement principal relève d'une déclaration normale, vous devrez compléter le formulaire en ligne de déclaration normale ainsi que l'onglet transfert. Seul le transfert fera l'objet d'une décision d'autorisation spécifique de la CNIL.

Q6. Les transferts que j'effectue sont issus de traitements relevant du champ d'application d'une norme simplifiée ou d'une autorisation unique. Suis-je dispensé de toute formalité concernant les transferts ?

Les normes simplifiées et les autorisations uniques étant d'interprétation stricte, les transferts ne seront couverts que si la norme simplifiée⁷ ou l'autorisation unique⁸ prévoit expressément la possibilité d'un transfert, dans la limite du champ prévu pour ce transfert.

Exemple de norme simplifiée ou d'autorisation unique prévoyant expressément la possibilité d'un transfert

- Norme simplifiée 46 relative à la mise en œuvre de traitements portant sur la gestion du personnel,
- Norme simplifiée 48 relative aux traitements portant sur la gestion des fichiers de clients et de prospects,

⁷ Une norme simplifiée est une norme établie par la CNIL pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

⁸ Une autorisation unique est une décision adoptée par la CNIL pour certains traitements qui relèvent de la demande d'autorisation (article 25de la loi « Informatique et Libertés) et qui répondent à une même finalité, qui portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

- Autorisation unique 004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle,
- Autorisation unique 003 relative aux traitements de données à caractère personnel mis en œuvre par des organismes financiers relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi qu'à l'application des sanctions financières
- Méthodologie de référence 1 pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales.

Reportez-vous aux délibérations qui concernent les traitements que vous envisagez de mettre en œuvre : <http://www.cnil.fr/en-savoir-plus/deliberations/>

Q7. Puis-je transférer des données personnelles pour une finalité différente que celle pour laquelle elles ont été initialement collectées ?

Non.

La loi Informatique et Libertés prévoit expressément que les données doivent être collectées pour une finalité déterminée. Elles ne doivent donc pas être réutilisées pour des finalités incompatibles avec les finalités initiales, sauf disposition légale spécifique. En conséquence, tout transfert de données hors de l'Union européenne pour une finalité incompatible avec celle pour laquelle les données ont été initialement collectées est illégal.

Tout nouveau transfert de données personnelles pour une nouvelle finalité doit être soumis à la CNIL.

Exemple

Des données personnelles collectées et traitées pour mettre en place un réseau social interne ne peuvent pas être transférées à des fins de prospection commerciale.

Q8. Dois-je informer les personnes concernées lorsque je transfère leurs données vers un pays tiers?

Oui.

Afin de garantir un traitement légitime des données personnelles, vous devez informer les personnes concernées, avant tout transfert, de ce que leurs données feront l'objet d'un transfert vers un pays tiers. Les personnes concernées doivent notamment être informées de la finalité du transfert, du ou des pays destinataires, de la nature des données transférées, de la ou des catégories de destinataires, du niveau de protection offert par le pays destinataires, ainsi que de leurs droits d'opposition (pour motifs légitimes), d'accès et de rectification.

Q9. Qu'est-ce que je risque en cas de non respect des règles en matière de transferts ?

En cas de non respect des règles de transferts de données hors de l'Union européenne, des sanctions pénales peuvent être prononcées par les juridictions compétentes (jusqu'à **300 000 euros d'amende pour les personnes physiques ou 1,5 million d'euros pour les personnes morales**⁹ et **5 ans d'emprisonnement**¹⁰).

Par ailleurs, la CNIL dispose également de pouvoirs propres de sanction. Ainsi, aux termes de l'article 45 de la loi de 1978 modifiée, elle peut :

- prononcer un avertissement qui peut être rendu public,
- mettre en demeure de faire cesser le manquement constaté dans un délai qu'elle fixe.

Après mise en demeure, la Commission peut prononcer à l'encontre du responsable de traitement :

- une sanction pécuniaire (allant de 150 000 euros pour le premier manquement à 300 000 euros en cas de manquements réitérés ou 5% du chiffre d'affaires dans la limite de 300 000 euros pour les entreprises)¹¹
- une injonction de cesser le traitement ou un retrait de l'autorisation accordée.

Les parties au transfert

Q10. Qu'est-ce qu'un « responsable de traitement » ?

Un responsable de traitement est défini par la loi comme « *la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement* »¹². Un responsable de traitement se caractérise donc par **son autonomie dans la mise en place et la gestion d'un traitement**. C'est lui qui décide de créer ou de supprimer le traitement. Il doit donc veiller au respect de toutes les obligations imposées par la loi.

Q11. Qu'est-ce qu'un « sous-traitant » ?

Le sous-traitant est la personne physique ou morale traitant des données à caractère personnel **pour le compte du responsable du traitement**. Le sous-traitant a pour mission d'exécuter des tâches sur les instructions et sous la responsabilité du responsable de traitement, exportateur des données.

Attention : tout traitement de données personnelles par un sous-traitant, ou transfert de données personnelles à un sous-traitant, ne peut être réalisé que :

- sur instruction du responsable de traitement,

et

⁹ Conformément aux articles 226-24 et 131-38 du Code pénal, l'amende prononcée à l'encontre de personnes morales peut être portée au quintuple du taux prévu pour les personnes physiques.

¹⁰ Articles 226-16 et 226-22-1 du Code pénal

¹¹ Articles 47 de la loi Informatique et Libertés

¹² Article 3-I de la loi de 1978 modifiée

- si un contrat garantissant notamment les mesures de sécurité et de confidentialité qui doivent être mises en place par le sous-traitant est signé¹³.

Q12. Qu'est-ce qu'un « destinataire de données » ?

Le destinataire de données est celui qui reçoit les données à caractère personnel qui sont exportées.

Q13. Pourquoi faut-il distinguer le responsable de traitement du sous-traitant dans le cadre de transferts de données à caractère personnel ?

Dans le cadre de clauses contractuelles, leurs obligations sont différentes. C'est pourquoi il existe différents modèles de contrats selon la qualité du destinataire (voir les informations ci-après relatives aux Clauses Contractuelles Types).

Dans le cadre de BCR, les transferts de données vers des entités externes au groupe doivent bénéficier d'un encadrement permettant d'atteindre un niveau de protection suffisant différent selon que le destinataire est responsable de traitement ou sous-traitant (notamment grâce aux Clauses Contractuelle Types).

Les exceptions, prévues à l'article 69 de la loi Informatique et Libertés du 6 janvier 1978 ne s'appliquent pas à la relation de responsable de traitement à sous-traitant.

Q14. Quels indices permettent de distinguer le responsable de traitement du sous-traitant ?

Plusieurs indices permettent d'orienter vers une qualification de responsable de traitement ou de sous-traitant.

Indices	Le prestataire pourra être qualifié de sous-traitant	Le prestataire pourra être qualifié de responsable de traitement
Transparence : Le prestataire de service se présente-t-il sous son nom propre ou sous le nom de son client ?	L'employé du centre d'appel en Tunisie se présente sous le nom du client.	Le centre d'appel en Tunisie se présente sous son propre nom.
Niveau d'instruction : Le niveau d'instruction donné par le client indique le degré d'autonomie laissé au prestataire. Par conséquent, il permet d'apprécier s'il est plus qu'un simple sous-traitant.	Le contrat de prestation et les directives données au cours de son exécution sont très précis dans les instructions et le niveau de qualité demandé.	Le contrat de prestation et les directives données au cours de l'exécution sont très généraux en termes d'instruction et laissent expressément une grande autonomie au prestataire.

¹³ Article 35 de la loi de 1978 modifiée

<p>Niveau de contrôle : Le degré de contrôle du client sur les prestations et sur les données révèle également la liberté dont peut disposer le prestataire.</p>	<p>La société audite son prestataire et lui demande des comptes régulièrement.</p>	<p>La société ne s'intéresse pas à la façon dont le prestataire réalise ses prestations et le laisse libre d'utiliser les données comme bon lui semble.</p>
<p>Expertise : Un prestataire qui dispose d'une expertise peut ainsi décider des moyens à mettre en place dans le cadre de la réalisation des prestations.</p>	<p>Le prestataire utilise l'infrastructure technique du client pour réaliser sa prestation.</p>	<p>Le prestataire expert dans son domaine impose des outils au client qui n'a pas de pouvoir de négociation, ne peut les modifier parce qu'il n'a pas les compétences, ou parce que l'outil est un outil qui ne fait pas l'objet d'un développement spécifique.</p>

Les règles internes d'entreprise ou BCR (*binding corporate rules*)

- Q1. Les BCR, qu'est-ce que c'est ?
- Q2. A quoi servent les BCR ?
- Q3. Quelles sont les entreprises concernées ?
- Q4. Quels sont les avantages des BCR ?
- Q5. Quelle est la première étape lorsque mon entreprise souhaite adopter des BCR ?
- Q6. Existe-t-il des documents auxquels je peux me référer pour rédiger les BCR ?
- Q7. Quelles sont les grandes étapes lorsque l'on recourt aux BCR ?
- Q8. Quelles procédures doivent être développées au sein de mon entreprise afin de mettre en œuvre les BCR ?
- Q9. De quels droits les individus peuvent-ils se prévaloir au titre des BCR ?
- Q10. Quelles formalités administratives dois-je effectuer lorsqu'un transfert hors UE est basé sur des BCR approuvées par la CNIL et par les autres autorités de protection des données compétentes ?

Q1. Les BCR, qu'est-ce que c'est ?

Les Binding Corporate Rules (ci-après BCR) désignent un **code de conduite interne** qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne.

Les BCR doivent être contraignantes et respectées **par toutes les entités du groupe, quel que soit leur pays d'implantation**, ainsi que par tous leurs **salariés**.

Q2. A quoi servent les BCR ?

Les BCR constituent une alternative aux Clauses Contractuelles Types puisqu'elles permettent d'assurer un **niveau de protection suffisant** aux données transférées hors de l'Union européenne. En ce sens, elles constituent également une alternative aux principes du Safe Harbor pour les transferts vers les Etats-Unis.

Q3. Quelles sont les entreprises concernées ?

Les entreprises concernées sont les **multinationales** exportant des données **depuis leurs entités** situées au sein de l'Union européenne **vers des pays tiers** n'assurant pas un niveau de protection équivalent à celui de l'Union européenne.

Q4. Quels sont les avantages des BCR?

Les BCR permettent...

- d'être en **conformité avec les principes** de la directive européenne 95/46/CE ;
- d'**uniformiser** les pratiques relatives à la protection des données personnelles au sein d'un groupe. ;
- de **prévenir les risques** inhérents aux transferts de données personnelles vers des pays tiers ;
- d'**éviter de conclure autant de contrats** qu'il existe de transferts au sein d'un groupe ;
- de **communiquer** sur la politique d'entreprise en matière de protection des données personnelles auprès de ses clients, partenaires et salariés et de leur assurer un niveau de protection satisfaisant lors des transferts de leurs données personnelles ;
- de constituer un **guide interne** en matière de gestion des données personnelles ;
- de placer la protection des données au rang des **préoccupations éthiques du groupe**.

Q5. Quelle est la première étape lorsque mon entreprise souhaite adopter des BCR ?

Lorsque votre entreprise souhaite adopter des BCR, elle doit tout d'abord désigner une autorité européenne de protection des données dite « chef de file », telle que la CNIL, qui sera en charge de la procédure de coopération avec les autorités des autres pays européens auprès desquelles vous déposerez des demandes d'autorisation de transfert sur la base des BCR. Cette autorité chef de file sera votre unique point de contact puisque c'est à cette autorité que votre entreprise présentera son projet de BCR.

Le service des affaires européennes et internationales de la CNIL vous accompagne dans la finalisation de votre document afin d'avoir un instrument juridique satisfaisant au regard des exigences posées par le G29.

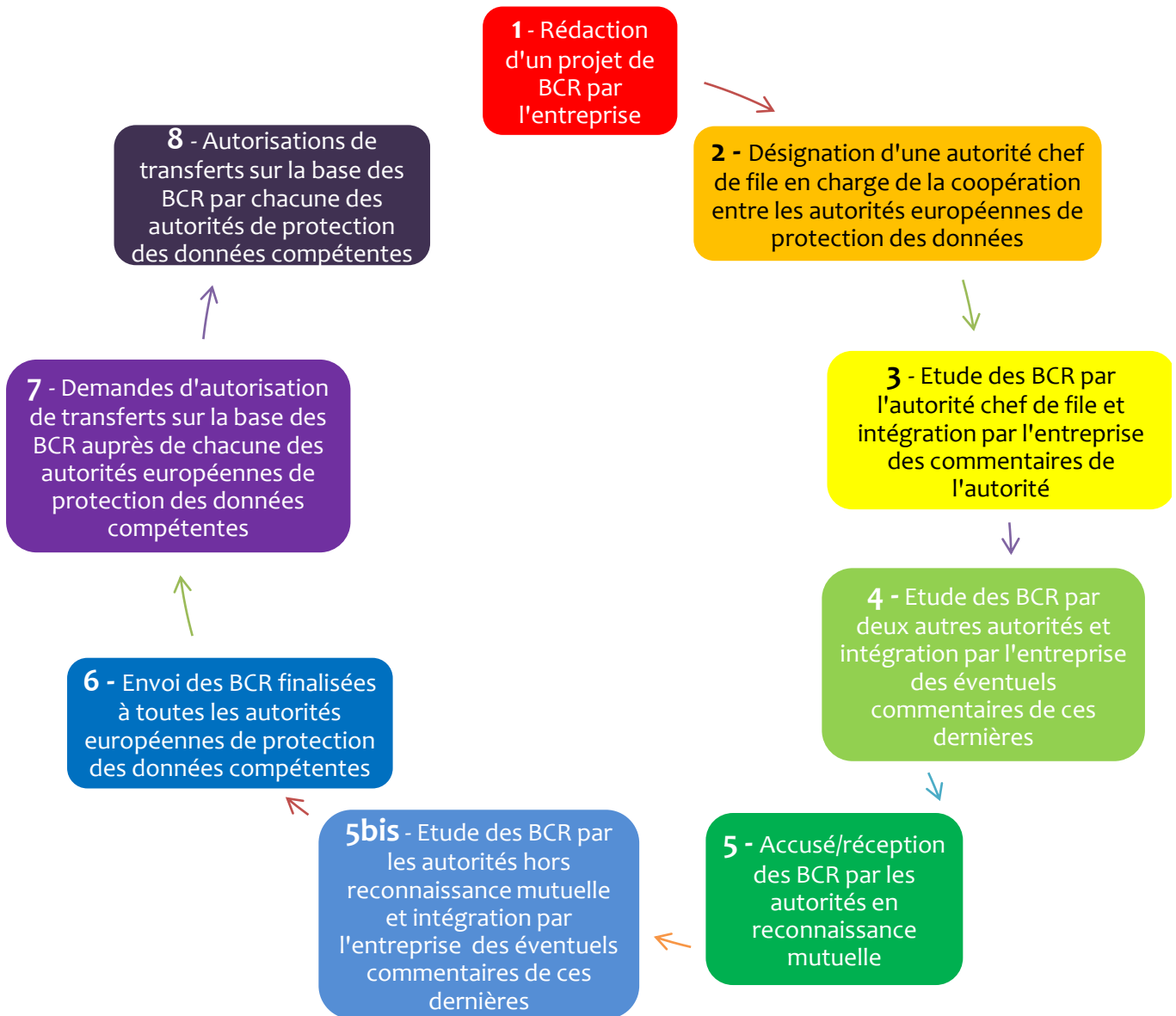
Q6. Existe-t-il des documents auxquels je peux me référer pour rédiger les BCR ?

Le G29 (Groupe des CNIL européennes) a adopté plusieurs documents présentant les exigences requises dans les BCR :

- Le WP154 est une véritable trame de BCR sur laquelle vous pourrez vous baser pour élaborer la structure de vos BCR.
- Le WP153 est une grille de lecture qui vous permettra de vérifier que tous les éléments exigés par le G29 sont présents dans vos BCR.
- Le WP155 est une foire aux questions qui permet de préciser certains points de droit.
- Le document de travail WP133 est le formulaire de demande officiel à remplir par l'entreprise afin que ses BCR soient étudiées par les autorités de protection des données européennes. Le WP133 est un formulaire composé de deux parties :
 - La partie I permet à l'entreprise de choisir officiellement l'autorité de protection qu'elle souhaite désigner comme autorité de coordination,
 - La partie II permet à l'entreprise de démontrer que les BCR qu'elle soumet aux autorités répondent aux exigences posées par le G29.

Ces documents sont téléchargeables sur le site internet de la CNIL (<http://www.cnil.fr/vos-responsabilites/transferer-des-donnees-a-letranger/les-bcr/>).

Q7. Quelles sont les grandes étapes lorsque l'on recourt aux BCR ?



A l'heure où nous publions ce guide, 21 Etats membres de l'Espace économique européen font partie de la reconnaissance mutuelle : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Espagne, Estonie, France, Irlande, Islande, Italie, Lettonie, Liechtenstein, Luxembourg, Malte, Norvège, Pays-Bas, République Tchèque, Royaume-Uni, Slovénie et Slovaquie.

Q8. Quelles procédures doivent être développées au sein de mon entreprise afin de mettre en œuvre les BCR ?

L'entreprise doit notamment s'engager à mettre en œuvre :

- Un régime de responsabilité pesant sur le siège européen ou sur la filiale européenne responsable par délégation de la protection des données (ou autre régime de responsabilité, sur justification),
- Une procédure de formation du personnel quant aux règles posées par les BCR,
- Une procédure d'audit,
- Une procédure interne de gestion des plaintes,
- Un réseau de responsables à la protection des données ou d'employés qualifiés pour la gestion des plaintes, la surveillance et le contrôle du respect des règles internes.

Q9. De quels droits les individus peuvent-ils se prévaloir au titre des BCR ?

Les personnes dont les données sont traitées et transférées par les groupes qui mettent en place des BCR pourront se prévaloir de tout manquement aux principes suivants :

- Limitation des finalités,
- Qualité et proportionnalité des données personnelles traitées,
- Traitement de données personnelles fondé sur une base légale,
- Information des personnes concernées par les traitements et accès aisé aux BCR par celles-ci,
- Droit d'accès, de rectification, d'effacement et de verrouillage des données, et objet du traitement,
- Droits en cas de décisions individuelles automatisées,
- Sécurité et confidentialité,
- Restrictions en cas de transferts ultérieurs en-dehors du groupe,
- Toute entité membre du groupe doit informer le responsable à la protection des données désigné au sein du groupe de l'existence d'une législation locale risquant d'empêcher cette entité de respecter les BCR,
- Mise en place d'un mécanisme interne de gestion des plaintes afin de recevoir les plaintes des personnes concernées,
- Devoir de coopération du groupe avec les autorités de protection des données personnelles compétentes
- Responsabilité juridique du groupe et voies de recours.

Q10. Quelles formalités administratives dois-je effectuer lorsqu'un transfert hors UE est basé sur des BCR approuvées par la CNIL et par les autres autorités de protection des données compétentes ?

Les formalités à accomplir auprès de la CNIL en matière de transferts internationaux doivent s'articuler avec les formalités relatives au traitement principal dont le transfert est issu.

Ainsi, la formalité qui devra être effectuée auprès de la CNIL est celle correspondante au régime juridique applicable au traitement principal (déclaration normale, demande d'autorisation ou demande d'avis).

Dans ce formulaire, il devra être précisé qu'un transfert de données vers un pays non-membre de l'Union européenne est envisagé et qu'il sera encadré par des règles internes d'entreprise (BCR).

Une fois le formulaire soumis à la CNIL, le déclarant recevra un récépissé pour le traitement principal, tandis que le transfert sera instruit en vue de la délivrance d'une décision autorisant le transfert.

Les formalités auprès de la CNIL s'effectuent en ligne sur le site internet www.cnil.fr, rubrique « Déclarer un fichier ».

Les Clauses Contractuelles Types de la Commission européenne

- Q1.** Qu'est-ce que les « Clauses Contractuelles Types » ?
- Q2.** Quelles sont les grandes étapes lorsque je souhaite avoir recours aux Clauses Contractuelles Types ?
- Q3.** Quelles sont les différentes Clauses Contractuelles Types ?
- Q4.** Mes transferts déjà existants de responsable de traitement à sous-traitant sont encadrés par les Clauses Contractuelles Types préexistantes. Dois-je signer les nouvelles clauses de 2010 afin de remplacer les anciennes ?
- Q5.** Pourquoi la Commission européenne a-t-elle publié de nouvelles Clauses Contractuelles Types pour encadrer les transferts de responsable de traitement à sous-traitant ?
- Q6.** Quelles nouvelles obligations ces clauses mettent-elles à la charge du sous-traitant et des éventuels sous-traitants ultérieurs ?
- Q7.** Où puis-je trouver les Clauses Contractuelles Types ?
- Q8.** Dois-je reprendre les Clauses Contractuelles Types in extenso ?
- Q9.** Quel est le régime de responsabilité applicable dans le cadre des Clauses Contractuelles Types permettant d'encadrer les transferts entre responsables de traitement ?
- Q10.** Quel est le régime de responsabilité applicable dans le cadre des Clauses Contractuelles Types permettant d'encadrer les transferts entre un responsable de traitement et un sous-traitant (aux termes des clauses de 2010 qui remplacent celles de 2001) ?
- Q11.** Quelles démarches dois-je effectuer lorsque j'ai recours à des Clauses Contractuelles Types ?

En pratique : hypothèses de transferts

- H1.** Transfert par un responsable de traitement UE vers un autre responsable de traitement situé hors UE
- H2.** Transfert par un responsable de traitement UE vers un sous-traitant situé hors UE
- H3.** Transfert par un responsable de traitement UE vers un autre responsable de traitement situé hors UE, qui transfère à son tour les données vers un autre responsable de traitement situé hors UE
- H4.** Transfert par un responsable de traitement UE vers un autre responsable de traitement situé hors UE, qui transfère à son tour les données vers un sous-traitant situé hors UE
- H5.** Transfert par un responsable de traitement UE vers un sous-traitant situé hors UE, qui transfère à son tour les données vers un autre sous-traitant situé hors UE

- H6.** Transfert par un responsable de traitement UE vers un sous-traitant UE, qui transfère à son tour les données vers un autre sous-traitant situé hors UE
- H7.** Transfert par un responsable de traitement UE vers un autre responsable de traitement UE, qui transfère à son tour les données vers un sous-traitant situé hors UE
- H8.** Transfert par un responsable de traitement UE vers un sous-traitant situé hors UE, qui transfère à son tour les données vers un responsable de traitement situé hors UE

Q1. Qu'est-ce que les « Clauses Contractuelles Types »?

Il s'agit de modèles de clauses contractuelles adoptées par la Commission européenne qui permettent d'encadrer les transferts de données personnelles hors de l'Union européenne. Elles ont pour but de faciliter la tâche des responsables de traitement dans la mise en œuvre de contrats de transfert.

Q2. Quelles sont les grandes étapes lorsque je souhaite avoir recours aux Clauses Contractuelles Types ?

Etape n°1 – Identifiez les parties, qualifiez le type de transfert de données personnelles effectué et identifiez les Clauses Contractuelles Types dont vous avez besoin (de responsable de traitement à responsable de traitement ou de responsable de traitement à sous-traitant)¹⁴.

Etape n°2 – Complétez les Clauses Contractuelles Types (notamment les Annexes sur la description des transferts)¹⁵.

Etape n°3 – Effectuez les démarches nécessaires auprès de la CNIL¹⁶.

Q3. Quelles sont les différentes Clauses Contractuelles Types ?

On distingue les transferts de responsable de traitement à responsable de traitement et les transferts de responsable de traitement à sous-traitant. Il existe donc deux types de clauses afin d'encadrer chacun de ces transferts.

➤ **Clauses contractuelles encadrant les transferts de données personnelles d'un responsable de traitement à un autre responsable de traitement**

Afin d'encadrer les transferts de données entre deux responsables de traitement, il existe deux ensembles de clauses contractuelles applicables aux transferts.

Le premier ensemble résulte de la décision de la Commission du 15 juin 2001 (2001/497/CE) et le second de la décision de la Commission du 24 décembre 2004 (2004/915/CE) modifiant la décision 2001/497/CE.

Les principales différences entre ces deux ensembles de clauses ont trait aux clauses de responsabilité, de règlement des litiges, aux modalités d'exercice de leurs droits d'accès par les personnes concernées et la coopération avec les autorités de protection des données.

➔ Vous devez choisir lequel de ces deux modèles de clauses vous souhaitez signer.

¹⁴ Cf. question 3 pour davantage d'information

¹⁵ Cf. question 8 pour davantage d'information

¹⁶ Cf. question 11 pour davantage d'information

➤ **Clauses contractuelles encadrant les transferts de données personnelles d'un responsable de traitement à un sous-traitant**

Les Clauses Contractuelles Types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers résultent de la décision de la Commission du 5 février 2010 (2010/87/UE). Ce jeu de clauses remplace, depuis le 15 mai 2010, les Clauses contractuelles antérieures de 2001 (décision 2002/16/CE).

Q4. Mes transferts déjà existants de responsable de traitement à sous-traitant sont encadrés par les Clauses Contractuelles Types préexistantes (2001). Dois-je signer les nouvelles clauses de 2010 afin de remplacer les anciennes ?

Non, ce n'est pas nécessaire.

Tout contrat conclu en vertu des Clauses Contractuelles Types de 2001 avant le 15 mai 2010 reste en vigueur dans son intégralité pour encadrer les transferts et les conditions de leur mise en œuvre.

Q5. Pourquoi la Commission européenne a-t-elle publié de nouvelles Clauses Contractuelles Types pour encadrer les transferts de responsable de traitement à sous-traitant ?

Les nouvelles Clauses Contractuelles Types de 2010 permettent de mieux prendre en compte les chaînes de sous-traitance que celles de 2001.

Q6. Quelles nouvelles obligations ces clauses mettent-elles à la charge du sous-traitant et des éventuels sous-traitants ultérieurs ?

Aux termes de ces nouvelles clauses contractuelles, un sous-traitant qui souhaite à son tour sous-traiter des données à caractère personnel devra au préalable obtenir l'accord écrit de l'exportateur pour le compte duquel les données sont transférées hors UE. Par ailleurs, le contrat conclu entre le sous-traitant initial et le sous-traitant ultérieur devra imposer à ce dernier les mêmes obligations que celles auxquelles est soumis le sous-traitant initial.

Q7. Où puis-je trouver les Clauses Contractuelles Types ?

Les Clauses Contractuelles Types sont téléchargeables sur le site internet de la CNIL : <http://www.cnil.fr/vos-responsabilites/le-transfert-de-donnees-hors-ue/contrats-types-de-la-commission-europeenne/>.

Vous pourrez également consulter sur cette page les questions-réponses rédigées par la Commission européenne sur les différents modèles de Clauses Contractuelles Types.

Q8. Dois-je reprendre les Clauses Contractuelles Types in extenso ?

Aucune disposition légale ne vous oblige à reprendre les Clauses Contractuelles Types in extenso. Cependant, une telle pratique est préférable.

En effet, dans le cadre de l'autorisation de transfert qu'elle délivre, la CNIL doit s'assurer que ce contrat accorde des « **garanties suffisantes** » ou un « **niveau de protection suffisant**», au sens de la directive 95/46/CE et de la loi Informatique et Libertés.

La CNIL appréciera donc le niveau de ces garanties par référence au niveau de protection résultant des Clauses Contractuelles Types émises par la Commission européenne.

Reprendre les Clauses Contractuelles Types, c'est s'assurer une procédure d'autorisation plus rapide et accroître la sécurité juridique de vos transferts.

Par ailleurs, vous pouvez librement décider d'ajouter des clauses supplémentaires du moment qu'elles ne contredisent pas directement ou indirectement les Clauses Contractuelles Types et ne portent pas préjudice aux libertés et droits fondamentaux des personnes dont les données sont transférées.

Q9. Quel est le régime de responsabilité applicable dans le cadre des Clauses Contractuelles Types permettant d'encadrer les transferts entre responsables de traitement ?

Le régime de responsabilité diffère selon que l'on se trouve dans le cadre des clauses contractuelles de 2001 ou dans celles de 2004.

- Aux termes des clauses de 2001, le régime de responsabilité repose sur un système de responsabilité solidaire des dommages subis par les personnes concernées ayant subi un dommage causé par le non respect des clauses contractuelles par l'exportateur, l'importateur ou par les deux. Les personnes concernées pourront donc obtenir des dommages et intérêts aussi bien auprès de l'exportateur de données que de l'importateur de données. En d'autres termes, en cas de violation des Clauses Contractuelles Types, les personnes concernées pourront poursuivre en justice l'exportateur de données, l'importateur de données ou les deux à la fois. Toutefois, cette responsabilité solidaire ne s'applique pas pour les violations qui ne portent pas préjudice aux personnes concernées. Dans ce cas, chaque partie sera responsable du traitement illicite qu'elle aura effectué.
- Aux termes des clauses de 2004, chaque partie est responsable envers l'autre partie des dommages qu'elle cause par suite d'un manquement aux présentes clauses. Ainsi, la responsabilité entre les parties se limite au dommage effectif subi par l'autre partie signataire.

De plus, chaque partie est responsable envers les personnes concernées des dommages qu'elle cause par suite d'une violation des droits des tiers au titre des présentes clauses, sans que cela n'affecte la responsabilité de l'exportateur de données en vertu de la loi sur la protection des données à laquelle il est soumis.

Aussi, d'une façon générale, la personne concernée pourra agir à l'encontre de l'exportateur ou de l'importateur de données pour les manquements respectifs à leurs obligations contractuelles.

Q10. Quel est le régime de responsabilité applicable dans le cadre des Clauses Contractuelles Types permettant d'encadrer les transferts entre un responsable de traitement et un sous-traitant (aux termes des clauses de 2010 qui remplacent celles de 2001)?

L'exportateur de données étant seul responsable de traitement, c'est lui qui endossera la responsabilité vis-à-vis des personnes concernées en cas de violation des règles applicables en matière de protection des données.

Les personnes concernées ne pourront rechercher la responsabilité de l'importateur de données que pour autant qu'il est responsable de la violation et uniquement si l'exportateur de données a disparu ou a cessé d'exister.

Il convient cependant de noter que l'exportateur tenu responsable en cas de violation des clauses contractuelles pourra se retourner contre l'importateur de données en cas de manquement commis par ce dernier.

Q11. Quelles démarches dois-je effectuer lorsque j'ai recours à des Clauses Contractuelles Types ?

Les formalités à accomplir auprès de la CNIL en matière de transferts internationaux doivent s'articuler avec les formalités relatives au traitement principal dont le transfert est issu.

Ainsi, la formalité que vous devrez effectuer auprès de la CNIL est celle correspondante au régime juridique applicable au traitement principal (déclaration normale, demande d'autorisation ou demande d'avis).

Dans ce formulaire, vous devrez préciser qu'un transfert de données vers un pays non-membre de l'Union européenne est envisagé et qu'il sera encadré par l'adoption de Clauses Contractuelle Types de la Commission européenne.

Vous n'avez pas à transmettre à la CNIL les Clauses Contractuelles Types conclues avec l'importateur des données, vous devez seulement les tenir à la disposition de la CNIL.

Toutefois, si vous avez modifié le contenu des Clauses Types, ce contrat de transfert devient « ad hoc » et nécessite d'être revu par les services de la CNIL afin de s'assurer que le niveau de protection des données à caractère personnel transférées est suffisant.

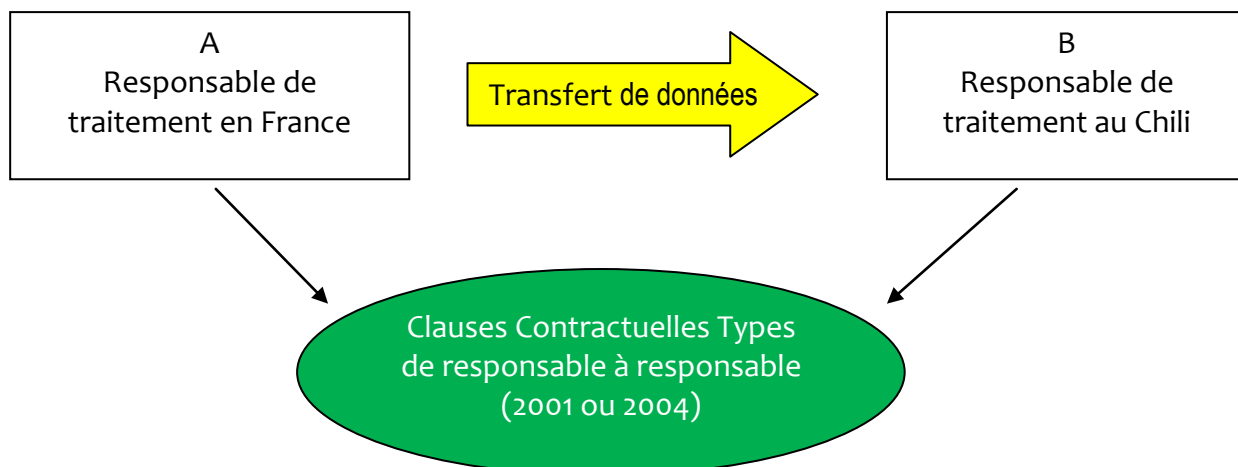
Une fois le formulaire soumis à la CNIL, le déclarant recevra un récépissé pour le traitement principal, tandis que le transfert sera instruit en vue de délivrer une autorisation de transfert.

Les formalités auprès de la CNIL s'effectuent en ligne sur le site internet www.cnil.fr, rubrique « Déclarer un fichier ».

En pratique : hypothèses de transferts

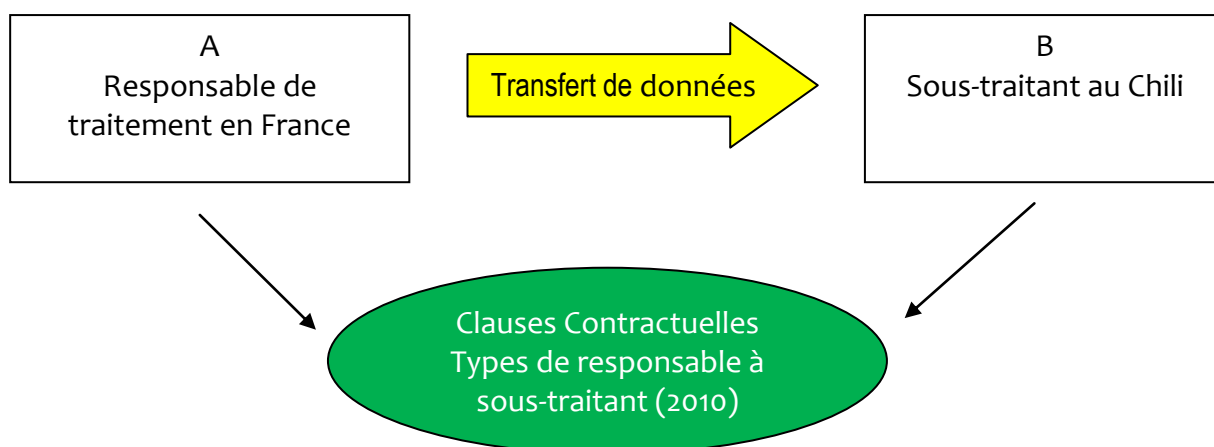
H1. Transferts de données personnelles par un responsable de traitement UE vers un autre responsable de traitement situé hors UE

A et B signent des Clauses Contractuelles Types de responsable de traitement à responsable de traitement (2001 ou 2004).



H2. Transferts de données personnelles par un responsable de traitement UE vers un sous-traitant situé hors UE

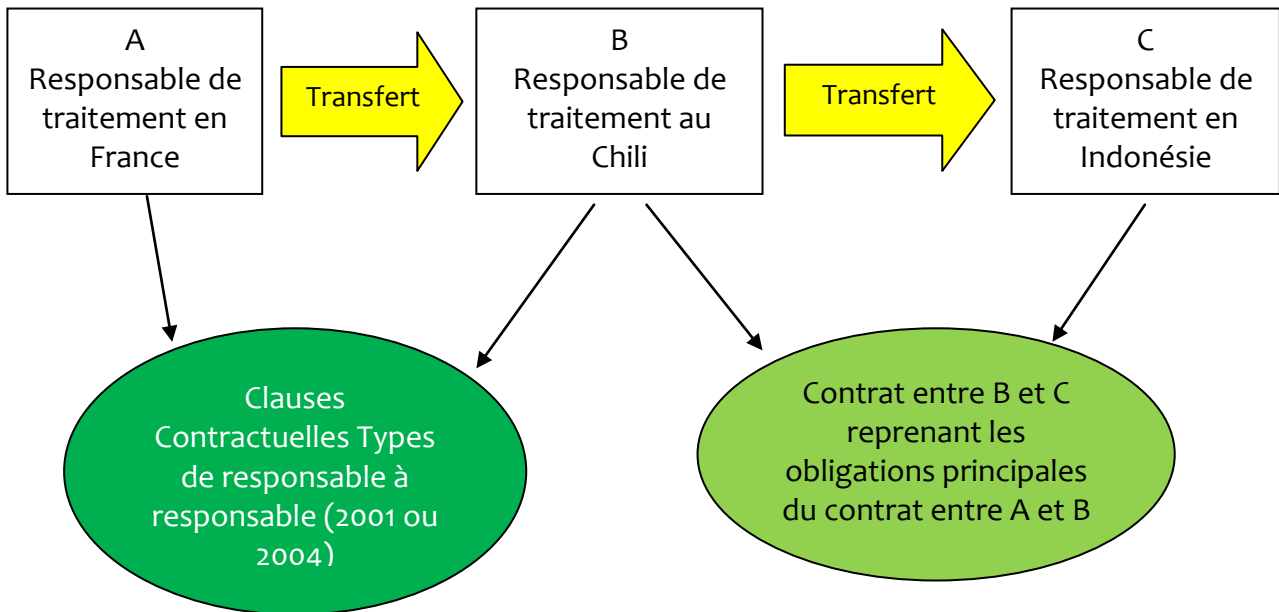
A et B signent des Clauses Contractuelles Types de responsable de traitement à sous-traitant (2010).



H3. Transferts de données personnelles par un responsable de traitement UE vers un autre responsable de traitement situé hors UE, qui transfère à son tour les données vers un autre responsable de traitement situé hors UE.

A et B signent des Clauses Contractuelles Types de responsable de traitement à responsable de traitement (2001 ou 2004).

Le transfert entre les deux responsables de traitement situés hors de l'Union européenne doit être encadré par un contrat qui reprend les mêmes obligations que celles contenues dans les Clauses Contractuelles Types entre A et B.



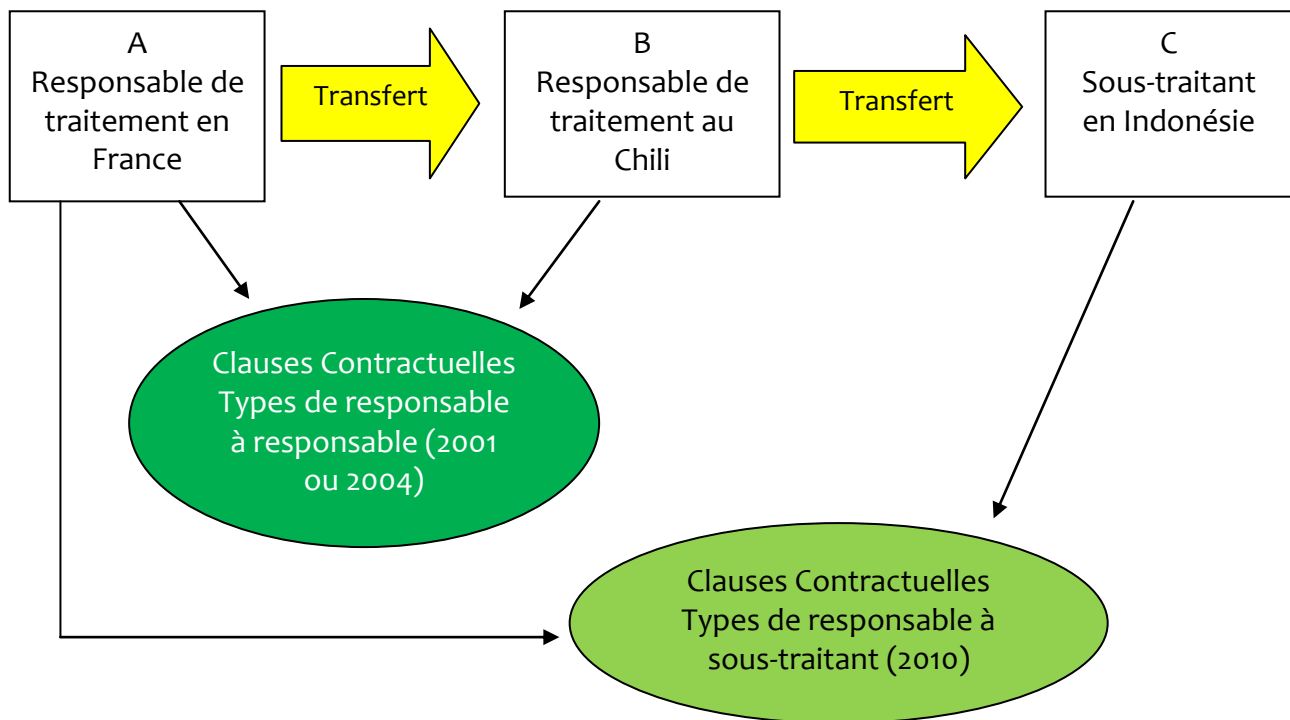
Dans le contrat qui lie A et B, il est nécessaire d'insérer une clause relative à l'obligation de B de signer un contrat équivalent aux clauses contractuelles (2001 ou 2004) avec C.

H4. Transferts de données personnelles par un responsable de traitement UE vers un autre responsable de traitement situé hors UE, qui transfère à son tour les données vers un sous-traitant situé hors UE → 2 options

Option 1

A et B signent des Clauses Contractuelles Types de responsable de traitement à responsable de traitement (2001 ou 2004).

A et C signent des Clauses Contractuelles Types de responsable de traitement à sous-traitant.

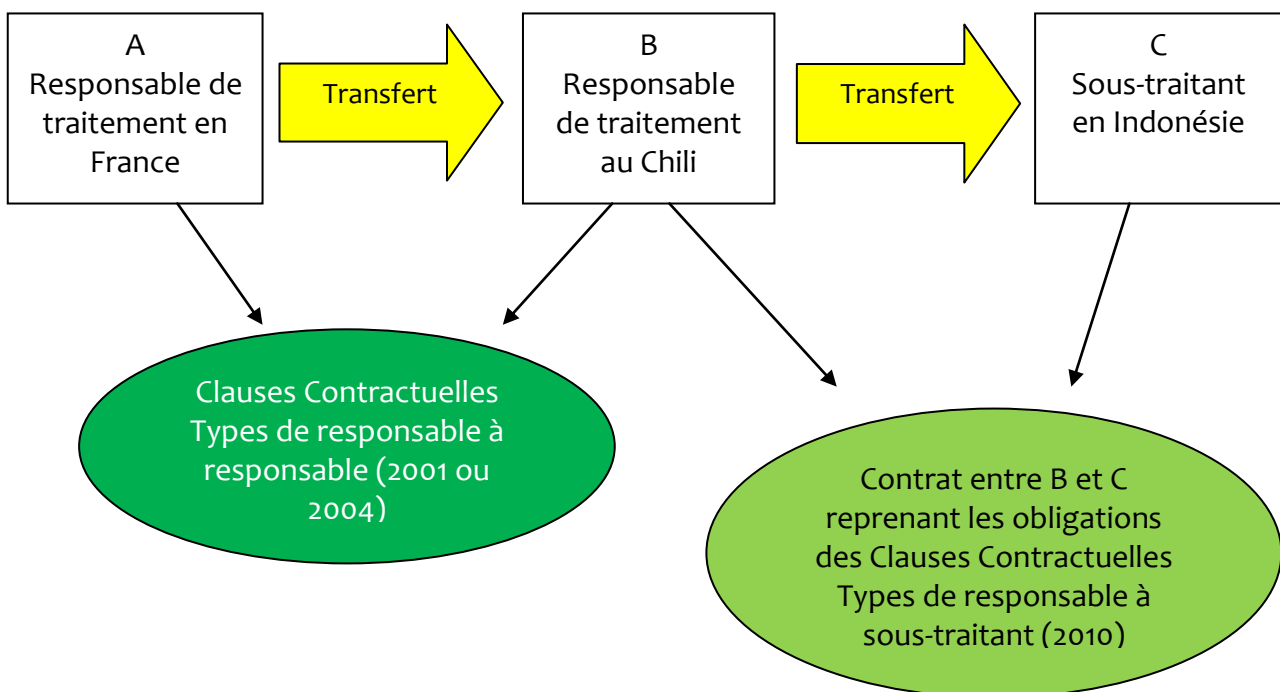


Option 2

A et B signent des Clauses Contractuelles Types de responsable de traitement à responsable de traitement (2001 ou 2004).

B étant responsable de traitement, il a également la possibilité de signer avec C un contrat équivalent aux Clauses Contractuelles Types de responsable de traitement à sous-traitant.

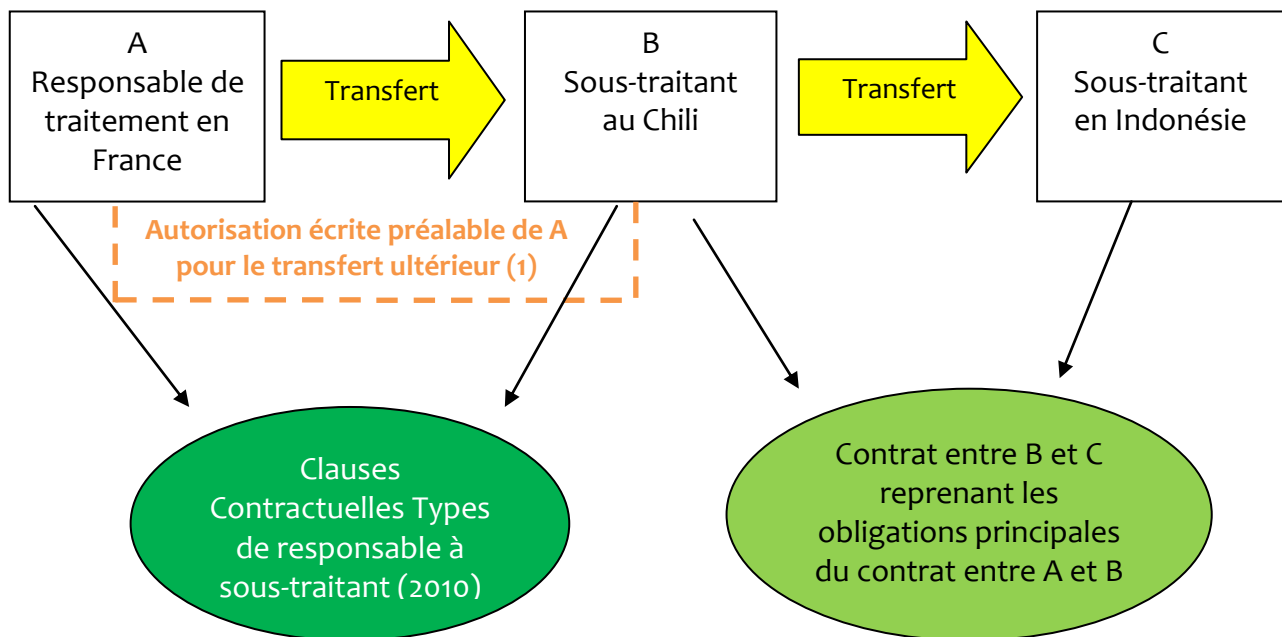
Dans le contrat qui lie A et B, il est nécessaire d'insérer une clause relative à l'obligation de B de signer avec C un contrat équivalent aux Clauses Contractuelles Types de responsable de traitement à sous-traitant (2010).



H5. Transferts de données personnelles par un responsable de traitement UE vers un sous-traitant situé hors UE, qui transfère à son tour les données vers un autre sous-traitant situé hors UE

A et B signent des Clauses Contractuelles Types de responsable de traitement à sous-traitant.

Le transfert entre les deux sous-traitants situés hors de l'Union européenne doit être encadré par un contrat qui reprend les mêmes obligations que celles contenues dans les Clauses Contractuelles Types entre A et B.



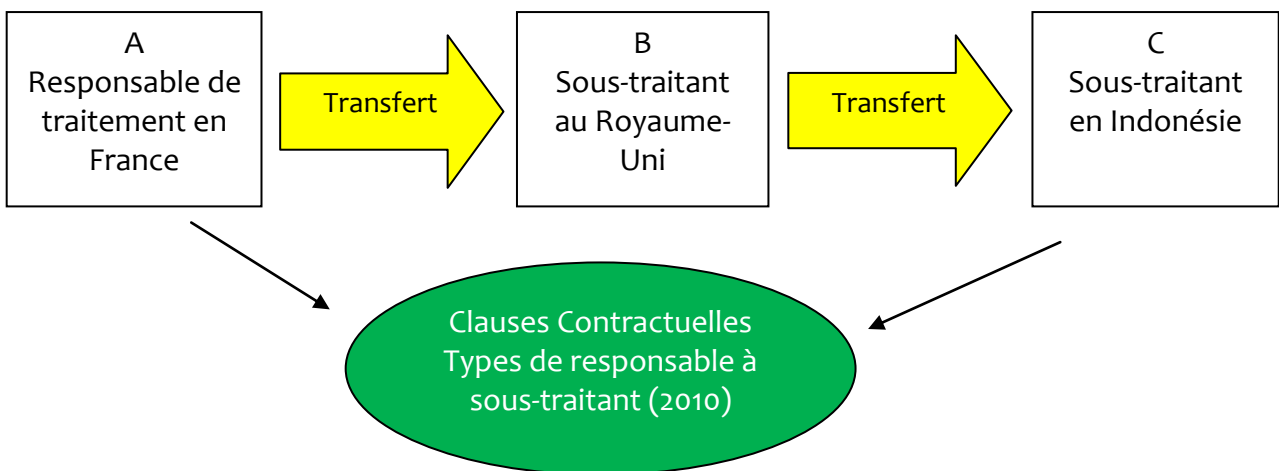
(1) L'accord écrit préalable du responsable de traitement (A) autorisant la sous-traitance ultérieure est expressément prévu par la les clauses de 2010 (clause 11, paragraphe 1). Cet accord peut être général ou spécifique pour chaque sous-traitance ultérieure.

H6. Transferts de données personnelles par un responsable de traitement UE vers un sous-traitant UE, qui transfère à son tour les données vers un autre sous-traitant situé hors UE : 2 options

A et B n'ont pas besoin de signer de Clauses Contractuelles Types de responsable de traitement à sous-traitant puisque les données restent au sein de l'Union européenne. En revanche, il faut encadrer le transfert entre B et C puisque ce dernier est situé en-dehors de l'Union européenne. B étant sous-traitant, il ne peut pas conclure de Clauses Contractuelles Types avec C qui est également sous-traitant. Deux options sont envisageables.

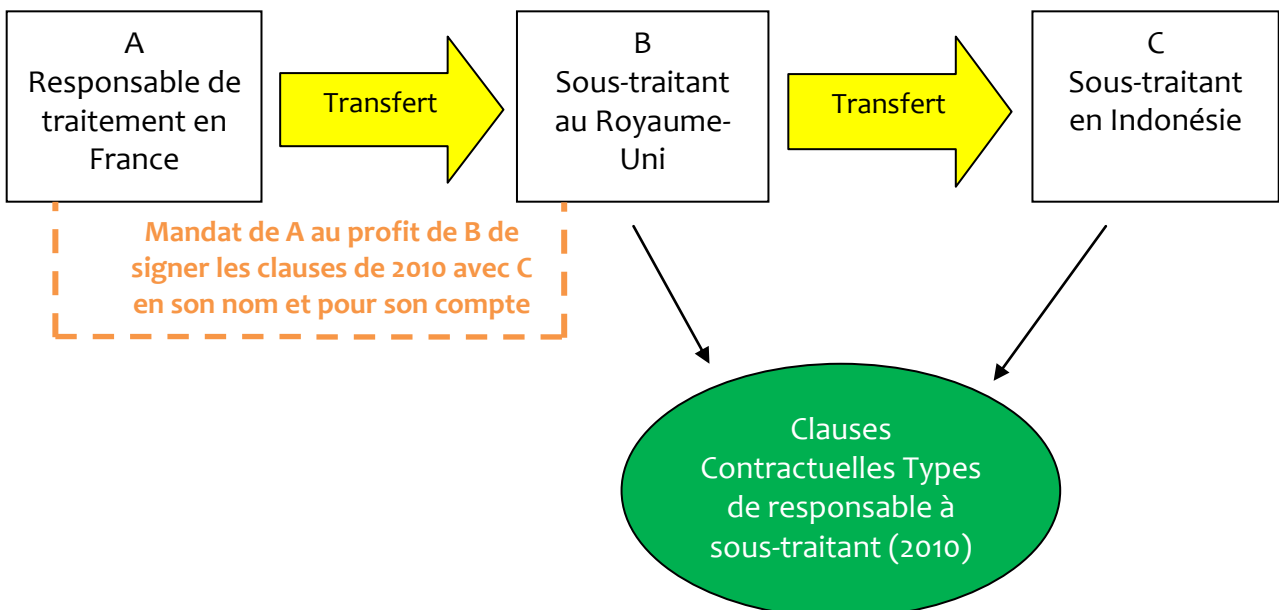
Option 1

A et C signent des Clauses Contractuelles Types de responsable de traitement à sous-traitant.



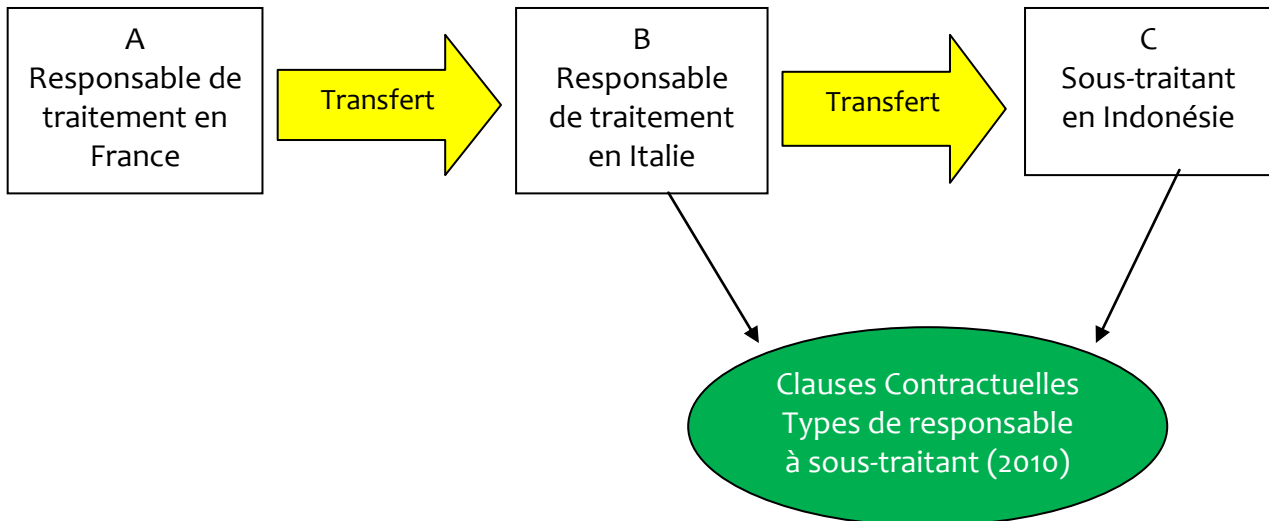
Option 2

B signe avec C les Clauses Contractuelles Types de responsable de traitement à sous-traitant au nom et pour le compte de A (en vertu d'un mandat de A au profit de B).



H7. Transferts de données personnelles par un responsable de traitement UE vers un responsable de traitement UE, qui transfère à son tour les données vers un sous-traitant situé hors UE

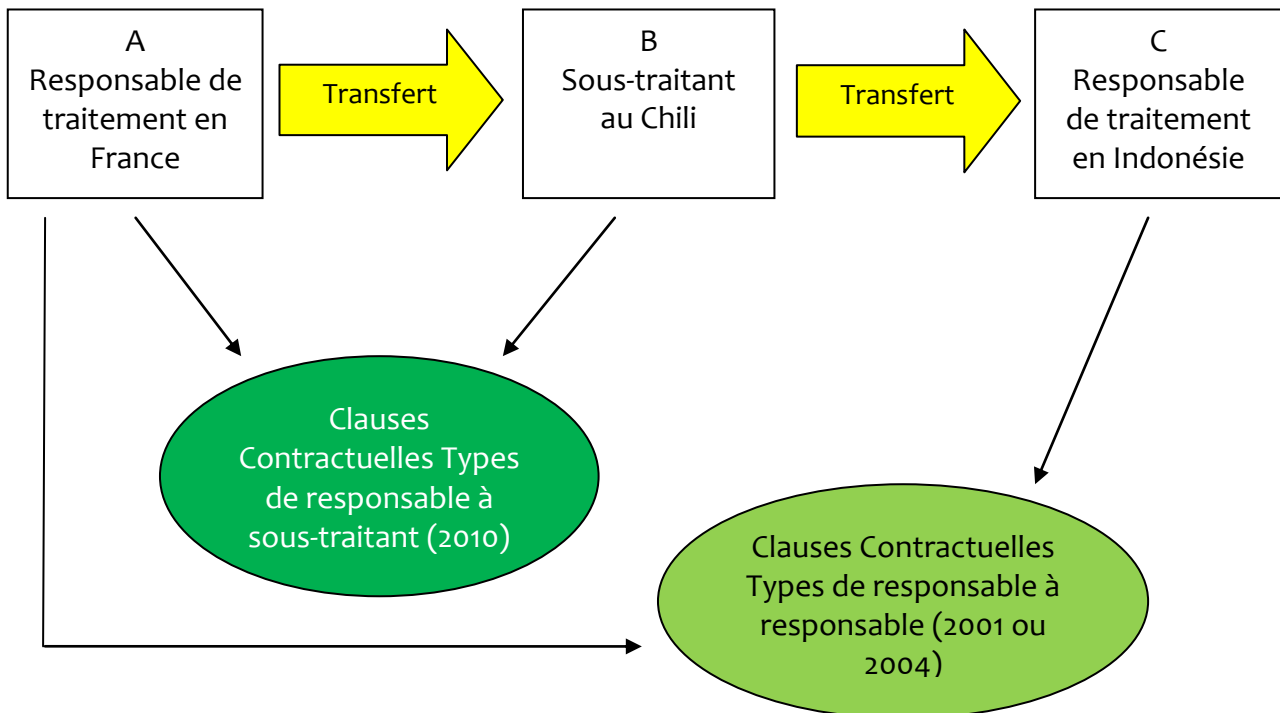
A et B n'ont pas besoin de signer de Clauses Contractuelles Types de responsable de traitement à responsable de traitement puisque les données restent au sein de l'Union européenne. En revanche, il appartient à B d'encadrer le transfert entre B et C puisque ce dernier est situé en-dehors de l'Union européenne.



La logique est la même lorsque B est situé dans un pays reconnu par une décision de la Commission européenne comme offrant un niveau de protection suffisant et le transfert devra être encadré conformément à la loi locale de B.

H8. Transferts de données personnelles par un responsable de traitement UE vers un sous-traitant hors UE, qui transfère à son tour les données vers un responsable de traitement hors UE

A et B signent des Clauses Contractuelles Types de responsable de traitement à sous-traitant. B étant sous-traitant, il ne peut pas conclure des Clauses Contractuelles Types avec C qui est responsable de traitement. Afin d'encadrer le transfert de données de B vers C, A doit signer avec C des Clauses Contractuelles Types de responsable de traitement à responsable de traitement.



Le Safe Harbor

- Q1.** Qu'est-ce que le Safe Harbor ?
- Q2.** Où puis-je trouver la liste des entreprises ayant adhéré aux principes du Safe Harbor ?
- Q3.** Quelles formalités dois-je accomplir lorsque je transfère des données personnelles à une entreprise ayant adhéré aux principes du Safe Harbor ?
- Q4.** Si le destinataire de données a adhéré aux principes du Safe Harbor mais ne les respecte pas, que puis-je faire ?

Q1. Qu'est-ce que le Safe Harbor ?

Il s'agit d'un ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne.

Ces principes, négociés entre les autorités américaines et la Commission européenne en 2001, sont essentiellement basés sur ceux de la Directive 95/46 du 24 octobre 1995 :

- information des personnes,
- possibilité accordée à la personne concernée de s'opposer à un transfert ou à une utilisation des données pour des finalités différentes,
- consentement explicite pour les données sensibles,
- droit d'accès et de rectification,
- sécurité des données,

Le Safe Harbor **permet donc d'assurer un niveau de protection suffisant** pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux Etats-Unis.

Q2. Où puis-je trouver la liste des entreprises ayant adhéré au Safe Harbor ?

Vous pouvez trouver la liste des entreprises ayant adhéré aux principes du Safe Harbor sur le site internet du Département du Commerce américain¹⁷. Vous devez vérifier sur ce site que l'adhésion de l'entreprise est bien à jour (« current ») et qu'elle couvre bien le transfert envisagé (ex : catégorie de données traitées).

Q3. Quelles formalités dois-je accomplir lorsque je transfère des données personnelles à une entreprise ayant adhéré aux principes du Safe Harbor ?

L'adhésion au Safe Harbor permettant de garantir un niveau de protection suffisant au transfert de données vers une entreprise située aux Etats-Unis, ce transfert n'est pas soumis à une décision d'autorisation de la CNIL.

La formalité que vous devez accomplir est celle qui est applicable au traitement principal (déclaration normale, demande d'autorisation ou demande d'avis). Le transfert de données vers les Etats-Unis et la garantie qui encadre le transfert, ici le Safe Harbor, devront être mentionnés dans le formulaire.

Les formalités auprès de la CNIL s'effectuent en ligne sur le site internet www.cnil.fr, rubrique « Déclarer un fichier ».

¹⁷ <https://safeharbor.export.gov/list.aspx>

Q4. Si le destinataire de données a adhéré aux principes du Safe Harbor mais ne les respecte pas, que puis-je faire ?

Si vous constatez que le destinataire ayant adhéré aux principes du Safe Harbor ne les respecte pas, outre les mécanismes prévus au contrat qui vous lie, vous pouvez adresser un courrier à la CNIL en France et à la *Federal Trade Commission* aux Etats-Unis (FTC, <http://www.ftc.gov>) indiquant que vous avez relevé des violations aux principes du Safe Harbor. L'entreprise sera alors mise en demeure de se conformer aux principes auxquels elle a adhéré et potentiellement sanctionnée.

Les exceptions

- Q1.** Existe-t-il des exceptions au principe d'interdiction de transferts ?
- Q2.** Comment ces exceptions sont-elles interprétées ?

Q1. Existe-t-il des exceptions au principe d'interdiction de transferts ?

Outre les BCR, les Clauses Contractuelles Types et le Safe Harbor, il existe des exceptions au principe d'interdiction de transferts qui font l'objet **de limitations et d'une interprétation stricte**. Ces exceptions sont prévues à l'article 69 de la loi Informatique et Libertés du 6 janvier 1978 modifiée :

- Soit la personne a **consenti expressément** au transfert de ses données personnelles;
- Soit **le transfert s'avère nécessaire à l'une des conditions suivantes** :
 - la **sauvegarde de la vie** de cette personne;
 - la **sauvegarde de l'intérêt public**;
 - le respect d'obligations permettant d'assurer la constatation, l'exercice ou la **défense d'un droit en justice**;
 - la consultation, dans des conditions régulières, d'un **registre public** qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime;
 - **l'exécution d'un contrat** entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci;
 - la conclusion ou **l'exécution d'un contrat** conclu ou à conclure, **dans l'intérêt de la personne concernée**, entre le responsable du traitement et un tiers.

Attention, **ces exceptions**, prévues à l'article 69 de la loi Informatique et Libertés du 6 janvier 1978 ne s'appliquent pas à la relation de responsable de traitement à sous-traitant.

Q2. Comment ces exceptions sont-elles interprétées ?

L'application des dispositions **doit être limitée à des cas ponctuels et exceptionnels**.

La CNIL et le G29 (groupe des CNIL européennes) recommandent en particulier que des transferts **répétitifs, massifs ou structurels** de données personnelles, dont l'importance ou la régularité justifient qu'ils soient encadrés, **fassent l'objet d'un encadrement juridique spécifique (BCR, Clauses Contractuelles Types ou Safe Harbor) et ne reposent pas sur ces exceptions de l'article 69¹⁸**.

Exemple 1 : L'exécution d'un contrat

Madame Lucas souhaite partir en vacances. Pour organiser son voyage en Inde, elle fait appel à une agence de voyage. Afin d'exécuter le contrat conclu avec Mme Lucas, l'agence de voyage devra réserver les hôtels dans lesquels elle séjournera. Pour cela, les données personnelles de Mme Lucas doivent être envoyées depuis l'agence de voyage située en France vers les hôtels situés en Inde, donc hors de l'Union européenne.

¹⁸ Voir également le document de travail du G29 relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, WP114, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_fr.pdf, qui recommande que les exceptions ne couvrent pas des transferts qui puissent être qualifiés de répétitifs, massifs ou structurels.

Cependant ce transfert de données ne doit pas faire l'objet d'un encadrement spécifique puisqu'il est effectué de façon ponctuelle aux fins d'exécuter le contrat que Mme Lucas a signé avec l'agence de voyage.

Exemple 2 : L'intérêt des personnes concernées

Monsieur Daniel, qui est actuellement en séjour au Mali, vient de se fracturer la jambe. Afin d'organiser son rapatriement, sa compagnie d'assurance doit transmettre certaines informations personnelles à la compagnie malienne en charge de son transport aérien. Le transfert de données ainsi effectué n'est soumis à aucun encadrement spécifique puisqu'il est effectué à titre exceptionnel dans l'intérêt de la personne concernée.