TRANSFERTS DE DONNEES A CARACTERE PERSONNEL VERS DES PAYS TIERS A L'UNION EUROPENNE

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 personnelles hors du territoire Français sont interdits à moins que le pays ou le destinataire n'assure un niveau de protection adéquat.

Plusieurs outils ont été développés pour permettre aux acteurs d'apporter un niveau de protection adéquat : les règles internes d'entreprises (ou BCR), les Clauses Contractuelles Types, le Safe Harbor. La loi prévoit également des exceptions permettant de transférer les données sans qu'un niveau de protection adéquat ne soit apporté aux données transférées dans des hypothèses exceptionnelles.

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

Commission Nationale de l'Informatique et des Libertés

LES TRANSFERTS

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

Q2 – Quelles dispositions régissent les transferts de données à caractère personnel ?

Q3 – Exemples de transferts

Q4 – Comment encadrer les transferts de données ?

Q5 – Y a-t-il d'autres règles à respecter dans le cadre d'un transfert de données ?

Q6 – Quelles sont les formalités à respecter lorsque l'on effectue un transfert hors de l'UE ?/ Comment obtenir une autorisation de transfert ?

Q7 – Les transferts que j'effectue sont issus de traitements relevant du champ d'application d'une norme simplifiée[1]. Suis-je dispensé de la demande d'autorisation ?

Q8 – Puis-je transférer des données pour une finalité différente que celle pour laquelle les données ont été initialement collectées ?

Q9 – Dois-je informer les personnes concernées lorsque je transfère leurs données vers un pays tiers ?

Q10 – Quelles sanctions encourt le responsable de traitement en cas de non respect des règles en matière de transferts ?

Q11 – Qu'entend-on par « destinataire de données » ?

Q12 – Qu'entend-on par « responsable de traitement » ?

Q13 – Qu'entend-on par « sous-traitant » ?

Q14 – Pourquoi est-il important de distinguer le responsable de traitement du sous-traitant dans le cadre de transferts de données à caractère personnel ?

Q15 – Quels critères 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.

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

On parle de transfert de données personnelles lorsque les données personnelles sont transférées depuis le territoire européen vers un ou des pays situés hors de l'Union européenne. Le transfert peut s'effectuer, par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre (ex. d'un disque dur d'ordinateur à un serveur).

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

➢ **Loi « Informatique et Libertés » du 6 janvier 1978 modifiée[2] et le décret du 20 octobre 2005 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 loi[3] : les transferts en dehors de l'Union européenne sont **interdits**.

Les exceptions sont prévues par l'article 69 de la loi [4] :

Les transferts en dehors de l'Union européenne sont autorisés si le pays ou l'entreprise destinataire assure un niveau de protection adéquat aux données transférées. Cette protection adéquate peut être apportée de plusieurs manières :

- ✓ **Légalement**, si le pays destinataire des données personnelles a une législation reconnue par la Commission européenne comme offrant une **protection adéquate**. C'est le cas du Canada, de l' Isle de Man, de la Suisse, de l'Argentine, de Guernesey et de Jersey, ou
- ✓ **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, ou
- ✓ **Lorsque l'entité importatrice est basée aux Etats-Unis et qu'elle adhère au principe de Safe Harbor.**
- ✓ **L'article 69 permet également d'opérer des transferts dans des situations exceptionnelles.**

Q3 – Exemples de transferts

Exemple 1 - Une entreprise souhaite sous-traiter la gestion des relances téléphoniques de ses clients à une société située dans un 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.

[2] 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,
[3] Transposant l'article 25 de la directive européenne 95/46/CE.
[4] Transposant l'article 26 de la directive européenne 95/46/CE.

Q4 – Comment encadrer les transferts de données ?

Pour que les transferts hors de l'Union européenne soient autorisés, il faut que le pays ou l'entreprise destinataire assure un niveau de protection adéquat aux données transférées. (article 69)

C'est le cas lorsque :

✓ le transfert a lieu vers **un pays reconnu** par la Commission européenne comme "**adéquat**". C'est le cas du **Canada, de la Suisse, de l'Argentine, des territoires de Guernesey, de Jersey et de l'Isle de Man**. Cette liste évolue et peut être consultée sur le site de la CNIL (www.cnil.fr).

ou

✓ des Clauses Contractuelles Types de la Commission Européenne sont signées entre deux entreprises (voir le PDF dédié aux Clauses Contractuelles Types)

ou

✓ des Règles internes d'entreprises (BCR) sont adoptées au sein d'un groupe (voir le PDF dédié aux BCR)

ou

✓ l'entreprise destinataire est située aux Etats-Unis et adhère au Safe Harbor (voir la partie du site dédiée au Safe Harbor),

ou

✓ des exceptions de l'article 69 de la loi Informatique et Libertés peuvent être invoquées (voir le PDF dédié aux exceptions).

Q5 – Existe-t-il d'autres règles à respecter dans le cadre d'un transfert de données ?

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 :

✓ Tout transfert de données vers l'étranger 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 doivent être transférées doivent être **informées** de l'existence de ce transfert ; (Article 91 du décret 2007)

✓ La **durée de conservation** des données transférées ne doit pas être excessive;

✓ Les personnes doivent se voir garantir **un droit d'accès et un droit de rectification** en ce qui concerne les données transférées, ainsi qu'un droit d'opposition aux transferts;

✓ Des **mesures techniques de sécurité** doivent être mises en place afin de protéger les données contre tout accès ou toute destruction, altération ou diffusion non autorisé desdites données.

Q6- Quelles sont les formalités à respecter lorsque l'on effectue un transfert hors de l'UE ?

Si votre entreprise n'a pas désigné de Correspondant Informatique et Libertés (CIL)

Cadre du transfert	Déclaration normale	Demande d'autorisation
Safe Harbor	√	
Pays présentant une protection adéquate	√	
Clauses Contractuelles Types		√
Exceptions au principe d'interdiction de transfert	√	
BCR		√

Si votre entreprise a désigné un Correspondant Informatique et Libertés (CIL)

Cadre du transfert	Inscription au registre	Demande d'autorisation
Safe Harbor	√	
Pays présentant une protection adéquate	√	
Clauses Contractuelles Types		√
Exceptions au principe d'interdiction de transfert	√	
BCR		√

Q7 - 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 la demande d'autorisation pour les transferts ?

Pas nécessairement. Les normes simplifiées et les autorisations uniques étant d'interprétation stricte la dispense d'autorisation de transfert ne sera possible que si la norme simplifiée[5] ou l'autorisation unique prévoit expressément la possibilité d'un transfert, dans la limite du champ prévu par la norme 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 et portant abrogation des normes simplifiées 11, 17 et 25.*
- *autorisation unique 004* portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle

(Reportez-vous aux normes simplifiées qui vous concernent http://www.cnil.fr/en-savoir-plus/deliberations/normes-simplifiees/)

Q8 – Puis-je transférer des données personnelles pour une finalité différente que celle pour laquelle les données 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 pas être réutilisées pour des finalités incompatibles avec les finalités initiales, à moins que la législation ne l'exige. 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 expressément autorisé par la CNIL.

Q9 – 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, les responsables de traitement doivent 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, et du niveau de protection offert par le pays destinataires.

Q10 - Quelles sanctions encourt le responsable de traitement en cas de non respect des règles en matière de transferts ?

[5] 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.

Les sanctions pénales en cas de non respect des règles en matière de transferts peuvent aller de **300 000 euros d'amende à 5 ans d'emprisonnement** (Art. 226-16 et 226-16 A du Code pénal et l'Art. 226-22-1 du même Code).

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

- prononcer un avertissement à l'égard du responsable de traitement qui ne respecterait pas les obligations découlant de la présente loi,

- mettre en demeure de faire cesser le manquement constaté dans un délai qu'elle fixe.

Après une mise en demeure, la Commission peut également 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)

- une injonction de cesser le traitement ou un retrait de l'autorisation accordée par la CNIL.

Q11 - Qu'entend-on par « destinataire de données » ?

Le destinataire de données est celui vers lequel les données à caractère personnel sont exportées. Il peut s'agir d'un responsable de traitement ou d'un sous-traitant.

Q12 - Qu'entend-on par « 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 ». 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.

Q13 - Qu'entend-on par « sous-traitant » ?

Le sous-traitant est la personne physique ou morale traitant des données à caractère personnel agissant **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 d'un responsable de traitement à un sous-traitant, que ce soit vers un pays membre de l'Union européenne ou vers un Etat hors de l'Union européenne, ne peut être réalisé que :

- ✓ sur instruction du responsable de traitement, et

- ✓ si un contrat garantissant notamment les mesures de sécurité et de confidentialité qui doivent être mises en place par le sous-traitant est signé (Article 35 de la loi).

Q14 - Pourquoi est-il important de distinguer le responsable de traitement du sous-traitant dans le cadre de transferts de données à caractère personnel ?

Dans le cadre de clauses contractuelles, il est important de distinguer le responsable de traitement du sous-traitant car leurs obligations sont différentes, c'est pourquoi il existe différents modèles de contrats selon la qualité du destinataire (voir les informations relatives aux Clauses Contractuelles Types).

Dans le cadre des BCR, il est important de distinguer le responsable de traitement du sous-traitant, puisque les transferts de données vers des entités externes au groupe devront bénéficier d'un encadrement permettant d'atteindre un niveau de protection adéquat 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.

Q15 - 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 son exécution sont très généraux en termes d'instruction et laissent expressément une grande autonomie au prestataire.
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.	La société audite son prestataire et lui demande des comptes régulièrement.	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.
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.	Le prestataire utilise l'infrastructure technique du client pour réaliser sa prestation.	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 spécifiques.

LES BCR - BINDING CORPORATE RULES

OU

REGLES INTERNES D'ENTREPRISE

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

Q2 - A quoi servent les BCR ?

Q3 - Quelles sont les entreprises concernées ?

Q4 - Quels avantages les BCR présentent-elles?

Q5 - Existe-t-il des documents auxquels je peux me référer pour rédiger les BCR ?

Q6 - Quelle est la première étape lorsque mon entreprise souhaite adopter des BCR?

Q7 - De quels droits les personnes concernées peuvent-elles se prévaloir au titre des BCR ?

Q8 - Quelles procédures doivent être développées au sein de l'entreprise afin de mettre en œuvre les BCR ?

Q9 - Quelles sont les grandes étapes lorsque l'on a recours aux BCR ?

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

Les BCR désignent un **code de conduite** qui définit la politique interne 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** et par 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 filiales** 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 avantages les BCR présentent-ils?

Les BCRs 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 – 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 revus par les autorités de protection. 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 de la CNIL (ww.cnil.fr).

Q6 – Quelle est la première étape lorsqu'une entreprise souhaite adopter des BCR?

Lorsque votre entreprise souhaite adopter des BCR, il convient tout d'abord de désigner une autorité de coordination qui sera en charge de la procédure de coopération avec les autres autorités auprès desquelles vous déposerez des demandes d'autorisation de transfert sur la base des BCR. Cette autorité de coordination sera votre unique point de contact puisque c'est à cette autorité que l'entreprise présentera son projet de BCR.

Le service des affaires européennes et internationales de la CNIL vous accompagne dans la finalisation du document afin d'avoir un instrument juridique satisfaisant par rapport aux exigences posées par les documents adoptés par le G29.

Q7 - De quels droits les personnes concernées peuvent-elles se prévaloir au titre des BCR ?

Les personnes concernées pourront se prévaloir des droits suivants au titre des BCR :

- ✓ Limitation des finalités
- ✓ Qualité des données et proportionnalité
- ✓ Critères de légitimation du processus
- ✓ Transparence et accessibilité des BCR
- ✓ 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 aux transferts ultérieurs en dehors du groupe
- ✓ Droit de se prévaloir du fait qu'une entreprise n'a pas fait part au responsable à la protection des données d'une législation applicable risquant d'empêcher l'entreprise de respecter les BCR
- ✓ Droit de porter plainte par l'intermédiaire du mécanisme interne de réclamation des entreprises
- ✓ Devoir de coopération avec l'autorité de protection des données
- ✓ Possibilité d'engager la responsabilité du responsable de traitement

Q8 – Quelles procédures doivent être développées au sein de l'entreprise afin de mettre en œuvre les BCR ?

Aux termes des BCR, l'entreprise doit notamment s'engager à mettre en œuvre :

- ✓ Un régime de responsabilité pesant sur l'entité responsable ou sur la filiale européenne responsable par délégation de la protection des données (ou autres),

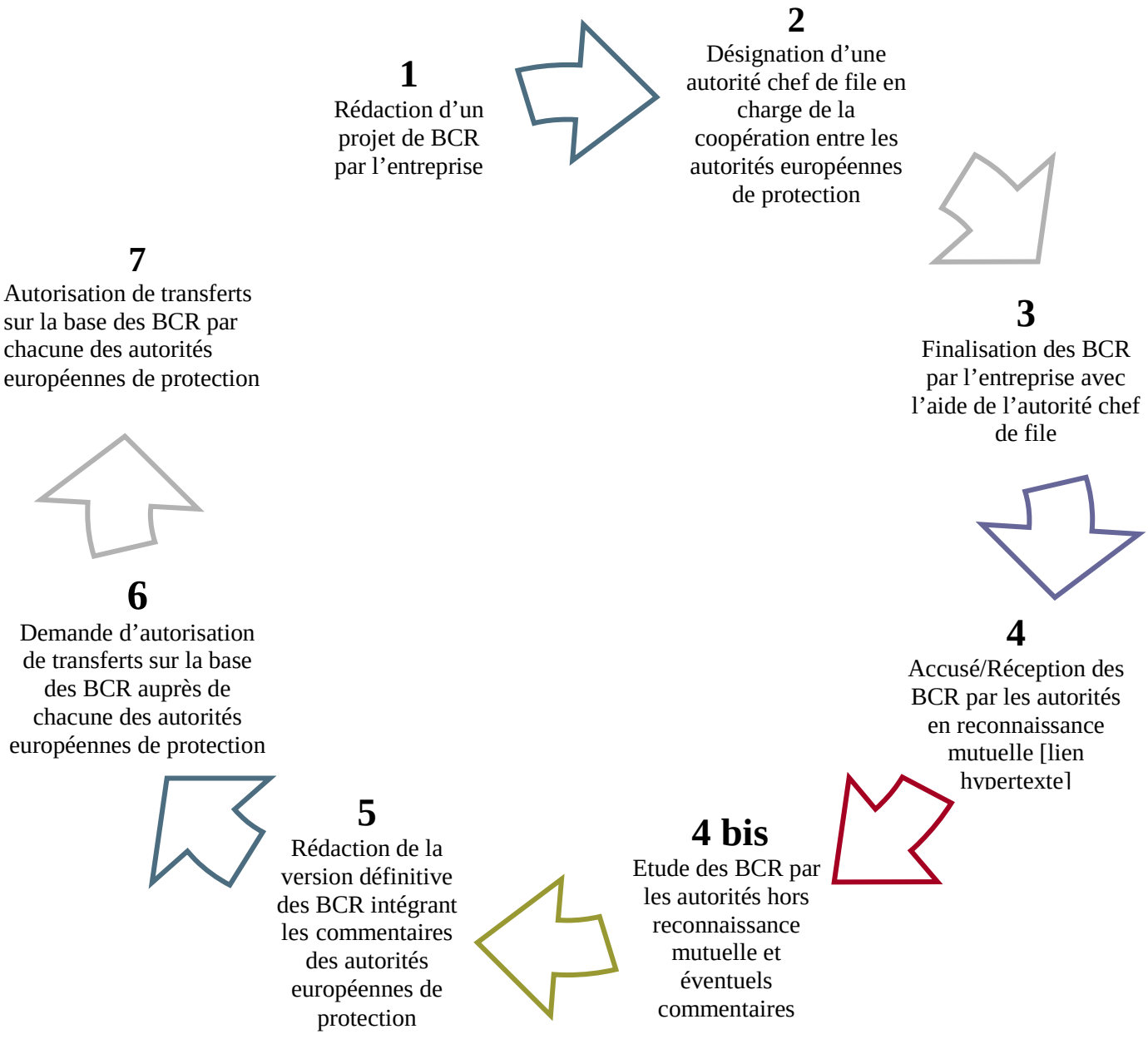
- ✓ Une procédure de formation du personnel quant aux règles posées par les BCR

- ✓ Une procédure d'audit,

- ✓ Une procédure de gestion de plainte interne,

- ✓ 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.

Q9 – Quelles sont les grandes étapes lorsque l'on a recours aux BCR ?



LES CLAUSES CONTRACTUELLES TYPES DE LA COMMISSION EUROPEENNE

Q1 − Qu'est-ce que les Clauses Contractuelles Types ?

Q2 − Faut-il reprendre les Clauses Contractuelles Types in extenso ?

Q3 − Quelles sont les grandes étapes lorsque l'on souhaite avoir recours aux Clauses Contractuelles Types ?

Q4 − Où trouver les Clauses Contractuelles Types ?

Q5 − Quelles démarches effectuer lorsque j'ai recours à des Clauses Contractuelles Types ?

Q6 - Quel est le régime de responsabilité applicable dans le cadre des Clauses Contractuelles Types permettant d'encadrer les transferts entre responsables de traitement ?

Q7 - 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 ?

Q8 - A partir de quand le nouveau jeu de Clauses Contractuelles Types sera-t-il applicable ?

Q9 - Mes transferts existants sont encadrés par les Clauses Contractuelles Types préexistantes. Dois-je signer les nouvelles clauses afin de remplacer les anciennes clauses ?

Q10 - Pourquoi de nouvelles Clauses Contractuelles Types ?

Q11 - Quelles nouvelles obligations ces clauses mettent-elles à la charge du sous-traitant et du sous-traitant ultérieur ?

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

Il s'agit de modèles de clauses contractuelles adoptées par la Commission européenne et permettant d'encadrer les transferts de données personnelles effectués par des responsables de traitement vers des destinataires 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 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 des transferts.

✓ **Clauses contractuelles encadrant les transferts de données personnelles par un responsable de traitement vers 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 2001/497/CE du 15 juin 2001 et le second de la décision de la Commission du 24 décembre 2004 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 et la coopération avec les autorités de protection des données.

➔ L'entreprise doit choisir lequel de ces deux modèles de clauses elle souhaite signer.

✓ **Clauses contractuelles encadrant les transferts de données personnelles par un responsable de traitement vers 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. Ce jeu de clauses remplace, depuis le 15 mai 2010, les Clauses contractuelles antérieures de 2002.

Q3 - Faut-il reprendre les Clauses Contractuelles Types *in extenso* ?

Aucune disposition légale n'oblige les entreprises 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 et de la loi. 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 préjudices aux libertés et droits fondamentaux des personnes dont les données sont traitées.

Q4 - Quelles sont les grandes étapes lorsque l'on souhaite avoir recours aux Clauses Contractuelles Types ?

ETAPE No 1 – Identifier les parties, qualifier le type de transferts de données personnelles effectuées et identifier les Clauses Contractuelles Types dont on a besoin (de responsable de traitement à responsable de traitement ou de responsable de traitement à sous-traitant)

ETAPE No 2 – Compléter les Clauses Contractuelles Types (notamment les Annexes sur la description des transferts)

ETAPE No 3 – Effectuer les démarches nécessaires auprès de la CNIL

Q5 - Quelles démarches 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 demande d'autorisation de transfert devra notamment préciser :

1- qu'un transfert de données a lieu vers un pays non-membre de l'Union européenne et,

2- que le transfert soumis à autorisation est encadré par les Clauses Contractuelles Types de la Commission européenne.

Q6 - Quel est le régime de responsabilité applicable dans le cadre des clauses contractuelles 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 aux termes duquel les personnes concernées ayant subi un dommage du fait de la violation des droits dont elles peuvent se prévaloir pourront 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.

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. Chaque partie est responsable envers l'autre partie des dommages qu'elle cause par suite d'un manquement aux présentes clauses.

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.

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.

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.

Q7 - Quel est le régime de responsabilité applicable dans le cadre des clauses contractuelles permettant d'encadrer les transferts entre un responsable de traitement et un sous-traitant ?

L'exportateur de données étant seul responsable de traitement, c'est lui seul qui endossera la responsabilité 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 violation par ce dernier.

Q8 - A partir de quand le nouveau jeu de Clauses Contractuelles Types sera-t-il applicable ?

Le nouveau jeu de clauses adopté le 3 février 2010 par la Commission européenne entrera en vigueur le 15 mai 2010 et remplacera les clauses résultant de la décision de la Commission de décembre 2001.

Avant cette date, les transferts de données vers des sous-traitants situés dans des pays tiers doivent être encadrés par les Clauses Contractuelles Types de 2001.

Q9 - Mes transferts existants sont encadrés par les Clauses Contractuelles Types préexistantes. Dois-je signer les nouvelles clauses afin de remplacer les anciennes clauses ?

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 activités de traitement de données ayant fait l'objet d'une autorisation de transfert sur la base des Clauses Contractuelles Types de 2001.

Q10 - Pourquoi de nouvelles Clauses Contractuelles Types ?

Ces nouvelles Clauses Contractuelles Types permettent de mieux prendre en compte les chaînes de sous-traitance.

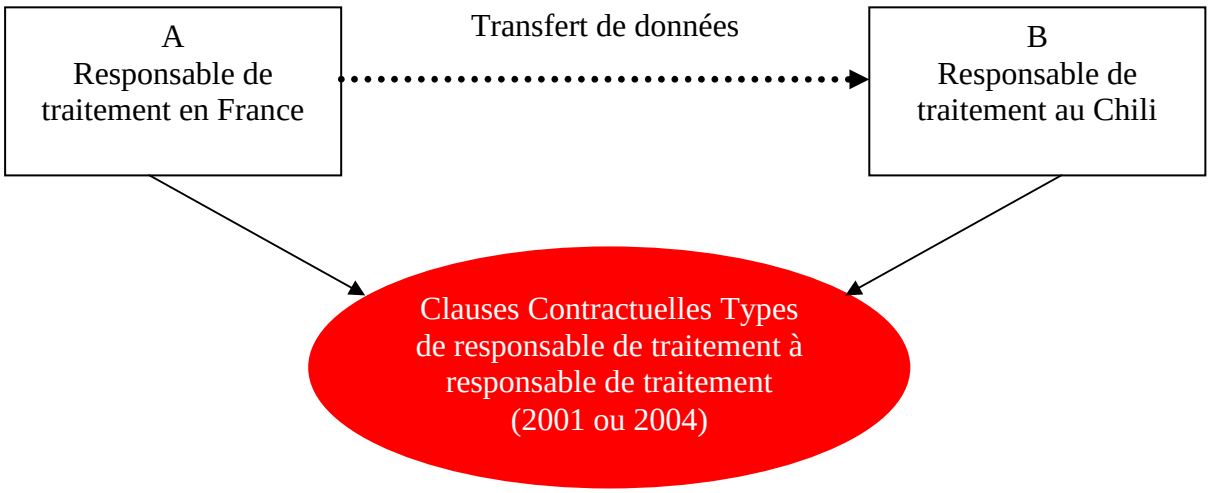
Q11 – Quelles nouvelles obligations ces clauses mettent-elles à la charge du sous-traitant et du sous-traitant ultérieur ?

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.

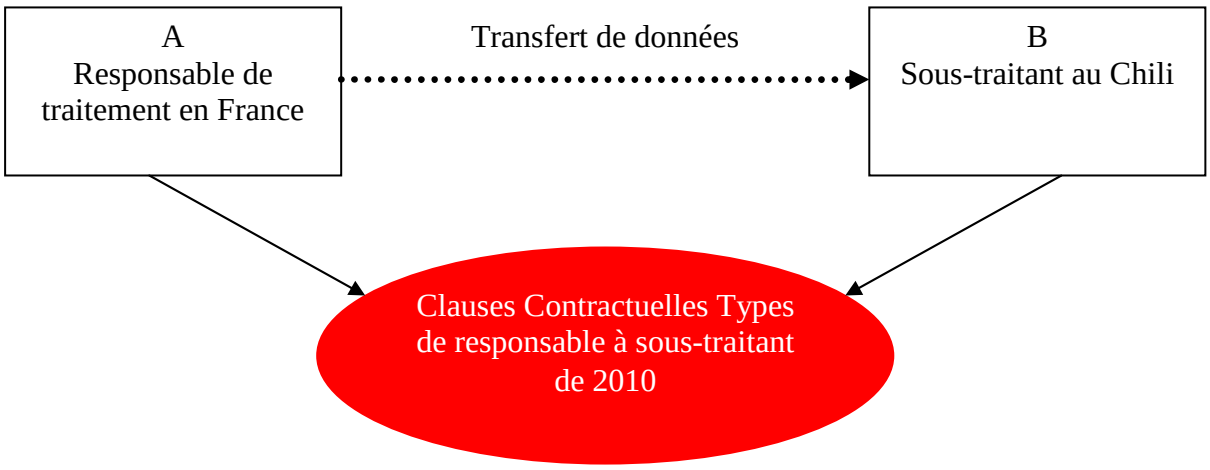
EN PRATIQUE :

HYPOTHESES DE TRANSFERTS

Hypothèse 1 – Transferts de données personnelles par un responsable de traitement vers un autre responsable de traitement situé dans un pays tiers à l'Union européenne.



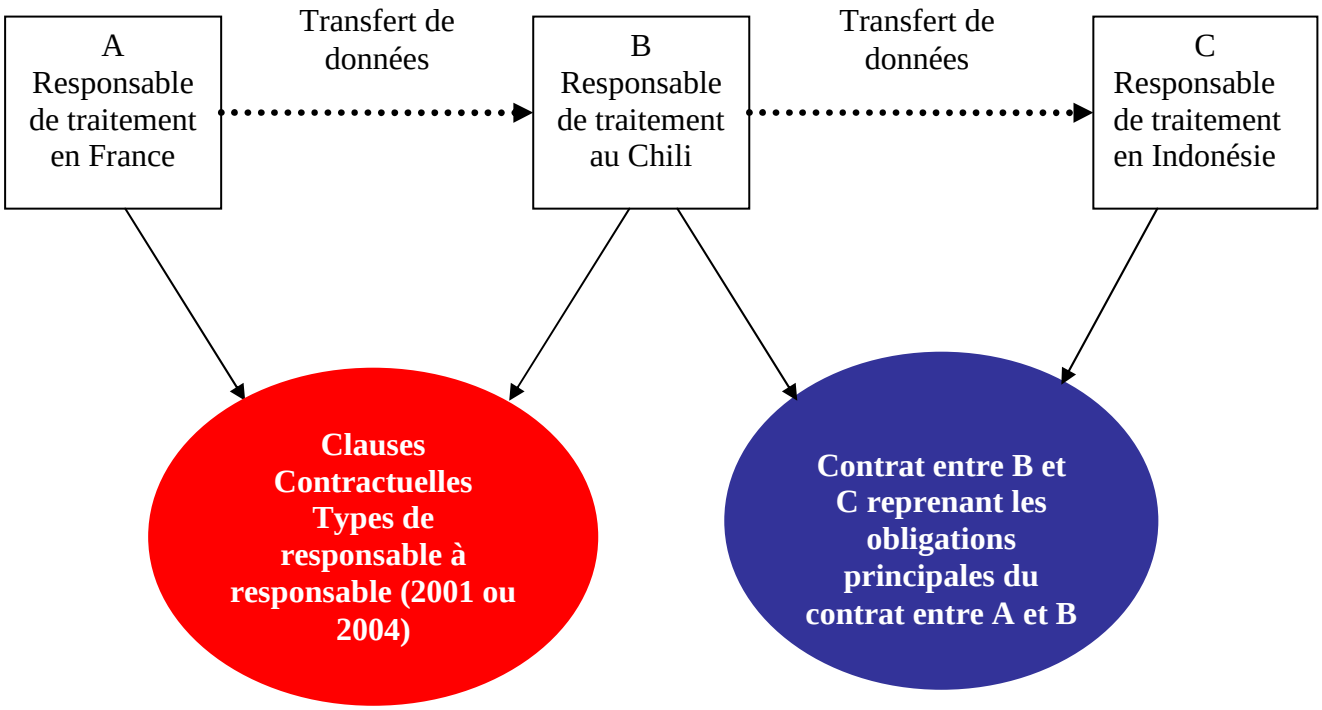
Hypothèse 2 – Transferts de données personnelles par un responsable de traitement vers un sous-traitant situé dans un pays tiers à l'Union européenne.



Hypothèse 3 – Transferts de données personnelles par un responsable de traitement vers un autre responsable de traitement situé dans un pays tiers à l'Union européenne, qui transfère lui-même les données vers un autre responsable de traitement situé dans un autre pays tiers à l'Union européenne.

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

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

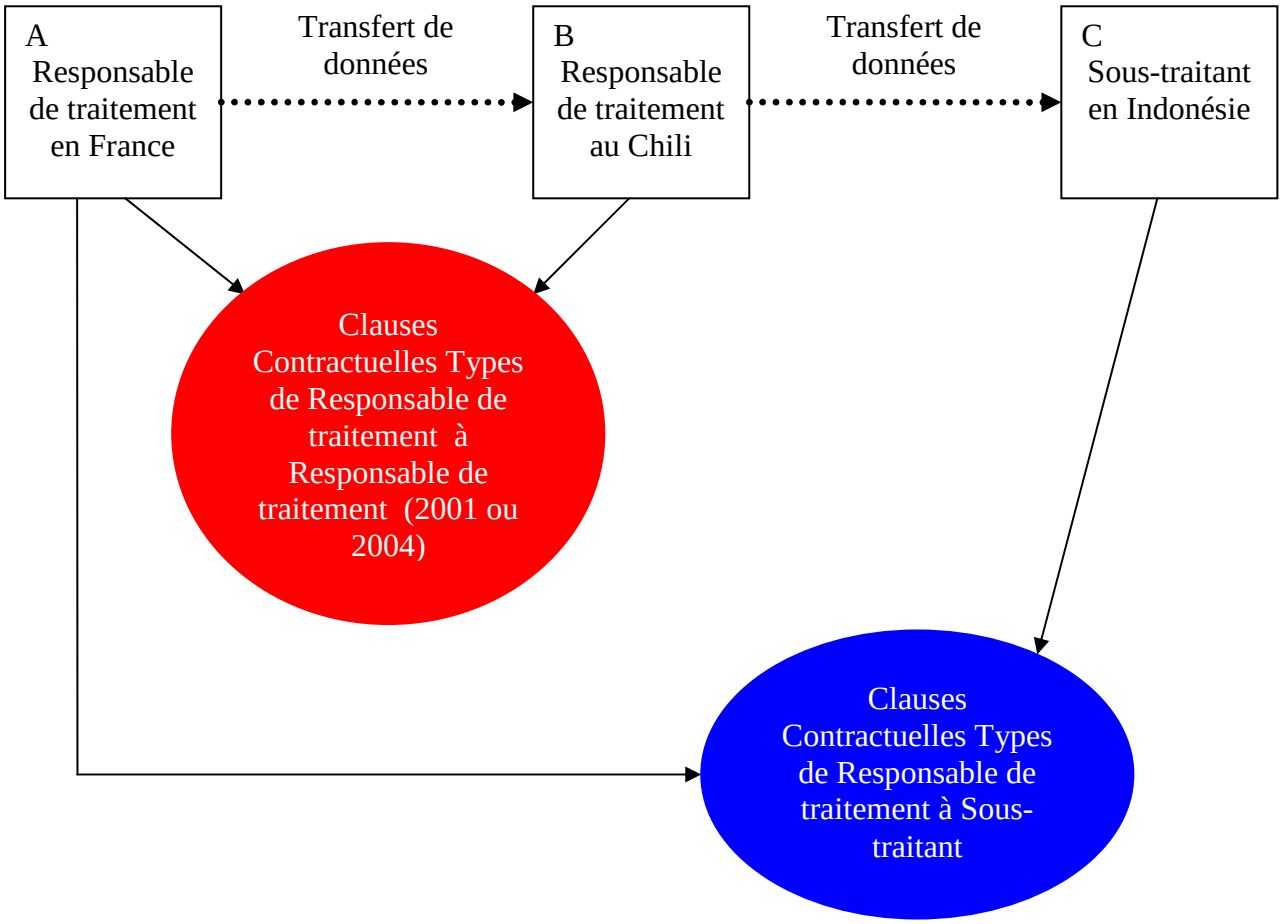


Hypothèse 4 – Transferts de données personnelles par un responsable de traitement vers un autre responsable de traitement situé dans un pays tiers à l'Union européenne, qui transfère lui-même les données vers un sous-traitant situé dans un autre pays tiers à l'Union européenne.

Option 1

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

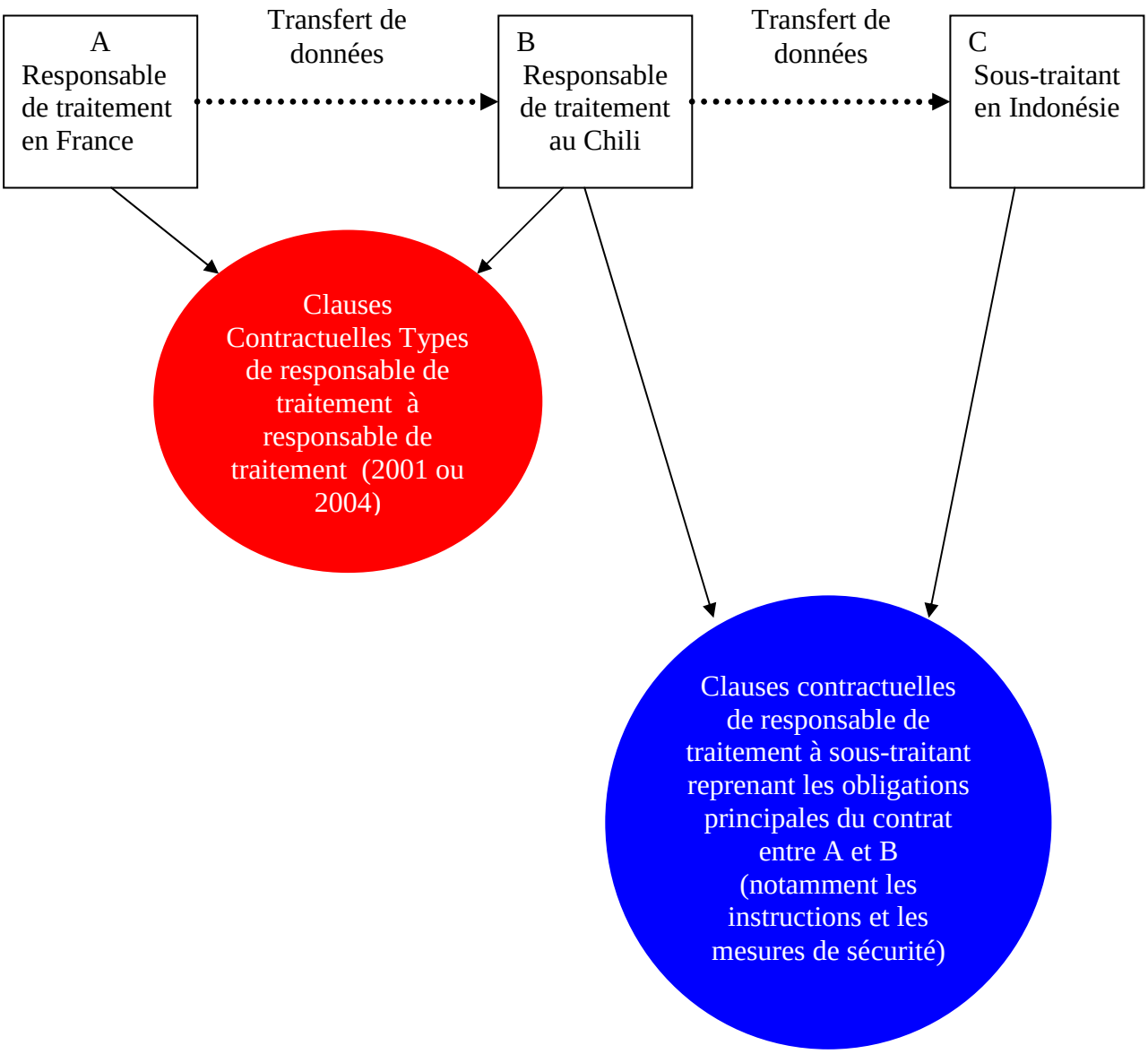
A et C signent des Clauses Contractuelles Types de responsable de traitement à sous-traitant.



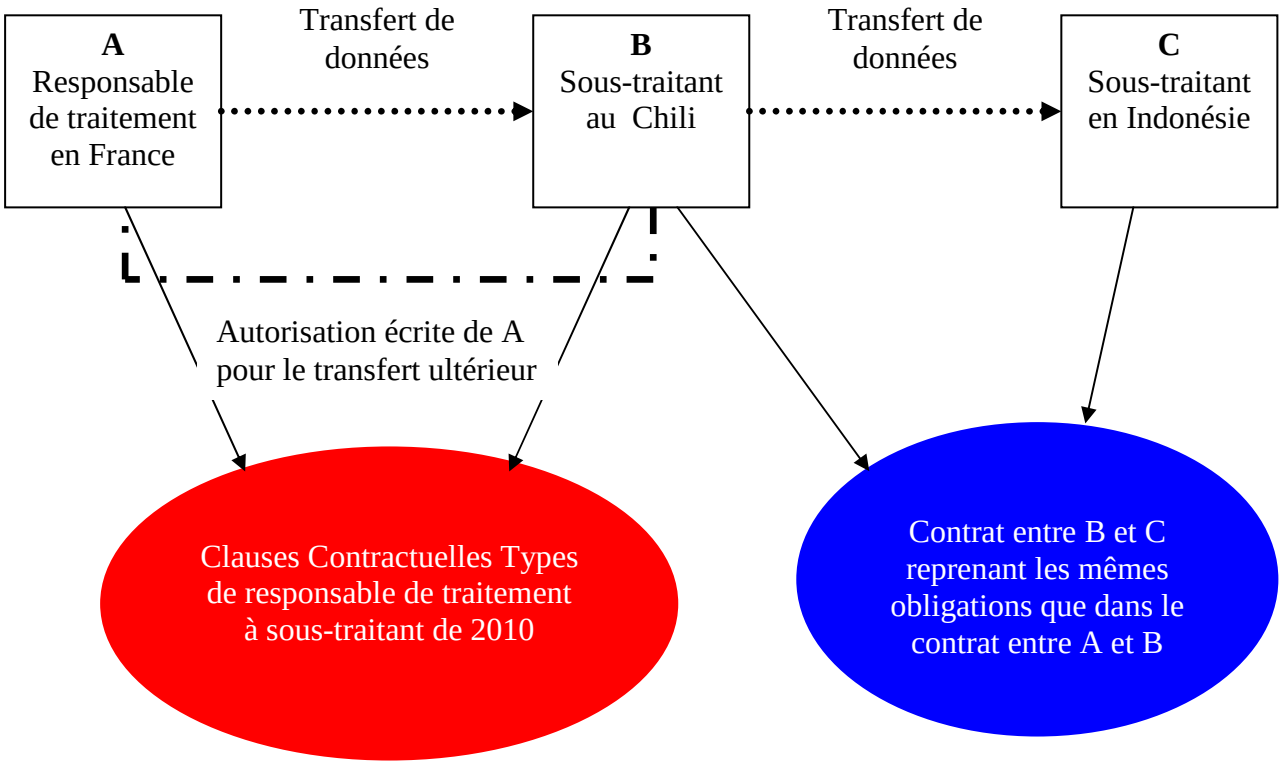
Option 2

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

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

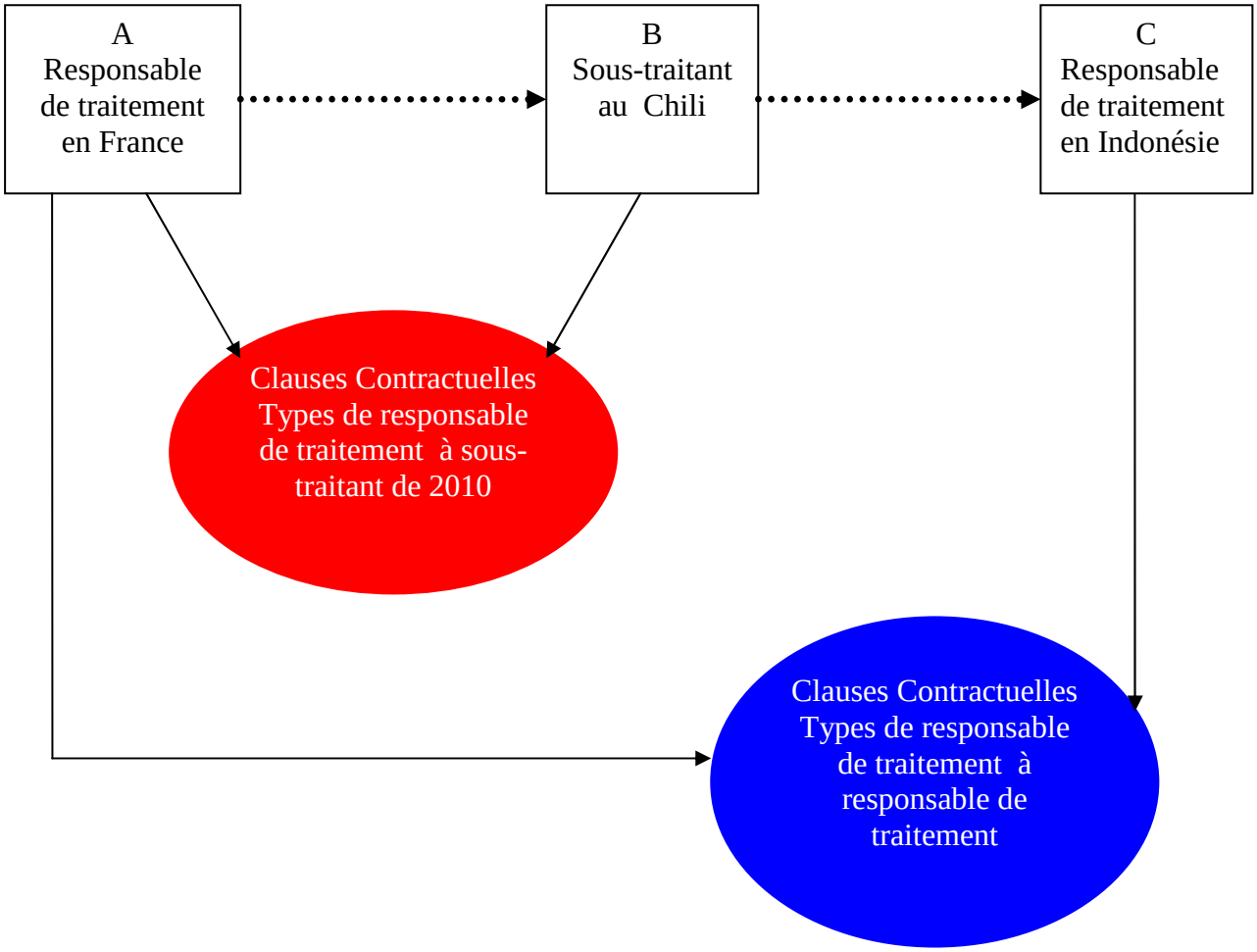


Hypothèse 5 – Transferts de données personnelles par un responsable de traitement vers un sous-traitant situé dans un pays tiers à l'Union européenne, qui transfère lui-même les données vers un autre sous-traitant situé dans un autre pays tiers à l'Union européenne.



Hypothèse 6 – Transferts de données personnelles par un responsable de traitement vers un sous-traitant situé dans un pays tiers à l'Union européenne, qui transfère lui-même les données vers responsable de traitement situé dans un autre pays tiers à l'Union européenne.

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 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 au Safe Harbor ?

Q3 - Le destinataire de données adhère au Safe Harbor, quelles formalités accomplir ?

Q4 - Le destinataire de données a adhéré aux principes du Safe Harbor mais ne les respecte pas, que faire ?

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

Il s'agit d'un ensemble de principes de protection des données personnelles, publiés par le Département du Commerce américain, auxquels des entreprises établies aux Etats-Unis adhèrent afin de pouvoir recevoir des données 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 à des tiers ou à une utilisation des données pour des finalités différentes,
- ✓ consentement explicite pour les données sensibles,
- ✓ droit d'accès, de rectification,
- ✓ sécurité,

Le Safe Harbor **permet donc d'assurer une protection adéquate** 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 ?

La liste des entreprises ayant adhéré aux principes du Safe Harbor se trouve sur le site du Département du Commerce américain [http://www.export.gov/safeHarbor/]. Vous devez vérifier sur ce site, que l'adhésion de l'entreprise est bien à jour (« current ») et que l'adhésion couvre bien le transfert envisagé (ex : catégorie de données traitées)

Q3 – Si le destinataire de données adhère au Safe Harbor, quelles formalités sont à accomplir ?

Vous n'êtes pas soumis au régime d'autorisation de la CNIL, vous devez néanmoins effectuer une déclaration normale pour votre traitement de données et indiquer que vous effectuez un transfert vers un pays tiers à l'Union européenne.

Q4 – Le destinataire de données a adhéré aux principes du Safe Harbor mais ne les respecte pas, que 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 et à la Federal Trade Commission indiquant que vous avez relevé des violations des principes. L'entreprise sera alors mise en demeure de se conformer aux principes auxquels elle a adhérés.

LES EXCEPTIONS

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

Q2 - Comment ces exceptions sont-elles interprétées ?

Q3 - Exemples d'application des exceptions

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

Oui, il existe des exceptions au principe d'interdiction de transferts mais qui sont 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 :**

  ✓ à la **sauvegarde de la vie** de cette personne ;

  ✓ à la sauvegarde de **l'intérêt public** ;

  ✓ au respect d'obligations permettant d'assurer la constatation, l'exercice ou la **défense d'un droit en justice** ;

  ✓ à 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 ;

  ✓ à **l'exécution d'un contrat** entre le responsable du traitement et l'intéressé, ou de mesures pré-contractuelles prises à la demande de celui-ci ;

  ✓ à la conclusion ou à **l'exécution d'un contrat** conclu ou à conclure, **dans l'intérêt de la personne concernée**, entre le responsable du traitement et un tiers.

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 et ne reposent donc pas sur ces dérogations.**

Q3 - Exemples d'application des exceptions

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 madame Lucas, l'agence de voyage devra réserver les hôtels dans lesquels elle séjournera. Pour cela, les données personnelles de madame Lucas doivent être envoyées depuis l'agence de voyage située en France vers les hôtels situés en Inde donc dans un pays tiers à l'Union européenne. 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 madame Lucas a signé avec l'agence de voyage.

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 du transport aérien de monsieur Daniel. Le transfert de données ainsi effectué afin de permettre le rapatriement de monsieur Daniel n'est soumis à aucun encadrement spécifique puisqu'il est effectué à titre exceptionnel dans l'intérêt de la personne concernée.