Commission Nationale de l'Informatique et des Libertés

Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques

La loi du 6 août 2004 a donné à la CNIL le pouvoir d'autoriser les transferts internationaux de données vers les pays n'appartenant pas à l'Union européenne, lesquels, pour la plupart ne disposent pas, d'un niveau de protection des données estimé adéquat. Le rapport d'activité 2005 a rappelé les conséquences de ces nouvelles dispositions[1].

Parallèlement, la CNIL s'est intéressée à la question spécifique de la protection des données personnelles dans le cadre des centres d'appels délocalisés et avait décidé de constituer un groupe de travail à cet effet, ainsi que l'a relaté le rapport d'activité 2006[2].

Comme il est apparu très vite que la question des centres d'appels ne devait pas être traitée isolément, le problème posé étant celui de l'externalisation des traitements informatiques en général, le sujet a été élargi à l'ensemble des transferts de données personnelles.

Le service des affaires internationales de la CNIL a organisé de février à mai 2009 une série d'auditions de cabinets de conseil et d'avocats d'affaires impliqués dans le conseil offshore et la préparation de contrats de prestations, ainsi que de sociétés pratiquant l'externalisation offshore, directement ou avec recours à des sociétés tierces.

Ces travaux s'inscrivent dans un contexte de réflexions menées à l'échelle européenne[3] et internationale relatives à la révision de la directive européenne et au développement des échanges internationaux de données.

Le groupe de travail de la CNIL a ainsi tenté de faire le point sur les questions posées par l'externalisation hors de l'Union européenne des traitements informatiques et de proposer des solutions, ce dont il est rendu compte dans le présent document

La Commission est consciente de la sensibilité de ce sujet sur le plan économique, l'externalisation hors de l'Union européenne correspondant souvent à des délocalisations, mais elle n'intervient ici que sur ce qui relève de sa compétence, à savoir la protection des données personnelles.

[1] Rapport d'activité 2005, page 39 en annexe 1
[2] Rapport d'activité 2006, page 74 en annexe 2
[3] Au sein d'un groupe de travail de l'article 29 chargé d'étudier les notions de responsables de traitement et de sous-traitants

I. Définition et contexte de l’externalisation offshore

L'externalisation par les entreprises de certaines de leurs activités par le recours à la sous-traitance est aujourd’hui de plus en plus fréquente. Elle est dite « offshore », si elle concerne la création ou l’utilisation d’une entité juridique dans un autre pays : elle a alors souvent pour but la recherche d’une réduction des coûts, notamment fiscaux, financiers ou salariaux. L’externalisation offshore, dénommée également « offshoring », s’apparente à une délocalisation, lorsqu’elle s’accompagne du transfert d’une activité préexistante en France ; mais, de plus en plus souvent, les activités sont externalisées dès l’origine dans un pays tiers. Dans les deux cas, lorsqu’elle porte sur des services, elle correspond à la consommation en France de prestations réalisées à l'étranger.

L'externalisation offshore des activités de services, qui porte d’ailleurs parfois directement sur les services informatiques, comporte généralement des prestations informatiques incluant le traitement de données personnelles. L’externalisation est surtout le fait des entreprises, mais elle est évidemment susceptible de concerner également d'autres organismes, voire des services publics.

Le terme « nearshore » (ou offshore de proximité) est souvent utilisé pour désigner l’externalisation vers des pays utilisant la même langue et situés dans un fuseau horaire identique ou avoisinant. Pour la France, le « nearshore » concerne les pays d’Europe de l’Est et d’Afrique du Nord, l’offshore s’appliquant notamment à la Chine et à l’Inde.

On utilise généralement l'expression anglaise de Business Process Outsourcing (BPO), littéralement « externalisation de processus d'affaires », pour désigner l'action de confier un pan complet de l'activité d’une entreprise à un prestataire extérieur. Les centres d'appels correspondent d'ailleurs à cette définition, puisqu'il s'agit de confier à un spécialiste un processus de support après-vente des produits, ou un processus de prospection de clients.

Sous le terme BPO, correspondent également des processus plus larges allant du BPO dit vertical portant sur une activité transversale ou fonctionnelle de l'entreprise telle que la comptabilité, la paye ou la gestion des ressources humaines, à un BPO dit horizontal reprenant un des métiers de l'entreprise, tel que par exemple le crédit immobilier pour une banque.

Certains distinguent maintenant une deuxième génération de BPO vertical, consistant pour la société délégataire de BPO à assurer l'infogérance de toute une série de processus. Ceci suppose parfois le rachat d’une filiale captive en charge de ce BPO. Ce peut donc être parfois tout le système d'information qui est externalisé, le but étant d'obtenir un moindre coût avec une seule plate-forme.

On utilise aussi parfois les termes Knowledge Process Outsourcing (KPO), littéralement « externalisation des processus de connaissance », pour identifier une externalisation susceptible de concerner différentes strates d'expertise, telles que l'expertise juridique, la recherche et le développement dans les domaines scientifique, médical, clinique et biologique...

Depuis quelques années, l'externalisation est très souvent associée au *Cloud Computing*, ou "informatique en nuage"[4] : ce concept fait référence à l'utilisation des capacités de mémoire et de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Comme le Cloud Computing pose des problèmes de contrôle, de sécurité et de traçabilité qui vont au-delà de l'externalisation offshore hors de l'Union européenne, la Commission va consacrer à ce sujet un rapport spécifique.

[4] Selon la traduction qui vient d'en être donnée par la Commission nationale de terminologie et de néologie (JO du 6 juin 2010).

II. Les règles applicables en matière « Informatique et libertés »

L'externalisation est un choix stratégique de l'entreprise, choix qui se doit toutefois, de prendre en compte les règles juridiques applicables, en particulier, celles de la loi du 6 janvier 1978 modifiée et de ses textes d'application.

A. L'identification des acteurs

Afin de déterminer les solutions juridiques applicables au transfert international de données envisagé par l'entreprise, il est indispensable d'identifier les parties, et de les qualifier; cette qualification ayant des implications importantes en termes de responsabilité.

Selon l'article 2 d) de la directive 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 des données, *« le responsable de traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, **seul ou conjointement avec d'autres**, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ».*

L'article 2 d) de la directive définit le sous-traitant comme «*la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel **pour le compte** du responsable du traitement* ».

L'article 35 de la loi de 1978 reprend la même notion mais définit plus précisément le rôle du sous-traitant. Il donne notamment plus d'indications sur la façon dont le sous-traitant agit, en rappelant notamment qu'il ne peut le faire que sur instruction du responsable de traitement.

Le sous-traitant n'est tenu que par des obligations contractuelles de confidentialité et de sécurité visant à protéger les données personnelles contre la destruction accidentelle ou illicite, l'altération, la diffusion ou l'accès non-autorisés. Il n'a aucune obligation spécifique résultant de la loi précitée.

B. L'encadrement des transferts de données personnelles hors de l'UE

La notion de transfert de données vers un pays tiers a été précisée dans le guide des transferts élaboré par les services de la Commission[5]. Sont donc soumis aux articles 68 et suivants de la loi de 1978, non seulement les transferts durables ou permanents de données vers un pays tiers, mais également les transferts temporaires impliquant seulement des consultations à distance par des entités établies dans un pays tiers.

[5] Diffusé sur le site Internet de la Cnil, et actuellement en cours de refonte.

1. Les transferts de données personnelles vers des pays tiers

L'article 68 de la loi de 1978 prévoit le principe d'interdiction de transfert de données vers un Etat n'appartenant pas à l'Union européenne, sauf si cet Etat offre un niveau de **protection adéquate** en raison de sa législation interne ou des engagements pris au niveau international.

A l'heure actuelle les pays reconnus comme adéquats sont : l'Argentine, le Canada, Guernesey, l'Ile de Man, Jersey, la Suisse, les Iles Féroé et les Etats-Unis uniquement dans le cadre de leur programme 'Sphère de Sécurité' dit 'Safe Harbor'.

Pour les transferts de données personnelles vers des pays ne présentant pas de protection adéquate, l'article 69 de la loi de 1978 prévoit des **instruments juridiques offrant des garanties suffisantes** : il s'agit notamment des clauses contractuelles types adoptées par la Commission européenne et des BCR (« Binding Corporate Rules » ou règles internes d'entreprise contraignantes). Par ailleurs, l'article 69 de la loi précitée a prévu un certain nombre d'exceptions permettant le transfert.

✓ **Les clauses contractuelles**

Ces clauses contractuelles peuvent être les clauses contractuelles type adoptées par la Commission européenne en 2001 ou bien des clauses alternatives qui seraient principalement basées sur les clauses types.

La Commission européenne vient d'adopter un nouvel ensemble de clauses types permettant de prendre en compte les sous-traitants ultérieurs dans la chaîne de sous-traitance hors de l'Union européenne : 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 ; en outre, 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.

Dans certains cas de chaînes de sous-traitance (cf. schémas ci-dessous), la CNIL accepte des solutions juridiques offrant une certaine flexibilité, telles que :

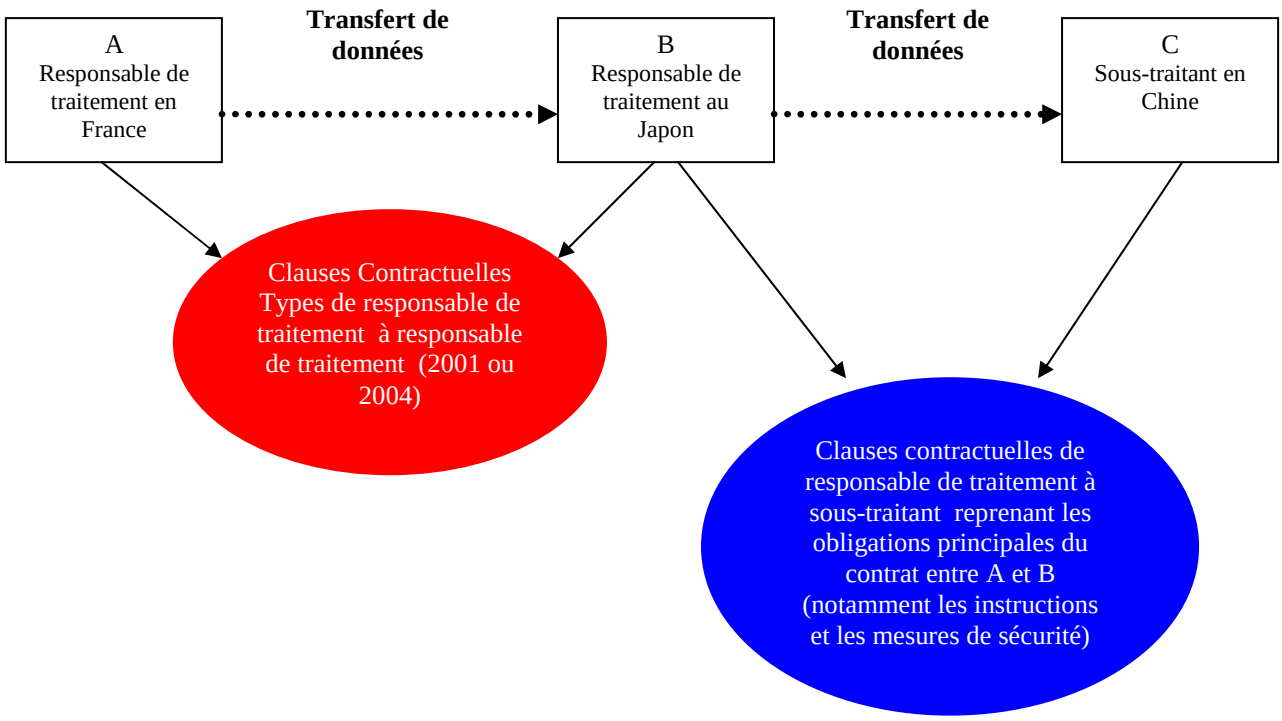
* le **mandat** (le responsable de traitement en France donne mandat au 1er destinataire des données (sous-traitant ou responsable de traitement) pour signer des clauses contractuelles avec le sous-traitant qui intervient en bout de chaîne) ou
* les **clauses contractuelles type tripartites**, ou
* la **combinaison de clauses**.

Différentes hypothèses d'utilisation de clauses contractuelles dans le cadre de chaînes de sous-traitance sont illustrées ci-dessous :

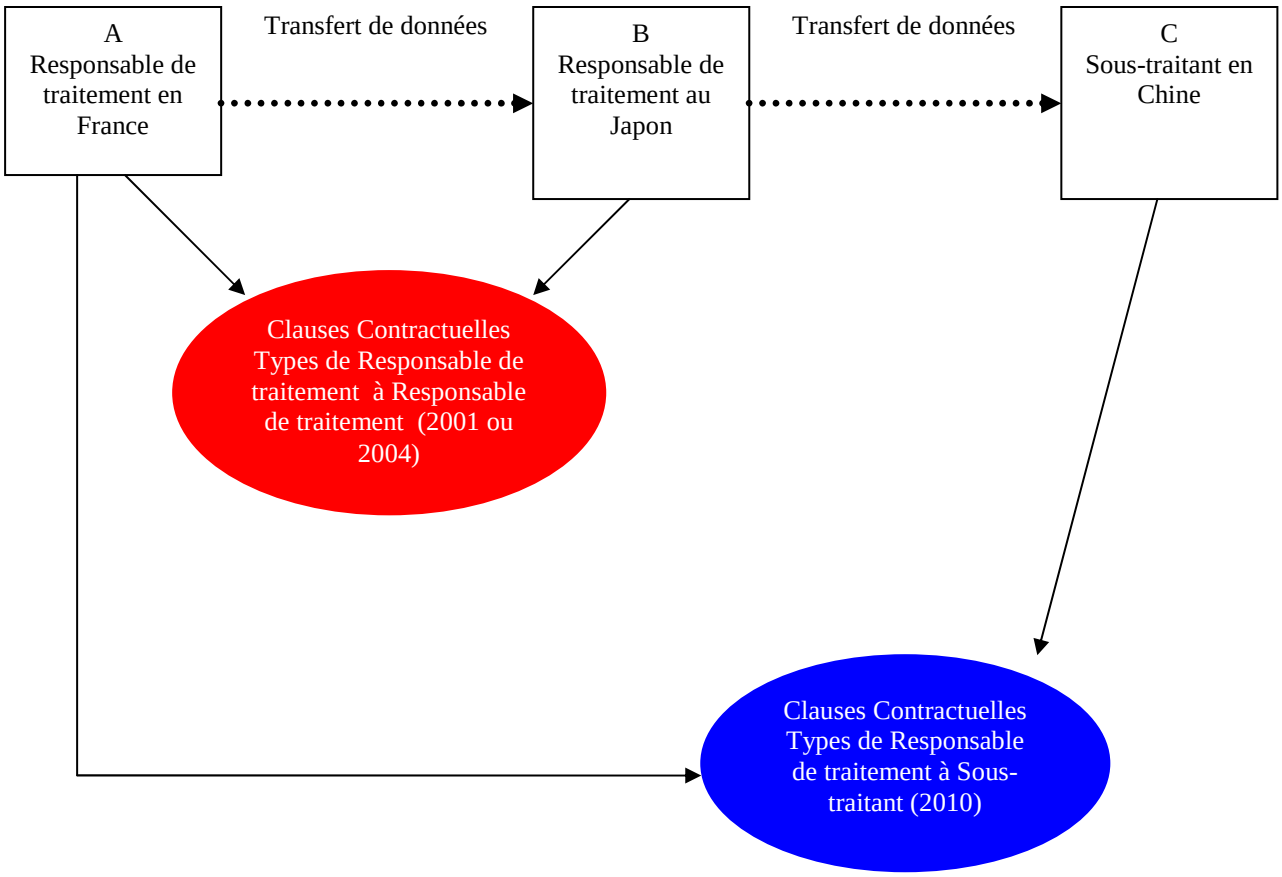
Cas n°1 : Transferts de données personnelles par un **responsable de traitement** vers un autre **responsable de traitement** situé dans un pays hors de l'Union européenne, qui transfère lui-même les données vers un **sous-traitant** situé dans un autre pays hors de l'Union européenne.

Exemple : une société française (A) s'adresse à une société basée au Japon (B) pour la gestion de son fichier clients. La société japonaise sous-traite à une société chinoise (C) les opérations de maintenance du réseau sur lequel les données sont stockées.

Solution 1 : 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.

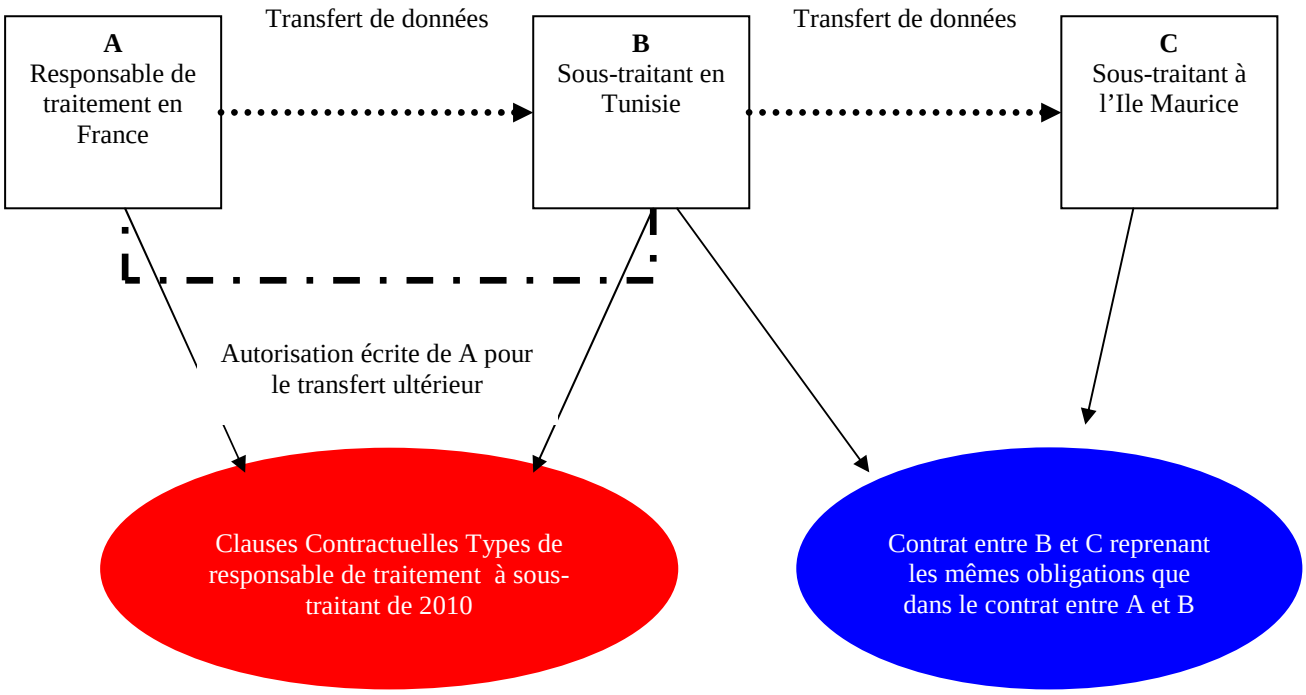


Solution 2 : A et B signent des Clauses contractuelles types de responsable de traitement à responsable de traitement. A et C signent des Clauses contractuelles types de responsable de traitement à sous-traitant.



Cas n°2 : Transferts de données personnelles par un **responsable de traitement** vers un **sous-traitant** situé dans un pays hors de l'Union européenne, qui transfère lui-même les données vers un **autre sous-traitant** situé dans un autre pays hors de l'Union européenne.

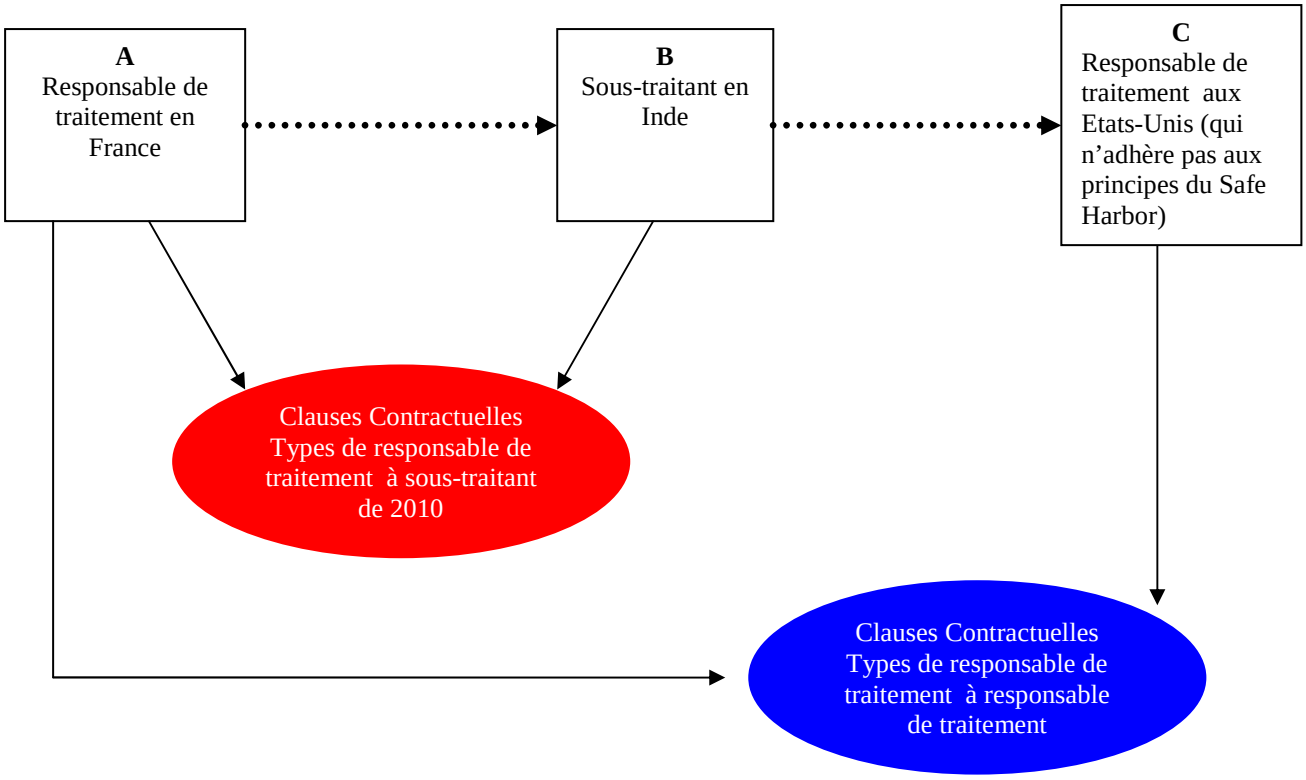
Exemple : une société française(A) charge un sous-traitant tunisien (B) de gérer ses feuilles de paye.
Le sous-traitant tunisien, fait appel à sa filiale à l'Ile Maurice (C) pour procéder à la saisie des informations dans la base de données.



Cas n°3 : Transferts de données personnelles par un **responsable de traitement** vers un **sous-traitant** situé dans un pays hors de l'Union européenne, qui transfère lui-même les données vers un **responsable de traitement** situé dans un autre pays hors de l'Union européenne.

Exemple : un hôtel français(A), filiale d'un groupe d'hôtel américain qui n'adhère par aux principes du Safe Harbor, fait appel à un hébergeur de données en Inde (B). La maison mère de l'hôtel (C) (situé aux Etats-Unis) récupère des données de sa filiale française sur le serveur situé en Inde.

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.



✓ **Les BCRs (Binding Corporate Rules)**

Les BCR, ou règles internes d'entreprise, correspondent à un **code de conduite** qui définit la politique interne d'un **groupe** en matière de transferts de données personnelles hors de l'Union européenne.

Exemple : les BCR peuvent être utilisées lorsque l'activité d'une filiale française d'un grand groupe est externalisée auprès d'une filiale du même groupe située en Russie, si ces BCR couvrent bien le même type de traitement que celui faisant l'objet d'une externalisation (à titre d'exemple : les données des collaborateurs pour la gestion des ressources humaines)

✓ **Les exceptions de l'article 69**

Il existe des exceptions au principe d'interdiction de transferts mais ces dernières sont l'objet de limitations et d'une interprétation stricte car elles ne bénéficient pas des garanties juridiques offertes par l'encadrement qu'apportent l'existence d'une loi de protection jugée comme adéquate par la Commission européenne ou encore les BCR ou les clauses contractuelles types.

La CNIL estime que les exceptions de l'article 69 sont en quelque sorte des exceptions individuelles ou spécifiques, qui ne peuvent s'appliquer aux cas des transferts répétitifs, massifs ou structurels de données personnelles, dont l'importance ou la régularité justifient qu'ils soient encadrés de manière précise.

2. Les données en provenance de pays tiers, sous-traitées en France, et repartant vers le pays tiers d'origine

Cette hypothèse vise des cas où des responsables de traitement établis dans des pays tiers font appel à des sous-traitants localisés en France et les chargent de traiter des données personnelles pour leur compte. Une fois les données personnelles traitées par le sous-traitant français, ce dernier les restitue au responsable de traitement localisé à l'étranger.

Au sens de la loi de 1978, ces données personnelles sont traitées en France et font l'objet d'un transfert de la France vers le pays d'origine, imposant ainsi l'application de la loi Informatique et Libertés, qu'il s'agisse de la déclaration préalable, du respect de toutes les obligations inscrites dans la loi et, enfin, de la nécessité d'obtenir une autorisation de la CNIL pour le transfert en retour des données de la France vers le pays d'origine.

Si les règles de protection françaises doivent s'appliquer au bénéfice de personnes résidant des pays extérieurs à l'Union européenne, il est permis de s'interroger tant sur leur effectivité que sur la lourdeur des procédures imposées aux prestataires français. On peut donc légitimement se demander si une telle approche ne respecte pas plus la lettre que l'esprit de la loi..

C'est pourquoi cette question fait actuellement l'objet d'une étude particulière de la Commission.

C. Les formalités déclaratives

C’est au responsable de traitement de procéder à des déclarations à la CNIL, même s’il n’a pas la maîtrise du traitement, notamment lorsque les données sont hébergées par un prestataire. Pour les transferts vers des pays hors de l'Union européenne n’assurant pas une protection adéquate (ou ne pouvant pas se fonder sur une des exceptions de l’article 69), il est nécessaire d’obtenir l’autorisation de la Commission.

III. Enjeux et solutions

L'externalisation soulève plusieurs enjeux, tant pour les entreprises, qui y ont recours, que pour la CNIL.

Les entreprises doivent définir clairement leurs rôles et responsabilités, tout en recherchant des solutions qui leur permettent de sécuriser leurs demandes d'externalisation tout en évitant les excès de formalités. La CNIL, quant à elle, doit s'efforcer de rationaliser sa procédure de gestion des transferts internationaux de données tout en s'assurant que les règles relatives à la protection des données personnelles ainsi externalisées sont respectées.

A. Aider les entreprises à qualifier leurs rôles et leurs responsabilités

1. Les termes du débat

Bien que les définitions légales soient assez précises, la détermination de la qualité de responsable de traitement ou de sous-traitant n'est pas toujours évidente[6].

Fréquemment, les entreprises faisant appel à des sous-traitants déterminent bien les finalités, mais beaucoup moins les moyens. Le plus souvent, cependant, elles soutiennent que l'externalisation offshore est un choix réalisé en connaissance de cause après avoir analysé l'offre de services et les moyens mis en œuvre par le sous-traitant.

La sophistication des offres de service des prestataires mondiaux tend parfois à responsabiliser davantage le sous-traitant et à lui accorder une certaine autonomie dans la réalisation des opérations. Dans le cadre des auditions organisées par le groupe de travail de la CNIL, il a été constaté que les prestataires proposent des offres de service parfois très sophistiquées, et une expertise unique.

Ainsi, dans les cas d'externalisation de traitements informatiques complexes comportant des sous-traitances en chaîne, l'autonomie du sous-traitant est susceptible de faire débat.

2. Solution proposée

Plusieurs critères d'analyse ont été dégagés par le groupe de travail de la CNIL afin de faciliter l'appréciation de la fonction de prestataire et de cerner les cas où il serait utile de qualifier de responsables de traitement ceux qui ne pouvaient recevoir une telle qualification jusqu'ici.

[6] « Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens » Le sous-traitant est «la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »

a) Le niveau des instructions préalables données par le responsable de traitement

Il s'agit d'apprécier si le niveau d'instruction donné par le client au prestataire dans le cadre du contrat d'externalisation est général ou précis.

b) Le niveau du contrôle de l'exécution des prestations

Il s'agit d'apprécier le degré de contrôle du client sur ses données une fois que ces dernières sont adressées et/ou rendues disponibles au prestataire. En particulier, il s'agit de s'interroger sur le degré de « surveillance » du client en tant que responsable de traitement sur la prestation de son Prestataire.

c) La transparence

Il s'agit d'apprécier le degré de transparence du responsable de traitement au niveau de la prestation de services. En effet, si l'identité de la SCC est connue par les personnes concernées qui utilisent les services du Client, la SCC pourra être présumée comme agissant comme responsable de traitement.

d) L'expertise

Il s'agit d'apprécier le degré d'expertise du prestataire par rapport au client, notamment quant à son niveau de connaissance.

➔ Ces critères doivent être **appréciés dans leur ensemble** et constituent à ce titre un faisceau d'indices. En effet, seule **la réalisation de plusieurs de ces critères** permettra de qualifier le prestataire.

Le tableau ci-dessous pourrait servir d'outil de référence.

Indices	Le prestataire pourra être qualifié de sous-traitant	Le prestataire pourra être qualifié de responsable de traitement
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 laisse le prestataire réaliser ses prestations et le laisse libre d'utiliser les données comme bon lui semble.
Transparence : Le prestataire de service se présente-t-il sous son nom propre ou sous le nom de son client et peut-il les réutiliser pour des fins qui lui sont propres?	L'employé du centre d'appel en Tunisie se présente sous le nom du client et ne réutilise pas les données pour son propre compte.	Le centre d'appel en Tunisie se présente sous son propre nom et réutilise les données à des fins qui lui sont propres.
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.

Ce faisceau d'indices, élaboré par la CNIL, avait d'ailleurs été largement repris dans un avis adopté par le G29 (Groupe des CNIL européennes) le 16 février 2009[7].

[7] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

3. Les solutions écartées

D'autres solutions ont été étudiées par le groupe de travail afin de permettre de contourner les difficultés de qualification. Toutefois, l'audition des différentes parties prenantes a permis au groupe de travail de conclure que ces solutions n'étaient pas pleinement satisfaisantes.

Il a ainsi été envisagé de développer la théorie du délégué permettant au client, responsable de traitement, de donner mandat à son prestataire afin que ce dernier procède aux formalités déclaratives pour son compte. Les risques de déresponsabilisation du responsable de traitement conduisent à écarter une telle solution. Afin d'éviter cet écueil, les obligations respectives du client et du prestataire devront être expressément définies dans le contrat qui les lie.

De même, la notion de co-responsabilité a rapidement semblé difficile à mettre en œuvre dès lors que les responsabilités sont souvent difficilement identifiables au moment de la négociation du contrat. On risque dès lors d'assister à une dilution des responsabilités.

Une solution à l'étude : la création d'un statut légal pour le sous-traitant

Un des constats soulevés dans le cadre des réflexions du groupe de travail est l'absence de statut légal du sous-traitant dans la loi de 1978.

La loi ne prévoit ainsi aucune obligation légale à la charge du sous-traitant, et aucune obligation de coopération vis à vis du responsable de traitement. Dès lors, une solution consisterait à créer un statut légal du sous-traitant lui imposant une responsabilité pénale notamment en cas de non-respect des obligations légales de sécurité et de confidentialité et une obligation de coopération vis à vis du responsable de traitement et des autorités compétentes.

B. « Désengorger » le système d'autorisation, tout en prenant en compte au cas par cas les traitements « sensibles »

1. La création d'un formulaire spécifique pour les demandes de transfert

Un nouveau formulaire de demande d'autorisation spécifique permettant au déclarant de préciser le cas échéant les finalités et les conditions d'un transfert de données personnelles vers un pays ne disposant pas d'une législation de protection des données adéquates a été mis en ligne sur le site de la CNIL. Même si celui-ci est susceptible de faire l'objet d'améliorations, son ergonomie est d'ores et déjà très appréciée des entreprises.

2. L'aménagement de la procédure d'autorisation des transferts

Avec l'entrée en vigueur de la loi n° 2009-526 du 12 mai 2009 qui a modifié l'article 15 de la loi de 1978, la Commission peut charger le président ou le vice-président délégué d'exercer eux-mêmes cette attribution. Elle a fait usage de cette possibilité par sa délibération n° 2009-674 du 26 novembre 2009 portant délégation d'attributions au président et au vice président délégué. Toutefois, la Commission reste compétente, sur demande du président, pour examiner en formation plénière, les demandes de transfert qui présentent des difficultés ou une complexité particulières (par exemple les demandes d'autorisation de transferts de données de santé).

La délégation de la procédure d'autorisation au président ou au vice-président délégué, évoquée plus haut, a apporté plus de fluidité dans la gestion de ces dossiers de transferts de données et par conséquent plus de rapidité du point de vue des déclarants.

3. Allègement des formalités et adaptation des normes

A l'instar des formalités allégées prévus pour les transferts de données dans le cadre de traitements relevant d'autorisations uniques[8], des possibilités de transfert ont été données dans le cadre de deux normes simplifiées n° 46 relative à la gestion des personnels et n° 48 relative à la constitution de fichiers clients et prospects. Comme ces possibilités de transfert ont un champ d'application jugé peu adapté par les déclarants pour pouvoir être utilisé, il est actuellement envisagé de procéder à une adaptation de ces normes.

4. La promotion des BCR

Les BCR (ou règles internes contraignantes) peuvent s'avérer un instrument juridique utile dans l'hypothèse où **l'externalisation se fait au sein d'un même groupe de sociétés.** La CNIL s'investit beaucoup pour la promotion des BCR auprès des grandes entreprises françaises et internationales externalisant leurs activités vers des filiales ou « centre d'excellence » situés hors de l'Union européenne[9].

Elle a ainsi mis en place des clubs BCR sectoriels[10] visant à informer et aider les entreprises dans leur démarche de rédactions de BCRs.

[8] Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitement automatisé de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle ;
- Délibération n° 2008-005 du 10 janvier 2008 portant autorisation unique de mise en œuvre par les entreprises ou organismes exploitants de médicaments de traitements automatisés de données à caractère personnel relatifs à la gestion des données de santé recueillies dans le cadre de la pharmacovigilance des médicaments postérieurement à leur mise sur le marché ;
- Délibération n° 2008-097 du 10 avril 2008 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la prévention et à la gestion des impayés par chèque bancaire.
- Délibération n° 2008-198 du 9 juillet 2008 modifiant l'autorisation unique n° AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit.

[9] Participation à des conférences rassemblant les grandes entreprises, édition d'une brochure sur les BCRs.

[10] Aéronautique, banque/assurance, IT, cabinets d'avocats, grande distribution …

En outre, à la demande de prestataires, la CNIL étudie la possibilité pour un sous traitant de rédiger des BCR garantissant la protection des données lors des transferts internationaux de données.

5. L'adoption de législations présentant un niveau de protection adéquat par les pays tiers.

Au-delà du développement de l'utilisation d'instruments juridiques prévus par la directive 95/46/CE et la loi de 1978, il est également primordial de promouvoir ce même modèle européen auprès de pays tiers ne disposant pas de législation en matière de protection des données.

Ainsi, les pays tiers ayant adopté une législation de protection des données fondée sur le modèle européen peuvent présenter à la Commission européenne une demande d'adéquation.
Si cette demande d'adéquation aboutit positivement, à savoir par l'adoption d'une décision d'adéquation par la Commission européenne, alors les transferts de données personnelles vers le pays tiers disposant d'une législation reconnue comme adéquate pourront se faire librement conformément à l'article 68 de la loi de 1978.

La CNIL soutient cette voie, dans laquelle se sont engagés notamment le Maroc et la Tunisie, qui disposent maintenant d'une loi de protection des données et devraient prochainement présenter une demande d'adéquation à la Commission européenne.

III. Conclusion

L'externalisation est un choix stratégique de l'entreprise, qui peut parfois mettre en jeu le niveau de protection assuré aux données personnelles. Les solutions apportées dans le présent document peuvent donc servir aux entreprises soucieuses d'encadrer de façon satisfaisante le traitement et les transferts de données effectués auprès de prestataires de services.

En particulier, le faisceau d'indices proposé par la CNIL devrait aider les entreprises à déterminer la qualification exacte de leurs prestataires.

Par ailleurs, l'encadrement des transferts de façon satisfaisante doit permettre aux entreprises d'apporter un niveau de protection adéquat aux données transférées.

Enfin, l'extension du champ d'application de certaines normes simplifiées ainsi que l'amélioration des procédures de traitement des demandes d'autorisation devraient participer à une meilleure gestion des demandes d'autorisations de transferts de données réalisées par les entreprises ayant recours à l'externalisation.