Association Française des Correspondants
à la protection des Données à caractère Personnel

Le cotraitement de données à caractère personnel

Mais qui est responsable ?

Pilotage

Sylvain LEBARBIER (AG2R LA MONDIALE)

Contributeurs

Yves-Philippe BREANT (MATMUT)
Nadine CHAUSSIER (AXA)
Patrick EADE (SURAVENIR)
Paul GARNIER (IPECA)
Gaëlle GISSOT (GMF)
Henri GUIHEUX (SCOR)
Michel JOUBREL (AXA)
Pierre-Charles JUHEL (MGP)
Virginie PANIER (ALICO)
Nathalie PINON (IMA)
Marie-Christine SUDRE (GMF)
Patrick VILLARD (SWISSLIFE)
Anne-Laure VILLEDIEU (cabinet CMS-BFL)
Alexandra YONC (APRIL)

Remerciements

Bruno RASLE (AFCDP)
Marie-Blanche NIEL-GILLY (Pages Jaunes)

A propos de l'AFCDP

L'AFCDP a été créée dès 2004, dans le contexte de la modification de la Loi Informatique & Libertés qui a officialisé une nouvelle fonction, celle de «Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant Informatique & Libertés).

L'AFCDP rassemble largement, au-delà des professionnels de la protection des données et des seuls Correspondants désignés par leurs organismes auprès de la CNIL : elle regroupe en effet toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : Correspondants Informatique & Libertés, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, universitaires et étudiants, experts en sécurité, qualiticiens, consultants…

Quelques membres AFCDP : 3 Suisses, Accor, Adecco, Aéroports de Paris, AG2R LA MONDIALE, AXA, BP France, Carrefour, CNP Assurances, Conseil Général de Seine-Maritime, CCIP, Crédit Immobilier de France, École Polytechnique, France Telecom, IBM France, Institut Curie, Groupe Casino, HALDE, Michelin, La Poste, Port autonome de Dunkerque, RATP, Région Lorraine, SCOR, SNCF, Total, Ville de Paris…

Pour plus d'information sur l'association : www.afcdp.net

Membre AFCDP ! Ce document vous est strictement réservé. Merci de ne pas le diffuser.

Il est soumis à votre critique. Vous êtes invité à faire part de vos remarques, commentaires, témoignages et suggestions pour l'améliorer et en permettre une publication définitive, corrigée et enrichie.

Des difficultés à clarifier les responsabilités de chacun dans le cadre d'un partenariat ou d'une sous-traitance ?
De multiples acteurs intervenant sur un même traitement ?

Ce document est fait pour vous…

L'objectif du présent document est d'apporter un éclairage sur des situations complexes où la notion de responsabilité peut-être difficile à appréhender en raison de la multiplicité des acteurs intervenants dans une même chaîne de traitement.

Cette étude entend également offrir aux responsables de traitements quelques pistes pour mieux mesurer l'étendue de leurs responsabilités, des recommandations et conseils pratiques ainsi qu'une méthodologie basée sur l'utilisation de critères permettant de clarifier les rôles de chacun et de limiter ainsi tout risque de mise en cause.

Le présent support prendra tout particulièrement en considération la dimension « Groupe », laquelle concerne la majeure partie des organismes qui ont contribué à son élaboration. Il fournira donc à cet égard un éclairage nouveau.

Le périmètre étudié concerne les traitements de données mis en œuvre

- par les professions de l'épargne, de l'assurance, de la prévoyance, de la santé et de la retraite ; leurs partenaires, prestataires ; leurs autorités de tutelle ; leurs organisations professionnelles (AGIRA, FFSA, GEMA, CTIP…) ;
- par des responsables de traitements distincts, qu'ils soient autonomes ou interdépendants ;
- à partir de données se rapportant à une seule et même personne (que la collecte ait lieu en une seule fois ou après plusieurs interventions) ;
- lors d'opérations simultanées (la donnée est nécessaire à la mise en œuvre de plusieurs traitements relevant de personnes différentes et autonomes), ou successives (la donnée doit être traitée par le premier responsable de traitement avant de pouvoir être exploitée par le second, qui est donc en situation de dépendance par rapport au premier).

Les situations de « cotraitement » abordées relèvent de trois logiques différentes

- la sous-traitance
- la cession de données
- la « co-gestion »

Signification des sigles et acronymes utilisés

AFCDP	Association Française des Correspondants à la protection des Données à caractère Personnel
AGIRA	Association de Gestion des Informations sur le Risque en Assurance
CNIL	Commission nationale de l'informatique et des libertés
CTIP	Centre Technique des Institutions de Prévoyance
FFSA	Fédération Française des Sociétés d'Assurance
FICP	Fichier national des incidents de remboursement des crédits aux particuliers
G29	Groupe de travail Article 29 sur la protection des données
GEMA	Groupement des entreprises mutuelles d'assurances
IARD	Incendie Accidents Risques Divers
IP	Institution de prévoyance
IRC	Institution de retraite complémentaire
LCEN	Loi pour la confiance dans l'économie numérique
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
UFMD	Union Française du Marketing Direct
VAD	Vente à distance

Synthèse de l'étude

- Le responsable de traitement est la personne qui décide de la création du traitement en déterminant notamment sa **finalité**. Cette détermination doit naturellement être libre et autonome.
- Cela permet ainsi de différencier le responsable de traitement qui détermine la finalité du traitement du sous-traitant qui se contente de mettre en œuvre les traitements.
- Il n'existe **pas de définition légale du « cotraitement »** qui aurait pu constituer une base légale pour la détermination d'une « coresponsabilité » permettant ainsi de clarifier l'étendue de la responsabilité de chacun.

La responsabilité d'un traitement est acquise à partir du moment où peut-être déterminée la personne qui décide de sa création.

- C'est par conséquent sur le fondement de **critères logiques** que nous nous sommes appuyés afin de mieux appréhender cette hypothèse de partage des responsabilités. Ces critères sont au nombre de trois :
  - **un critère formel** :

    Observer si la loi ou le contrat prévoit la responsabilité de l'acteur
  - **un double critère liberté/autonomie**

    Consiste à apprécier la liberté dans la décision de la création de traitement, et l'autonomie décisionnelle dans sa mise en œuvre opérationnelle
  - **un critère de contrôle**

    Consiste à déterminer quel est le « propriétaire » des données
- Il est progressivement apparu en se référant aux sources mêmes de la loi Informatique et Libertés et en recourant aux critères logiques énumérés précédemment, que cette coresponsabilité telle que nous l'entendions n'avait pas lieu d'être. On pourra ainsi prioritairement retenir l'existence :
  - soit d'une responsabilité unique d'un responsable de traitement par rapport à des sous-traitants (logique de « sous-traitance »),
  - soit d'un accord de partenariat commercial induisant une cession de données dans le cadre d'un second traitement de finalité différente ou identique (logique de « cession »),
  - soit d'un accord de partenariat à des fins de gestion, chaque acte de gestion étant subordonné à l'existence d'un second traitement incombant à un autre responsable de traitement (logique de « cogestion »).

Recommandations

Clarifier les responsabilités entre les différents intervenants sur les données

Au regard de ces critères, il est apparu comme indispensable d'attribuer clairement (par voie contractuelle) les responsabilités sur les données personnelles et les traitements entre les différents intervenants afin d'assurer une bonne application de la loi Informatique et Libertés (clarté des mentions d'information destinées aux personnes, accomplissement des formalités préalables…).

Points de vigilance

La contractualisation ne doit pas contribuer à masquer les responsabilités incombant fondamentalement à chacun, et notamment :

- que la contractualisation ne doit pas avoir pour objet de transférer la responsabilité originelle du responsable de traitement à son sous-traitant, et de méconnaître ainsi par la suite les obligations légales qui lui incombent ;
- que si la finalité du traitement est nécessairement déterminée par le responsable de traitement, le sous-traitant peut disposer d'une certaine latitude sur la détermination des moyens à mettre en œuvre (matériel, logiciel, conseils et propositions, savoir-faire, organisation…) pour atteindre le résultat attendu. Cette latitude est une autonomie « relative » dans la mise en œuvre du traitement, qui est toujours effectuée sous la responsabilité de l'organisme qui la délègue, et sur ses instructions. Le responsable du traitement reste ainsi, à la différence de son sous-traitant, la seule entité à pouvoir se prévaloir d'une autonomie « absolue » (ou indépendance décisionnelle) ;
- qu'un sous-traitant peut lui aussi être responsable de ses propres traitements, spécifiquement et distinctement par rapport à ceux qu'il met en œuvre pour le compte de ses donneurs d'ordre. Une nouvelle fois, la voie conventionnelle devra faire l'objet d'une attention toute particulière pour déterminer ce qui relève de la pure sous-traitance de ce qui découle d'un accord de partenariat entre responsables distincts.

Préface

L'imbrication de plus en plus complexe des systèmes d'informations des entreprises, notamment par le recours croissant à l'externalisation ou le développement de la logique partenariale, contribue à la multiplication des traitements de données personnelles de grande ampleur et favorise l'apparition d'une myriade d'intervenants ayant divers niveaux de responsabilité sur les données traitées.

Les acteurs du secteur de l'assurance, par la diversité de leurs activités (assurance IARD, retraite, prévoyance, épargne, santé, assistance etc.) et leurs rapprochements au sein de grands « groupes », sont particulièrement concernés par ces échanges et partages de données, pour lesquels il n'est cependant pas toujours aisé de déterminer précisément « qui » est responsable « de quoi ». Ainsi, depuis la réforme de la loi Informatique et Libertés n°78-17 du 6 janvier 1978 par la loi n°2004-801 du 6 août 2004, de nombreux acteurs du secteur ont engagé des chantiers de mise en conformité en passant au crible l'ensemble de leurs systèmes d'informations mettant en œuvre des traitements de données à caractère personnel.

Au cours des premiers échanges du groupe de travail constitué au sein de l'AFCDP pour réfléchir à la problématique en novembre 2009 est née l'idée qu'une responsabilité commune sur un seul et même traitement pouvait peut-être exister, la question étant de savoir « comment » celle-ci pouvait alors être mise en œuvre.

Cependant, après avoir étudié de manière approfondie plusieurs cas d'espèce, un net consensus a émergé sur le fait que la notion de « coresponsabilité » sur ce qui a alors été baptisé « cotraitements » ne reflétait en fait qu'un réflexe destiné à simplifier trop rapidement une situation complexe dans laquelle la détermination des responsabilités était particulièrement confuse.

Dans les cas qui ont été étudiés par l'AFCDP, il est en effet apparu que les responsabilités pouvaient bien souvent être abordées sous l'angle du partage et de la solidarité entre les différents intervenants. Au cours de la première réunion du 27 novembre 2009, le groupe de travail a ainsi listé certains cas, propres au secteur de l'assurance, où la détermination d'un responsable de traitement unique n'était *a priori* pas évidente.

Lors de la réunion du 29 janvier 2010, le groupe de travail a pu clarifier un certain nombre de situations identifiées dans un premier temps comme des cas de « cotraitements ». Plusieurs hypothèses ont alors pu se dégager : soit il existait plusieurs traitements autonomes mis en œuvre par des responsables de traitements distincts ; soit la détermination des responsabilités respectives des différents acteurs intervenants révélait des opérations de sous-traitance.

Ces hypothèses ont fondé toute la logique du présent document, que nous livrons aujourd'hui à tous les acteurs de la protection des données à caractère personnel. Réalisé grâce à la participation de nombreux intervenants particulièrement concernés par cette problématique de « cotraitement », il représente ainsi un outil destiné à tous les responsables de traitement afin de leur permettre de mieux appréhender les responsabilités de chacun dans le cadre de traitements de données complexes impliquant plusieurs intervenants. Il comprend deux parties : une analyse des textes dans un premier temps, puis une déclinaison opérationnelle.

Je tiens à saluer les contributeurs dont les réflexions ont donné naissance à ce document et vous souhaite une bonne lecture.

Paul-Olivier GIBERT
Président de l'AFCDP

Sommaire

1. Critères et définitions

1.1 Référentiel légal

1.1.1 Qualification de « responsable de traitement »

La définition de responsable de traitement est donnée à l'article 3 de la loi Informatique et Libertés : il s'agit *« sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, [de] la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* ».

Il convient d'ores et déjà de relever que la transposition de la directive 95/46/CE du 24/10/1995[1] en droit français n'a pas retenu dans sa définition la possibilité d'une responsabilité partagée avec d'autres personnes. Selon la directive, la détermination des finalités et des moyens du traitement pouvait être faite « *seul ou conjointement avec d'autres* ». La transposition de cette définition aurait en l'état permis une coresponsabilité des acteurs ayant décidé, de manière libre, autonome et concertée, de la création d'un traitement. Cette faculté n'a cependant pas été retenue par les parlementaires français[2].

La loi française prévoit que la responsabilité du traitement est établie en considération de **deux critères** :

- la personne est compétente pour décider de la **finalité** du traitement : il s'agit ici de choisir l'objectif de la collecte d'informations et le sort des données, la finalité pouvant notamment être évaluée au regard de la pertinence économique, technique, ou encore organisationnelle du traitement. Ces finalités correspondent à des besoins qui sont propres à l'organisme qui les invoque.
- la personne est compétente pour décider des **moyens** du traitement : celui qui décide à quoi va servir le traitement va décider également de ses modalités de mise en œuvre : quelles données seront traitées, pendant combien de temps, à partir de quelles applications …

Les « moyens » doivent être considérés comme une déclinaison opérationnelle du traitement, et entendus de manière générale : lorsqu'une personne confie à une seconde la responsabilité de mettre en œuvre pleinement et entièrement un projet, les opérations réalisées par cette dernière seront considérées comme relevant de la responsabilité de la première personne, quel que soit le degré d'autonomie accordé à la seconde : le responsable opérationnel n'est pas le « responsable du traitement » au sens de la loi Informatique et Libertés, et doit être considéré comme un simple « moyen » choisi par celui-ci pour mettre en œuvre le traitement. Ainsi, le degré d'autonomie du sous-traitant choisi par le responsable de traitement ne remet pas en cause la détermination du responsable de traitement, dès lors que le sous-traitant agit exclusivement sur instruction et dans l'intérêt exclusif de son client

Sur ce point, il convient de noter que l'avis du G29[3] précise que si la détermination de la finalité du traitement emporte nécessairement la qualification de responsable de traitement, la détermination des

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, 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

[2] Voir le rapport n°218 réalisé à l'issue de la réunion de la commission des lois en date du 19 mars 2003, présidée par M. Garrec, et qui révèle que « *L'Assemblée nationale a adopté, sur proposition de son rapporteur de la commission des Lois, M. Gérard Gouzes, et avec l'avis favorable du Gouvernement, un amendement supprimant les termes « seul ou conjointement avec d'autres », estimant imprécise cette notion de co-responsabilité. En effet, la notion de responsable détermine notamment le droit national applicable ; or, il s'agit d'éviter des conflits de lois en cas de pluralité des responsables, ou la répartition d'office de la présomption de responsabilité entre plusieurs personnes ».*

[3] Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant » adopté le 16 février 2010

moyens techniques et d'organisation peuvent tout à fait être déterminés par le sous-traitant sans remettre en cause les responsabilités initiales.

La responsabilité du traitement est donc acquise à partir du moment où peut être déterminée quelle personne décide de celui-ci[4]. Cette détermination doit naturellement être libre et autonome, ce qui peut éventuellement présenter des difficultés d'appréciation lorsque l'entité est soumise à des autorités dites « de tutelle » (fédérations AGIRC-ARRCO par exemple), qui encadrent et contrôlent son activité de manière suffisamment étroite pour dénoter une éventuelle responsabilité dans la détermination des finalités et des moyens des traitements.

Par ailleurs, la qualité de responsable de traitement s'oppose à celle de « sous-traitant », lequel se contente de mettre en œuvre les traitements déterminés par le responsable du traitement (cf. § suivants).

L'AFCDP s'interroge sur l'importance de l'autonomie conférée au sous-traitant, dont la responsabilité pourrait se retrouver confondue avec celle de son client. Cela pourrait *a priori* être le cas pour les groupements de moyens de type « GIE » dont l'autonomie décisionnelle par rapport aux membres qui les composent est très importante.

1.1.2 Le responsable de traitement et le sous-traitant

Le sous-traitant effectue des opérations pour le compte du responsable du traitement. À ce titre il agit uniquement sous l'autorité de celui-ci, « *sur instruction* » comme le spécifie l'article 35 de la loi Informatique et Libertés[5].

Le rapport de sous-traitance sera généralement perçu comme une relation contractuelle entre l'organisme responsable du traitement et un prestataire extérieur. Il convient toutefois de spécifier qu'au sein d'un même groupe de sociétés, ces relations de sous-traitance sont manifestes, même si elles n'apparaissent pas clairement en tant que telles. Ainsi, si une société se voit confier par une autre la mise en œuvre opérationnelle d'un traitement, la première devra être considérée comme le sous-traitant de la seconde au sens de la loi Informatique et Libertés, quand bien même ces services relèveraient d'un seul et même Groupe d'entreprises.

En définitive, cette conception pourrait aussi revenir à distinguer en interne les « maîtrises d'ouvrage », qui décident de la création du traitement (ex : les directions « métiers ») et de ses moyens de mise en œuvre, des « maîtrises d'œuvre » (ex : la direction des Systèmes d'Information) qui doivent être considérées comme leur sous-traitant interne au sens de la loi Informatique et libertés.

---

[4] Voir à ce titre la délibération n°2007-004 de la CNIL en date du 8 mars 2007 et reconnaissant à une plate-forme de mutualisation de fichiers clients issus du secteur bancaire (à des fins de profilage en vue de l'obtention de crédits immobiliers) le statut de responsable de traitement : « *les données sont traitées dans des fichiers informatisés distincts en fonction de l'établissement qui les a transmises à la société Experian, mais qui ont vocation à être mis en relation à tout moment pour permettre l'élaboration des rapports de crédit. Dès lors, ce projet constitue un traitement automatisé de données personnelles, caractérisé par des finalités et des moyens informatiques déterminés par la société Experian, qui, conformément au 1 de l'article 3 de la loi du 6 janvier 1978 susvisée, en est ainsi le responsable* ».

[5] « *Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.*
Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. […]
Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »

1.1.3 Absence de base légale pour la coresponsabilité Informatique et Libertés

Il n'existe pas de définition légale du « cotraitement » encadrant de manière fiable les modalités selon lesquelles un régime de coresponsabilité pourrait être appliqué. Il convient toutefois de remarquer que dans son avis du 16 février 2010, le G29[6] a retenu que « *la probabilité de voir de multiples acteurs participer au traitement de données à caractère personnel est naturellement liée à la multiplicité des activités qui, selon la directive, peuvent constituer un «traitement» devenant, au final, l'objet de la « coresponsabilité »*.

À cette occasion, le G29 a également précisé qu'il était très important « *que les rôles et les responsabilités puissent facilement être attribués, pour éviter que les complexités de la coresponsabilité n'aboutissent à un partage des responsabilités impossible à mettre en œuvre, qui compromettrait l'efficacité de la législation sur la protection des données »*.

La clarification des rôles et responsabilités des différents acteurs par la contractualisation sera donc absolument essentielle et sera par conséquent étudiée tout au long du présent document.

1.1.4 Responsabilité civile partagée (rappels)

Le partage de la responsabilité en cas de « cotraitement » représente notre principale préoccupation : en cas de dommage subi par une personne dans le cadre du traitement de ses données personnelles, celle-ci doit-elle se retourner contre une personne morale spécifique, ou lui est-il loisible de se retourner contre tout organisme impliqué dans la chaîne de traitements ? Si oui comment, et surtout, pourquoi ? Enfin, l'organisme dont la responsabilité aura été engagée ou retenue peut-il se retourner contre un autre responsable de traitement ?

La **responsabilité civile** pose pour principe la réparation de tout dommage causé à autrui (art. 1382[7] et 1384[8] du Code civil) par son auteur. Cette responsabilité ne sera engagée qu'à la condition qu'un fait générateur d'un préjudice soit établi.

Il est parfois difficile, dans les grands groupes, d'identifier la personne morale responsable d'un traitement de données. C'est donc naturellement l'entité la plus visible par le consommateur (*cf*. documents contractuels ou commerciaux, mentions Informatique et Libertés comportant l'adresse où exercer ses droits) qui verra sa responsabilité mise en cause.

Il convient donc de veiller à une communication externe claire vis-à-vis des personnes dont les données sont traitées afin que l'entité, responsable du traitement, apparaisse très clairement.

L'AFCDP constate que la plupart des membres du groupe ont déjà fait l'objet de demandes d'informations de la part de la CNIL ayant pour origine des plaintes de clients n'ayant pas identifié le bon responsable de traitement.

Cela est par exemple le cas lorsque l'assureur propose sous sa marque des produits d'un partenaire dont il n'est que le distributeur (principe de la « marque blanche ») ou le gestionnaire délégué, ou lorsque la donnée collectée est destinée simultanément à plusieurs responsables de traitements distincts.

Il est également important de signaler la confusion susceptible de naître de contrats multipartites : plusieurs responsables de traitements font appel au même prestataire ou partenaire dans le cadre d'un seul et

[6] Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», adopté le 16 février 2010 par le Groupe de travail «ARTICLE 29» sur la protection des données (dit "G29")

[7] « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer.* »

[8] « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. […] Les maîtres et les commettants, [sont responsables] du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés* » ;

unique contrat, si bien que les données manipulées peuvent relever indifféremment de l'un ou de l'autre responsable. Dans ce cas, il est important de préciser au sein de ce même contrat ou dans le cas de protocoles spécifiques annexés à celui-ci sur quel périmètre doit s'exercer la compétence de chacun, soit afin de tenter de s'exonérer de sa responsabilité en invoquant la faute d'un tiers, soit afin d'engager par la suite une action récursoire contre celui-ci.

1.1.5 Responsabilité solidaire/appel en garantie : le cas « Free-Pages Jaunes »

Un téléconseiller de l'opérateur Free, exaspéré par les appels à répétition d'une cliente, ajoute dans l'annuaire réalisé par la société la mention "*elle est blonde, ras-le-cul de la blonde*" à hauteur de son adresse et de son numéro de téléphone. L'annuaire est ensuite transmis en l'état aux Pages jaunes, qui publient cette information.

Dans un jugement du 23 décembre 2009[9], le tribunal d'instance d'Issoire a estimé que « *les deux fautes, l'une de nature contractuelle imputée à Free, et l'autre de nature délictuelle commise par la société Pages Jaunes ont produit le dommage consistant dans la publication de la mention dans l'annuaire* ».

Il convient de noter que la responsabilité contractuelle de Free avait été retenue principalement pour insuffisance d'information sur le droit d'opposition du client (alors même que ce droit était rappelé dans les conditions générales du contrat), et en établissant et diffusant des informations ne correspondant pas à l'identité de l'abonné auquel Free a attribué un numéro de téléphone, tandis qu'il été estimé que Pages Jaunes avait commis une « *faute d'imprudence* » au sens des articles 1382 et 1383 du Code civil. Dans l'exercice de son activité, il lui appartenait en effet de prendre toutes les précautions nécessaires pour que cette activité ne cause pas de dommage à autrui.

Enfin, le contrat liant Free aux Pages Jaunes prévoyait que Free garantissait cette dernière contre tout recours lié aux informations contenues dans la base annuaire de Free. Dans ces circonstances, cette dernière a été appelée en garantie par les Pages Jaunes.

Au final, seuls les dépens ont fait l'objet d'une condamnation *in solidum*, mais on peut supposer qu'en l'absence d'une clause de garantie dans la convention liant les deux sociétés, une condamnation solidaire portant sur la totalité des dommages aurait pu être prononcée, générant ainsi devant le tribunal une situation de cotraitement.

L'AFCDP recommande à tout responsable de traitement intervenant de manière successive dans une chaîne de traitements d'accomplir les diligences qui lui incombent lors de chaque nouvelle campagne de collecte de données, car sa responsabilité pourra être engagée pour négligence lors de l'exploitation d'un fichier acquis auprès d'un autre responsable de traitement si celui-ci contient des informations non conformes. Par ailleurs, les clauses de garanties doivent être encouragées entre les partenaires gérant un même fichier client.

1.1.6 Responsabilité pénale partagée (rappel)

La principale question est ici de savoir dans quelle mesure la responsabilité pénale de plusieurs organismes impliqués dans la mise en œuvre d'un traitement pourrait se trouver engagée, et si tel est le cas, à quel titre ?

[9] Tribunal Instance Issoire, 23 décembre 2009, RG n°11-09-000061

La responsabilité pénale vise à sanctionner un manquement à la loi pénale indépendamment de tout préjudice causé à un tiers. L'action pénale ne peut donner lieu à une condamnation qu'aux conditions cumulées suivantes :

- un texte sanctionne explicitement le comportement reproché,
- un fait a effectivement été accompli,
- l'auteur du fait incriminé l'a intentionnellement commis[10].

Les incriminations définies par la loi Informatique et Libertés sont d'ordre pénal[11]. La question d'une éventuelle complicité se pose par conséquent lorsque des infractions sont commises par un responsable de traitement.

La complicité est définie à l'article 121-7[12] du Code pénal comme le fait pour une personne de faciliter sciemment, par aide ou assistance, la préparation ou la consommation d'une infraction. Une action à l'encontre d'un responsable de traitement au titre de la complicité d'un délit commis par un autre responsable de traitement est par conséquent tout à fait envisageable d'un point de vue strictement juridique. Elle est par ailleurs pleinement compatible avec les dispositions des articles 121-2 et 226-24 du Code pénal (responsabilité possible des personnes morales pour les infractions commises pour leur compte par leurs organes ou représentants[13]).

Ce type de responsabilité semble toutefois pouvoir être mis en cause dans un nombre de cas pratiques très limités, et cela pour **deux raisons** :

- la typologie des comportements susceptibles de caractériser un acte de complicité lié à une violation de la loi Informatique et libertés est très restreinte, tout au plus est-il à première vue possible d'envisager une complicité directe par fourniture de moyens matériels (une société mère qui imposerait à ses filiales de mettre en œuvre un traitement illicite en utilisant un logiciel prohibé ou en collectant des données non autorisées, et hébergerait les données pour ses propres fins), ou indirecte par fourniture d'instructions (cas d'une société actionnaire principale d'une autre société responsable de traitement, et qui impulserait la politique de cette dernière dans le sens d'une violation évidente de la loi Informatique et Libertés pour satisfaire ses propres intérêts[14] ?).

- il n'est pas forcément évident dans le domaine de la protection des données personnelles de distinguer le « complice » du « coauteur » de l'infraction : il est en effet plus facilement concevable que plusieurs responsables de traitements interviennent sciemment dans une chaîne de traitements non conformes, ou mettent simultanément en œuvre des traitements similaires à partir d'une même source de données corrompue, ce qui aurait pour effet d'engager la responsabilité pénale propre à chacun de ces organismes.

Ainsi, un tiers qui se serait vu destinataire de données personnelles de la part d'un premier responsable de traitement (par exemple cession d'une base de données prospects) dans le cadre d'un contrat « en bonne et due forme » pourrait ne pas être reconnu pénalement responsable de l'utilisation de ces données malgré leur origine frauduleuse, sauf s'il n'a pas fait preuve de diligence au moment de l'acquisition des données ou s'il

[10] Le fait de mettre en œuvre un traitement en toute bonne foi, mais en méconnaissance des dispositions de la loi pénale, constitue une intention de commettre le fait incriminé (voir par exemple Cass. Crim. 21 janvier 1997 : « *la méconnaissance, par des professionnels, d'une obligation positive de vérification imposée par la loi constitue l'élément intentionnel de l'infraction* »)

[11] Art. 50 de la loi Informatique et Libertés : « *les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du Code pénal*. »

[12] Art 121-7 du Code pénal : Art 121-7 du Code pénal : « *Est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation. Est également complice la personne qui par don, promesse, menace, ordre, abus d'autorité ou de pouvoir aura provoqué à une infraction ou donné des instructions pour la commettre* ».

[13] … et il est cette fois-ci possible d'affirmer qu'une « co-responsabilité » existe pour un seul et même traitement ! (entre la personne physique et la personne morale qu'elle représente)

[14] Ces exemples sont des suppositions, uniquement destinées à enrichir la réflexion, ils constituent des « cas d'école » n'ayant pour l'heure, à notre connaissance, jamais donné lieu à une réalisation quelconque.

pouvait avoir connaissance ou au moins subodorer que celles-ci avaient une origine frauduleuse au moment de la contractualisation.

L'AFCDP recommande aux responsables de traitements destinataires de données qu'ils n'auraient pas collectées directement auprès de la personne, de manière générale, de prendre toutes les précautions utiles au moment de la contractualisation :

- en s'informant de la notoriété de l'organisme à l'origine de la cession (pays d'origine, situation juridique, passé judiciaire, actualité…),
- en exigeant l'insertion dans le contrat de cession de clauses garantissant l'origine licite des données cédées, le respect par le cédant du consentement et de l'information des personnes concernées par le traitement etc.…, et qu'il soit à jour de toutes les formalités obligatoires qui lui incombent. Le cas échéant, lui demander de fournir les documents attestant de la bonne exécution de ces formalités[15].
- en effectuant une veille sociétale sur les prestataires et partenaires émetteurs ou destinataires de données afin de prendre toutes les mesures nécessaires en cas d'incident judiciaire les concernant, et relatif à la protection des données personnelles.

1.1.7 Cas de contestation de responsabilité (AIS2)

La délibération de la CNIL n°2010-113 en date du 22 avril 2010[16], qui condamna la société ACADOMIA à la suite d'un contrôle sur la société AIS2, mérite une attention toute particulière.

Cette société exploitait des fichiers dans lesquels figuraient de nombreux commentaires abusifs, qui ont donné lieu à l'adoption par la CNIL d'une sanction. AIS2 a alors contesté ces griefs en estimant n'être que l'exploitant d'un fichier, le responsable du traitement étant la société holding ACADOMIA GROUPE SAS.

La CNIL a retenu que la société AIS2 était responsable du traitement en se fondant sur les éléments suivants :

- les constats avaient été effectués dans les locaux d'AIS2,
- le président de la société AIS2 n'a jamais contesté que la société AIS2 était responsable des traitements litigieux, et a répondu à la CNIL sur les manquements constatés avec le timbre d'AIS2,
- les lettres adressées aux clients au nom d'ACADOMIA portent le timbre d'AIS2, de même que les fiches « Enseignants ».

En conclusion, la CNIL a estimé que la société AIS2 devait être responsable du traitement :

- parce qu'elle bénéficie d'un **véritable contrôle sur les bases de données exploitées et sur leur contenu,**
- parce qu'elle **détermine de manière autonome** la manière dont sont traitées les données qu'elle collecte.

Nous pouvons donc à ce stade de notre étude retenir deux critères permettant de déterminer le responsable de traitement, et découlant des questions suivantes :

- l'exercice d'un **véritable contrôle** sur les bases de données,
- **l'autonomie** dans la détermination du traitement des données.

[15] Il est également possible d'insérer ces clauses directement dans les appels d'offres qui pourraient être menés par les sociétés à la recherche de partenaires divers pour optimiser la prise en compte « à la source » de la conformité juridique des traitements.

[16] Délibération n°2010-113 du 22 avril 2010 de la formation restreinte portant avertissement à l'encontre de la société AIS 2 exerçant sous l'enseigne ACADOMIA

L'AFCDP rappelle que le fournisseur d'outils techniques nécessaires à la mise en œuvre d'un traitement n'est pas nécessairement responsable des données qui y sont stockées, cette responsabilité incombant à l'entité qui collecte les informations, de manière autonome et pour ses propres besoins.

Dans sa délibération, la CNIL précise que « *la société AIS2 détient la faculté, à tout le moins partielle, de déterminer les finalités et les moyens des traitements mis en cause* ». Ce complément laisse entrevoir la possibilité d'une mise en cause commune avec l'organisme qui codéciderait des finalités et des moyens avec AIS2, qui pourrait donc être considéré comme coresponsable du traitement en question.

1.2 Critères proposés pour retenir la coresponsabilité

À ce stade de notre analyse, et à la lumière des dispositions légales et des jurisprudences récentes, nous pouvons concevoir qu'**une personne est considérée comme responsable de traitement dans une chaîne de traitements selon les critères suivants** :

- principe de **liberté** : celle-ci se manifeste au moment de l'évaluation de l'opportunité de créer le traitement. Ne peut être responsable que celui qui choisit librement de créer, de modifier, ou de supprimer un traitement. Cette liberté doit cependant être considérée de manière relative ; ainsi, les contraintes environnementales et réglementaires n'altèrent en aucune façon ce principe (ces contraintes peuvent en effet aussi bien être la cause que la conséquence de la mise en œuvre du traitement).

- principe **d'autonomie** dans la détermination des modalités de mise en œuvre opérationnelle et de contrôle du traitement : il s'agit à ce niveau de définir de quelle manière sera mis en œuvre le traitement. En choisissant de déléguer de manière globale les opérations requises par le traitement à un prestataire, le responsable du traitement choisit de manière originelle et macroscopique le moyen de le mettre en œuvre. Le recours par un prestataire à un autre sous-traitant constitue une possibilité reconnue par le responsable du traitement initial, et ne crée donc pas, *a priori*, de nouvelle responsabilité sur le prestataire au sens de la loi Informatique et Libertés.

  À la lecture du guide établi par la CNIL relatif aux transferts de données vers des pays extérieurs à l'UE[17], les concepts de liberté et d'autonomie se fondent : « *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 ».* Dans notre analyse, nous pensons qu'il peut être pertinent de distinguer la décision de créer le traitement de celle de déterminer ses modalités de mise en œuvre.

- principe d'**égalité** dans l'application des deux principes précédents. Cette égalité est relative, et revient simplement à vérifier s'il existe une situation d'interdépendance entre les responsables de traitement présumés.

Ainsi, une personne qui ne serait pas initialement désignée comme responsable de traitement le deviendrait de fait parce qu'elle influe de manière déterminante sur l'opportunité de créer et **est compétente** pour décider, avec le responsable du traitement identifié, de modifier ou de supprimer le traitement, ou parce qu'elle participe à la détermination des moyens nécessaires à sa mise en œuvre (la notion de « compétence » revient par ailleurs dans la convention 108[18]).

[17] Guide CNIL "*Transferts de données à caractère personnel vers des pays tiers à l'Union Européenne*", 2010

[18] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de Strasbourg en date du 28 janvier 1981, dite "Convention 108"

1.3 « Cotraitements » et « interconnexions »

La loi Informatique et Libertés ne définit pas de manière précise les « interconnexions » de fichiers dont la mise en œuvre est subordonnée à une autorisation de la part de la CNIL. Les seuls traitements visés par la loi[19] sont ainsi ceux qui ont pour **objet** :

- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents;
- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes.

Les organismes issus du secteur de l'assurance relèvent du second dispositif, lequel reste toutefois sujet à interprétation :

Qu'est-ce qu'une « *interconnexion* » au sens littéral du terme ?

Selon la CNIL[20], il s'agit d'une modalité technique de rapprochement de fichiers par « *corrélation*[21] » des données. Cela signifie deux choses : premièrement, qu'à partir du moment où existe une liaison entre des données relevant de fichiers habituellement gérés distinctement, l'interconnexion est caractérisée, et deuxièmement, que le « contenant » des données, s'il est commun, ne constitue pas pour autant une interconnexion s'il n'y a pas de corrélation de données (par exemple, une seule et même base de données gérant des fichiers distincts, et appelée par une seule et unique application proposant des profils différents aux utilisateurs afin de restreindre leurs droits d'accès ne constitue pas, *a priori*, une interconnexion de fichiers puisque ceux-ci ne sont pas liés techniquement).

Qu'est-ce qu'un fichier « *relevant d'autres personnes* » ?

Il s'agit à première lecture de fichiers mis en œuvre dans le cadre de traitements relevant de la responsabilité de personnes physiques ou morales distinctes. La lecture de cette disposition au sens strict ne nous permet pas de distinguer un régime spécifique pour les sociétés relevant d'un même groupe. Toutefois, il convient de considérer de manière raisonnable que la loi vise les personnes dotées de la personnalité juridique. Ainsi seraient exclusivement concernées les personnes morales de droit public ou privé et non une direction ou un service au sein d'un même organisme. Une interprétation plus large de cet article conduirait d'ailleurs à une augmentation considérable des demandes d'autorisations auprès de la CNIL pour des fichiers ne présentant pas nécessairement de sensibilité particulière.

Dans quelle mesure les finalités « *principales* » de fichiers sont-elles différentes ?

Il conviendrait selon nous de revenir à la finalité « macroscopique » du traitement afin d'en déterminer le caractère « principal », et d'évaluer le degré de sensibilité des traitements en cause[22]. Ainsi, nous pensons que la mise en commun de plusieurs fichiers commerciaux à des fins de prospection marketing ou de gestion sont susceptibles d'être considérés comme relevant d'une finalité principale identique (« gestion administrative et commerciale », « gestion client », « fichier prospect… »), quand bien même les cibles et produits concernés seraient différents[23].

---

[19] Art. 25 5° de la loi n°78-17 du 6 janvier 1978

[20] Voir sur http://www.cnil.fr/, mots-clés « premières décisions de la CNIL en matière d'autorisations »

[21] La CNIL ne donne toutefois pas de définition au terme « corrélation », que l'on peut toutefois comprendre comme la dépendance réciproque entre plusieurs fichiers, nécessaire à la poursuite de l'intérêt des responsables de traitements qui y recourent

[22] Rappelons à ce titre qu'au cours de la séance du 1er avril 2003 (lors de l'étude de propositions d'amendements débattus au Sénat, préalablement à l'adoption de la loi Informatique et Libertés), un amendement visant à « *supprimer l'exigence d'une autorisation préalable lorsque l'interconnexion est faite à des fins seulement commerciales et que la personne a donné son accord* » avait été déposé et approuvé par la CNIL

[23] La centralisation de l'identité des clients relevant d'une mutuelle, d'un organisme prêteur, ou encore d'un assureur auto peuvent ainsi être mutualisés (dans le cadre d'un accord de cession régulièrement encadrée et avec l'accord éclairé des personnes concernées) sans pour autant relever du champ de l'article 25 5° de la loi Informatique et Libertés, même s'il s'agit de fichier relevant de personnes différentes, et cela parce que la finalité principale des fichiers ainsi partagés est identique (« identification des clients »)

Ces critères sont-ils alternatifs ou cumulatifs ?

L'AFCDP estime que deux fichiers doivent impérativement relever de deux personnes morales distinctes ET posséder des finalités principales différentes pour qu'une interconnexion soit caractérisée au sens de la loi.

Les cotraitements doivent donc toujours être considérés avec méthode et rigueur pour déterminer si un régime d'autorisation préalable leur est ou non applicable.

Il est bien entendu fortement recommandé de contacter la CNIL avant toute mise en œuvre de projet susceptible d'aboutir à une interconnexion au sens légal du terme, afin de déterminer avec elle si le traitement en question relève ou non du régime de l'autorisation préalable.

1.4 Gestion des cotraitements par des conventions *ad hoc*

Lorsqu'il n'apparaît pas clairement que l'une des parties en présence est un sous-traitant de l'autre ou un responsable de traitement distinct, il est nécessaire d'adopter un dispositif contractuel explicitant clairement les responsabilités des uns et des autres.

Cette solution revient régulièrement dans les analyses menées par des organismes publics confrontés à une telle situation. Dans son guide « Informatique et Libertés » pour l'enseignement et la recherche[24], la Conférence des Présidents d'Université (en partenariat avec la CNIL) a ainsi constaté que « *les responsables du traitement sont d'une part l'université et d'autre part l'organisme de recherche puisque les deux assument la tutelle de l'unité. Cependant afin d'assurer la cohérence des politiques menées, il leur reviendra de définir dans les conventions qui les lient celui d'entre eux qui aura à s'assurer de la bonne application des dispositions "Informatique et Libertés" et donc à remplir le rôle de responsable pilote de traitement, unité par unité*[25]. »

La voie contractuelle a également été recommandée par la CNIL à l'occasion de son rapport d'étape sur l'application de la loi Informatique et Libertés par les communes[26]. La CNIL constatait en effet que la détermination du responsable de traitement était parfois confuse lorsque les communes et les établissements publics de coopération intercommunale (EPCI) disposaient d'un service informatique commun et centralisé.

Dans ce cas d'espèce, la CNIL recommande de vérifier :

- si l'établissement intervient seulement comme **prestataire technique** de la commune, auquel cas celle-ci demeure responsable du traitement et l'EPCI est assimilé à un sous-traitant de la commune,
- si l'EPCI, dans le cadre d'un **transfert de compétences**, s'est vu confier la gestion administrative du service des traitements de la commune, alors c'est l'EPCI qui sera responsable du traitement concerné.

La CNIL conclut cette analyse en précisant que « *les statuts de l'EPCI doivent explicitement prévoir que les transferts de compétences entraînant transferts de fichiers nominatifs conduisent à transmettre à cet établissement public la responsabilité de ces fichiers et notamment à effectuer les déclarations nécessaires auprès de la CNIL* ».

[24] Guide "Informatique et Libertés" pour l'enseignement supérieur et la recherche, Édition 2009, réalisé sous l'égide de la Conférence des Présidents d'Université, de l'Agence de Mutualisation des Universités et Établissements, et de la CNIL.

[25] En l'espèce, les Unités de Recherche concernées appartenaient pour moitié à chacune des deux entités

[26] Rapport d'étape sur l'application de la loi "Informatique et Libertés" par les communes, présenté en séance plénière le 9 décembre 2003 par Monsieur Pierre Leclercq, rapporteur, à partir d'un bilan de missions de contrôle effectuées en 2003

L'AFCDP recommande que tout contrat liant deux entités amenées à manipuler des fichiers détermine clairement les rôles et les responsabilités de chacun au regard de la loi Informatique et Libertés.

Ce contrat doit au minimum préciser :

- les rôles et responsabilités de chaque partie sur les données traitées,
- le rappel des obligations relatives aux formalités préalables issues de la loi Informatique et Libertés,

Si l'une des parties est le sous-traitant de l'autre, alors le contrat doit également comporter :

- un rappel des obligations de sécurité et d'action sur instruction (clauses légales),
- une clause d'information du responsable du traitement si le sous-traitant souhaite faire appel à des prestataires,
- une clause de demande d'autorisation du responsable du traitement si les données sont transmises par le sous-traitant à un prestataire ou une filiale basée à l'étranger, hors Union européenne,
- une clause définissant une procédure pour le traitement des demandes des personnes (droit d'accès, de rectification et d'opposition),
- une clause d'audit du sous-traitant (décrivant les actifs auditables),
- une clause de notification obligatoire des incidents de sécurité au responsable du traitement.

À noter qu'il peut être déduit de l'avis du G29, sur les notions de « responsable du traitement et de « sous-traitant » que ni les juges ni la CNIL ne seront tenus par les règles d'attribution des responsabilités telles qu'exposées dans le contrat, « *même si la désignation d'une entité en tant que responsable du traitement ou sous-traitant des données dans un contrat pouvait révéler des informations intéressantes sur le statut juridique de l'entité, cette désignation contractuelle ne permet cependant pas de déterminer avec certitude son véritable statut, qui doit être déduit de circonstances concrètes*. »

Ainsi, la détermination des responsabilités dans le contrat doit correspondre à une réalité factuelle, et les clauses qui en découlent clarifier une situation confuse. Le contrat ne saurait donc en tout état de cause permettre au responsable effectif du traitement de se décharger de sa responsabilité sur un prestataire.

En cas de confusion au niveau de la responsabilité des différents acteurs d'une chaîne de traitement (ou en cas de mise en œuvre simultanée de traitements identiques à l'issue d'une collecte unique de données), il est nécessaire de prendre le recul nécessaire pour évaluer de manière logique, pertinente et cohérente l'étendue des responsabilités de chacun. L'approche « client » pourrait faciliter cette démarche (du point de vue du client, quel est le responsable de traitement le plus vraisemblable ?)

1.5 De la sous-traitance « de droit » à la responsabilité « de fait » ?

L'une des problématiques les plus difficiles à appréhender pour un responsable de traitement est de savoir si les données qu'il transmet à une entité tierce sont en fait cédées dans une perspective bien définie, et donc dans le cadre d'un contrat de partenariat juridiquement encadré par des conventions en bonne et due forme, ou bien simplement communiquées dans un contexte de sous-traitance dans le cadre de laquelle le prestataire de services n'aurait qu'une marge de manœuvre très faible. Les critères énoncés ci-dessus peuvent permettre, selon l'autonomie accordée au tiers, une première esquisse dans la définition des responsabilités de chacun, et donc dans la détermination d'une responsabilité de fait dans le traitement de données personnelles mis en œuvre.

Dans un document publié le 11 octobre 2010 en matière d'externalisation de traitements[27], la CNIL propose une méthodologie très intéressante susceptible de définir le niveau de responsabilité entre un responsable de traitement et un tiers destinataire de données, et suggère même la qualification de « responsable de traitement » autonome pour une personne qui, en temps normal, devrait pourtant être considérée comme simple sous-traitant.

Ces critères sont les suivants :

- le **niveau d'instruction** donné par le client témoignerait de l'autonomie donnée par le responsable de traitement à son sous-traitant. Dans ce contexte, un contrat dont les termes resteraient très généraux placerait le prestataire dans une situation d'autonomie significative, lui conférant le statut de responsable de traitement à part entière.
- le **niveau de contrôle** sur le prestataire serait également un bon indicateur pour déterminer la marge de manœuvre dont dispose le prestataire pour traiter les données. Une réelle liberté dans cette mise en œuvre révèlerait là encore une situation de responsabilité pleine et entière.
- le **degré de transparence** impliquerait en fait de conférer la responsabilité du traitement à l'interlocuteur que la personne dont les données sont traitées pourrait, à juste titre, considérer comme son responsable de traitement. Lorsque le prestataire agissant pour le compte de client responsable de traitement se présente sous le nom de celui-ci, alors la personne physique n'a pas connaissance de l'identité de ce prestataire, qui fait partie d'un « tout » avec le responsable de traitement. Sa qualité en est indissociable, ce qui ne serait pas le cas d'un sous-traitant qui agit clairement en son nom propre, identifiable comme un interlocuteur distinct du responsable du traitement.
- le **degré d'expertise** du prestataire, qui ne laisserait aucune marge de manœuvre à son client et utiliserait ses propres moyens techniques, donnerait enfin un indice sur la marge d'autonomie dont il dispose et sur son potentiel de responsabilisation vis-à-vis des personnes dont les données sont traitées.

Le cumul de ces critères pourrait permettre la (re)qualification du sous-traitant en responsable de traitement autonome. Ils ne constituent à l'heure actuelle qu'un ensemble d'indicateurs envisagés par la CNIL, ils sont pourtant une réalité quotidienne pour les responsables de traitements, et commencent à prendre une place significative dans les contrats de prestation de service.

1.6 Cotraitement et coresponsabilité

Il convient de préciser que l'existence d'un cotraitement, qu'il s'agisse de l'intervention simultanée sur un seul et même fichier de plusieurs responsables de traitements, ou de la mise en œuvre d'opérations successives par ceux-ci dans le cadre d'une chaîne de traitements, n'emporte pas systématiquement responsabilité pour chacun des différents acteurs concernés.

Pour chaque traitement en question, il sera nécessaire de constater si une seule entité détermine de manière libre et autonome les finalités et les moyens du traitement. Ainsi, un responsable de traitement ne sera pas coresponsable de la mise en œuvre des parties du traitement pour lesquelles il n'aura pas exercé une influence significative et libre.

[27] « *Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques* », CNIL, oct. 2010

2. Détermination des responsabilités : transposition opérationnelle

L'objet de cette rubrique est de recenser différents cas auxquels les membres du groupe de travail ont été confrontés et ne sont pas exhaustifs. Certains domaines, situés en-dehors des métiers de l'assurance, ont par ailleurs également été retenus pour permettre de mieux appréhender ces problématiques.

Dans chacun de ces cas, la logique est de déterminer si nous sommes en présence :

- d'un responsable de traitement et de son sous-traitant (au sens de la loi)
- de deux responsables de deux traitements distincts
- de deux responsables d'un même traitement (cotraitement avec coresponsabilité éventuelle)

2.1 Recours aux groupements de moyens (de type GIE)

2.1.1 Contexte. Les groupements de moyens centralisent les moyens informatiques et/ou humains de l'ensemble des membres qui y adhèrent. À ce titre, les membres de ces groupements peuvent ne disposer ni de personnel, ni de moyens techniques propres. De cette manière, le groupement, qui n'a initialement qu'une fonction de sous-traitant, se voit confier l'intégralité de la mise en œuvre des traitements nécessaires à l'activité de ses membres. Dans ce contexte, il peut exister une confusion au niveau de la responsabilité incombant à l'organisme membre du groupement et la direction « MOA » de celui-ci décidant pour le compte de ces membres.

2.1.2 Responsabilités. L'autonomie dans la mise en œuvre des traitements par les groupements de moyens se limite à certains aspects techniques et organisationnels (choix d'un prestataire, détermination des ressources nécessaires, planification du projet…) mais est en réalité subordonnée aux décisions des conseils d'administration de ses membres. Ainsi, le recours à un tel groupement constitue en tant que tel une première démarche de la part d'un responsable de traitement pour déterminer les finalités et les moyens d'un ensemble de traitements.

Recommandations de l'AFCDP

- Les conventions conclues entre le groupement de moyens et le membre adhérent doivent indiquer clairement que le groupement agit en tant que sous-traitant pour le compte de ce membre. Ces mentions peuvent figurer directement dans les statuts du groupement, ou dans des conventions spéciales annexes.
- Chaque membre du groupement reste seul responsable des traitements dont la mise en œuvre lui a été déléguée et s'engage, à ce titre, à respecter les dispositions de la loi Informatique et Libertés et notamment l'accomplissement des formalités préalables.
- L'AFCDP invite également les entreprises à sensibiliser leurs personnels agissant en tant que « maîtrise d'ouvrage » aux obligations découlant de la loi Informatique et Libertés, afin que ceux-ci prennent conscience de leur statut de « responsables de traitements » et rappellent systématiquement aux personnels agissant en tant que « maîtrise d'œuvre » les principes fondamentaux inhérents à la protection des données à caractère personnel.

2.2 Traitements impulsés par une holding et mis en œuvre par ses filiales

2.2.1 Contexte. La logique se rapproche de celle des GIE lorsque les outils informatiques sont imposés par une société de type « tête de groupe » ou « holding » à ses filiales. Dans ce cas, la détermination du besoin

de créer le traitement et de ses modalités de mise en œuvre est bien prise par la filiale, celle-ci ayant lieu dans le cadre d'un processus décisionnel largement influencé par la holding, mais qui lui reste propre.

2.2.2 Responsabilités. Les traitements mis en œuvre par la filiale relèvent de sa responsabilité exclusive, même si la holding intervient ensuite dans le schéma d'exécution des traitements, par exemple en imposant à la filiale l'hébergement des applications nécessaires et des données traitées sur ses propres serveurs.

Recommandations de l'AFCDP

- Il convient de formaliser par écrit les rôles et responsabilités des différentes sociétés.
- Les conventions conclues entre la holding et sa filiale doivent indiquer clairement que la holding n'est pas responsable des traitements mis en œuvre par sa filiale, même si elle lui impose les moyens techniques nécessaires à leur réalisation.
- La holding peut exiger contractuellement de ses filiales qu'elles s'engagent à respecter les dispositions issues de la loi Informatique et Libertés et notamment l'accomplissement des formalités préalables.

NB : Ces recommandations n'ont pas vocation à s'appliquer aux « succursales » qui, simples extensions géographiques et commerciales de la société mère, n'endossent a priori pas la responsabilité des traitements qu'elles mettent en œuvre sur instruction de cette dernière (application des règles de la sous-traitance).

2.3 Demande et autorisation de prélèvement

2.3.1 Contexte. Lorsqu'un assureur propose à son client de verser ses cotisations par voie de prélèvement bancaire, celui-ci, qui devrait adresser cette demande directement à sa banque, peut, dans la pratique, la communiquer à l'assureur. Un seul et même support de collecte d'informations est ainsi destiné à deux responsables de traitement : l'assureur et la banque.

2.3.2 Responsabilités. Il faut distinguer deux étapes :

- la demande de prélèvement est un document adressé à l'assureur et par lequel le client va communiquer ses coordonnées bancaires en vue d'un paiement des services auxquels il a souscrit. Dans ce cadre, de nouvelles données sont collectées par l'assureur pour une finalité et selon une durée qui lui sont propres. Il s'agit d'un nouveau traitement dont la personne doit par conséquent être informée ;
- l'autorisation de prélèvement est un document destiné à la banque du client, et par lequel celui-ci va confirmer à sa banque que l'assureur est bien autorisé à prélever son compte bancaire. Ce traitement, qui s'inscrit dans le fonctionnement habituel d'un compte bancaire, relève de la responsabilité exclusive de la banque. L'information du détenteur du compte a, en principe, été assurée dans la convention de compte signée lors de l'ouverture de son compte.

Recommandations de l'AFCDP

- veiller à la cohérence des mentions légales utilisées ainsi qu'à leur mise à jour
- anticiper les erreurs d'adressage de la part des clients par des procédures adéquates (par exemple, utilisation de l'adresse relative à l'exercice du droit d'accès pour envoyer son autorisation de prélèvement)

2.4 Coassurance

2.4.1 Contexte. Des coassureurs interviennent via un même contrat. Ils portent ensemble le risque et partagent les informations relatives au souscripteur et à ses bénéficiaires.

2.4.2 Responsabilités. Chaque assureur est une personne morale indépendante qui met en œuvre en toute autonomie l'ensemble de ses traitements, dont celui relatif à la gestion de contrats et de sinistres en coassurance, dont elle assume la responsabilité.

Recommandations de l'AFCDP

- Bien préciser les rôles de l'apériteur et des coassureurs dans les conventions de coassurance ;
- S'assurer que les formalités préalables sont bien accomplies par chaque coassureur, en qualité de responsable de traitement ;
- Déterminer dans la convention de coassurance si les droits d'accès, d'interrogation, de rectification et d'opposition s'exercent auprès de l'apériteur (en cas de délégation de gestion) ou auprès de chaque coassureur pour les données qu'il traite ;
- Assurer une information claire de l'assuré sur l'identité des responsables de traitement (les coassureurs), les destinataires des données ainsi que les modalités d'exercice des droits Informatique et Libertés.

2.5 Gestion des contrats d'assurance collectifs obligatoires

2.5.1 Contexte. L'employeur fait appel à un organisme compétent pour gérer les prestations sociales dues aux salariés (notamment retraite, santé et prévoyance complémentaires). Il est à ce titre amené à transmettre des données à caractère personnel de ses salariés à l'organisme concerné afin de répondre à ses obligations légales. Ensuite, ces mêmes données peuvent être retransmises aux organismes sociaux et fiscaux (destinataires d'informations relatives au patrimoine, à la santé, à la vie familiale ainsi que du numéro de sécurité sociale).

2.5.2 Responsabilités. Nous avons tenté de distinguer dans le tableau suivant les responsabilités des différents acteurs intervenant successivement dans la mise en œuvre des « cotraitements » découlant de contrats d'assurance collectifs obligatoires.

		Employeur	Assureur	État
Traitement	Retraite	Responsabilité au niveau des opérations résultant de dispositions légales, de conventions collectives ou de stipulations contractuelles concernant les déclarations à l'administration fiscale et aux organismes de protection sociale, de retraite et de prévoyance. (*Traitements exonérés de déclaration, voir dispense n°2*[28])	Délicate appréhension du statut de l'institution de retraite complémentaire (IRC), dont l'activité est organisée, encadrée réglementairement et contrôlée par les Fédérations AGIRC-ARRCO. Néanmoins, il ne faut pas assimiler les directives émanant de cet organisme à des "instructions" de l'ordre de celles qui peuvent être données à un sous-traitant, mais à des dispositions réglementaires qui régissent l'activité de l'IRC qui, en sa qualité de responsable de traitement, sera amenée à traiter des informations selon une finalité spécifique (permettre aux adhérents de faire bénéficier leurs salariés du régime de retraite complémentaire par répartition). Bien que disposant d'une marge de manœuvre réduite, les IRC disposent d'une autonomie réelle qui leur confère la qualité de responsables de traitements à part entière. Les échanges entre les IRC, par exemple au moment de la reconstitution de la carrière, constituent dès lors nécessairement des cessions de données entre responsables de traitements, soumises aux obligations légales habituelles.	L'administration fiscale ainsi que les fédérations AGIRC-ARRCO sont également responsables, de manière indépendante, des traitements qu'elles mettent en œuvre à partir des données qui leur sont adressées par les institutions de retraite complémentaire. Elles ne reçoivent en effet aucune "instruction" de la part d'un autre organisme, et sont responsables de traitements répondant à des missions distinctes de celles des institutions de retraite complémentaire.
	Santé		Responsabilité des mutuelles, sociétés d'assurance et institutions de Prévoyance sur les données des salariés et de leurs ayants-droits, car autonomie dans la mise en œuvre des traitements (souscription directe et individuelle des personnes pour la partie Santé, indirecte pour la partie Prévoyance, avec toutefois une relation directe avec l'IP dès survenance du premier sinistre). Cette responsabilité vaut aussi pour les données émanant des CPAM et qui sont nécessaires au calcul de la part complémentaire. Coexistent bien deux traitements distincts et interdépendants mis en œuvre par deux responsables de traitement différents, mais portant sur les données d'une même personne. Les flux NOEMIE s'apparenteraient ainsi à des cessions de données selon une finalité déterminée.	Responsabilité des caisses d'assurance maladie sur les données des salariés et de leurs ayants-droits car autonomie dans la mise en œuvre des traitements (souscription directe et individuelle des personnes, adhésion distincte du régime complémentaire). La transmission d'informations dans le cadre de flux NOEMIE devrait être assimilée à une cession d'informations pour les besoins propres de l'assureur.
	Prévoyance			
	Action sociale	Si l'employeur décide par lui-même de mettre directement en œuvre une action sociale au profit de ses salariés, celle-ci sera indépendante de celle qui est proposée par l'organisme d'assurance (*ce type de traitement tendrait alors à relever de la norme RH n°46*). Idem si l'action sociale est mise en œuvre pas le Comité d'entreprise (*voir en ce sens la dispense de déclaration n°10 sur les traitements mis en œuvre par les CE*[29]).	Responsabilité unique de l'assureur qui décide de manière autonome de l'affectation des fonds dans le cadre de la réglementation régissant l'action sociale.	Sans objet

[28] Dispense n°2 - Délibération n°2004-097 du 9 décembre 2004 décidant la dispense de déclaration des traitements de gestion des rémunérations mis en œuvre par les personnes morales de droit privé autres que celles gérant un service public

[29] Dispense n°10 - Délibération n°2006-230 du 17 octobre 2006 dispensant de déclaration les traitements mis en œuvre par les comités d'entreprises ou d'établissements, les comités centraux d'entreprises, les comités de groupe ou les comités interentreprises ou les délégués du personnel pour la gestion de leurs activités sociales et culturelles

Recommandations de l'AFCDP

La multiplication des organismes en charge de la protection sociale est susceptible d'engendrer une confusion dans l'esprit de la personne dont les données sont traitées. Ainsi, il faut encourager la transparence dans la mise en œuvre de traitements successifs par une information pédagogique détaillant spécifiquement les catégories de destinataires de données et leur degré de responsabilité dans la chaîne de traitements.

De la même manière, il incombera à chacune de ces structures de veiller à être à jour de ses déclarations CNIL (ou du registre du CIL désigné), en déterminant avec précision les traitements qui relèvent effectivement de sa responsabilité.

2.6 Gestion des contrats d'épargne retraite

2.6.1 Contexte. L'épargne retraite individuelle (PERE) et collective (Article 83) sont des contrats d'assurance de groupe qui nécessitent la conclusion par l'employeur d'un contrat avec un partenaire financier. Il peut y avoir une confusion dans la détermination des responsabilités entre ces deux acteurs.

2.6.2 Responsabilités. Chaque entité est en fait seule responsable de deux traitements distincts :

- la *mise en œuvre d'une épargne retraite et salariale au profit des salariés* constitue un premier traitement dont les finalités se limitent à la conclusion d'un contrat entre l'employeur et un organisme assureur qui implique la cession préalable d'un fichier du personnel concerné par le contrat collectif au partenaire financier, dans un objectif déterminé ;
- la *gestion des contrats d'assurance collective d'épargne retraite et salariale*, incombe quant à elle à l'assureur (gestion des demandes d'adhésion des entreprises, adhésion et tenue des comptes individuels des épargnants, établissement de relevés de comptes et d'informations…).

Recommandations de l'AFCDP

- L'employeur doit informer ses salariés de l'existence d'un contrat collectif d'épargne souscrit auprès d'un partenaire financier, et de la transmission des données personnelles les concernant à celui-ci, préalable nécessaire à l'ouverture de leur compte individuel ;
- Il est souhaitable de proposer une mention d'information faisant apparaître un interlocuteur unique pour l'exercice des droits issus de la loi Informatique et Libertés ;
- Il convient de définir une procédure d'information réciproque en cas de réclamation « Informatique et Libertés » d'un salarié susceptible d'avoir un impact sur les traitements de l'autre partie (voir modèle en annexe) ;
- Il est utile de préciser aux salariés que le partenaire financier peut-être amené à les contacter directement pour la gestion de leur compte (versements, rachats, clôture) ;
- Il importe pour chaque société de veiller à être à jour de ses déclarations CNIL pour les traitements qui la concernent, sachant que la norme simplifiée n°46[30] relative à la gestion du personnel n'inclut pas cette finalité.

[30] Délibération n°2005-002 du 13 janvier 2005 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels

2.7 Intermédiation

2.7.1 Contexte. Les sociétés d'assurance recourent de manière significative aux professionnels de l'intermédiation pour diffuser leurs produits d'assurance. Ces intermédiaires, peuvent être courtiers d'assurance, agents généraux, mandataires d'assurance ou mandataires d'intermédiaires d'assurance. Les courtiers sont indépendants et ont une clientèle propre, qui va devenir également la clientèle de l'assureur. Les autres intervenants sont des mandataires qui interviennent au nom et pour le compte de l'assureur ou d'un autre intermédiaire, et n'ont ainsi pas de clientèle propre.
Par ailleurs, ces intermédiaires peuvent se voir déléguer par l'assureur tout ou partie de la gestion des contrats ainsi souscrits, et en particulier la gestion des primes et des sinistres.

2.7.2 Responsabilités. Dans le cadre du processus de souscription, l'intermédiaire courtier intervient auprès de différents assureurs afin d'obtenir des propositions de contrats. Il met ainsi en œuvre, en toute indépendance, un traitement dans le cadre duquel il est amené à adresser à des assureurs les données qu'il a collectées auprès de ses clients. Le courtier est le responsable de ce traitement, étant le seul à en définir les moyens et les objectifs.

Après la souscription du contrat, si le courtier bénéficie d'une délégation de gestion, il va collecter et traiter des données au nom et pour le compte de l'assureur, aux fins par exemple de gérer les sinistres. Ce traitement sera réalisé selon les critères et la finalité définis par l'assureur, et relève donc de sa responsabilité, le courtier n'étant ici qu'un sous-traitant. Toutefois, si la délégation ne précise pas clairement les données à traiter ainsi que les modalités du traitement, et que le courtier se retrouve donc à en définir au moins les moyens de mise en œuvre, il pourra alors être considéré comme responsable du traitement.

En ce qui concerne les agents généraux et les mandataires d'assurance, dans le cadre du processus de souscription, ceux-ci vont collecter et enregistrer des données, sauf exception, directement dans la base de l'assureur qui leur a donné mandat de distribuer ses produits. Le responsable du traitement sera donc ici l'assureur qui aura déterminé tant la finalité que les moyens. Il en ira de même pour la partie délégation de gestion des contrats. Toutefois, si le mandataire est amené à traiter des données différentes ou selon d'autres modalités que celles requises par l'assureur, et ainsi à établir son propre fichier, il sera alors responsable du traitement qu'il aura mis en œuvre.

Enfin, pour ce qui est des mandataires d'intermédiaires d'assurance, dans le cadre du processus de souscription, ceux-ci se trouvent dans la même situation que les mandataires ci-dessus, à ceci près qu'ils interviennent au nom et pour le compte d'un autre intermédiaire, qui lui-même peut être aussi un mandataire.

Recommandations de l'AFCDP

- Bien préciser dans les délégations de gestion entre assureurs et intermédiaires, qui de l'assureur ou de l'intermédiaire détermine le type de données à traiter, ainsi que les modalités de leur traitement (destinataires, durées de conservation …), la finalité du traitement et à qui incombe l'information de l'assuré.
- Bien préciser dans les mandats de distribution et de souscription, qui détermine les données à traiter ainsi que les moyens de mise en œuvre, la finalité du traitement et à qui incombe l'information de l'assuré.
- Bien préciser dans les mandats de distribution et de souscription les conditions et conséquences d'un éventuel sous mandat.
- Assurer une information claire de l'assuré sur l'identité des responsables des différents traitements (assureur et/ou intermédiaire), les destinataires des données ainsi que les modalités d'exercice des droits Informatique et Libertés.

2.8 Réassurance

2.8.1 Contexte. La réassurance consiste, pour une compagnie d'assurance, à faire assurer une partie de ses propres risques par une compagnie de réassurance. Cette dernière se voit à ce titre communiquer par l'assureur des informations à caractère personnel et peut devenir, à cette occasion, responsable de traitements, notamment pour la tarification médicale ou la gestion de sinistres corporels.

Pour certains risques importants, des informations peuvent à leur tour devoir être partagées par les réassureurs avec des rétrocessionnaires (assureurs des réassureurs). La logique est alors la même que lors de la collecte de données par le réassureur auprès de l'assureur.

2.8.2 Responsabilités. Plusieurs acteurs interviennent successivement dans le cadre de traitements dont l'interdépendance ne doit cependant pas occulter les finalités distinctes :

- l'assureur, auprès duquel s'effectue la souscription, est responsable envers son client de l'utilisation qui est faite de ses données de la collecte jusqu'à la transmission à son réassureur, et cela dans le cadre d'un traitement de type « *passation, gestion et exécution des contrats d'assurance* » ;
- le réassureur, qui collecte les données auprès de l'assureur, devient responsable, de manière totalement indépendante, des données traitées dans le cadre d'un traitement relatif à la « *gestion des traités de réassurance* » ;
- il en va de même pour les rétrocessionnaires qui deviennent à leur tour entièrement responsables des données qui leur sont transférées à des fins de réassurance.

NB : la norme simplifiée n°16 découlant de la délibération n°81-004 du 20 janvier 1981 prévoit les échanges de données entre assureurs et réassureurs. Elle n'a toutefois pas prévu de manière spécifique la répartition des responsabilités entre assureurs et réassureurs, et est même de nature à complexifier l'identification puisqu'elle englobe sans les distinguer ces deux types de traitements : si l'assureur et le réassureur effectuent une déclaration de leurs traitements sur la seule base de la norme 16, alors même qu'ils traitent des données personnelles concernant les mêmes clients, il peut y avoir une confusion dans la répartition des responsabilités de chacun. La voie conventionnelle devient alors le meilleur moyen de clarifier celles-ci.

Recommandations de l'AFCDP

- Bien préciser les rôles de l'assureur et du réassureur dans les traités de réassurance ;
- S'assurer que les formalités préalables sont bien accomplies par chaque assureur, en qualité de responsable de traitement
- Assurer une information claire de l'assuré sur les destinataires des données, parmi lesquels les réassureurs.
- Assureur et réassureurs doivent convenir d'un mode opératoire destiné à répercuter les demandes d'accès et de suppression éventuellement formulées par les clients du premier afin que le second puisse bien prendre en considération la demande.
- Les traités de réassurance devraient faire état d'une procédure d'information mutuelle en cas de fuite de données ou d'atteinte à leur intégrité.

2.9 Assistance

2.9.1 Contexte. L'assistance est une prestation complémentaire incluse dans le contrat d'assurance par laquelle l'assisteur va venir en aide physiquement ou matériellement à l'assuré en fournissant des prestations d'assistance (dépannage, remorquage, rapatriement sanitaire …).

L'assisteur reçoit de l'assureur un certain nombre d'informations qui lui permettent de vérifier que la personne est bien assurée. Souvent, des flux retours indiquent à l'assureur que l'assuré a bénéficié d'une prestation d'assistance.

2.9.2 Responsabilités. L'essentiel de l'activité d'assistance est sous la responsabilité de l'assisteur qui est responsable de traitement. En effet, l'assisteur dispose d'un système d'information propre, d'une autonomie dans l'organisation de son traitement et collecte de nouvelles informations liées à la finalité de gestion des sinistres. Ainsi, les données médicales recueillies au moment d'un rapatriement sanitaire sont couvertes par le secret médical et ne pourront pas être retransmises à l'assureur.

De même, l'assisteur est responsable de son système d'information et doit prendre les mesures de sécurité adaptées. L'assisteur est donc autonome dans la mise en œuvre du traitement de gestion des sinistres. Par exception, l'assisteur sera sous-traitant et l'assureur responsable de traitement lorsque ce dernier donne des directives très précises ou impose à l'assisteur la mise en œuvre de traitements spécifiques pour son compte. Ainsi, si l'assureur souhaite faire des enquêtes de satisfaction sur l'assistance auprès de ses clients et sollicite l'assisteur, celui-ci intervient alors comme sous-traitant.

Recommandations de l'AFCDP

- La mention Informatique et Libertés de l'assureur précise que l'assisteur est destinataire de certaines données ;
- L'assisteur déclare son activité de gestion des sinistres en précisant que l'assureur est destinataire de certaines informations d'assistance ;
- Un contrat est signé entre l'assureur et l'assisteur et précise que l'assureur est responsable de traitement pour les données qu'il transmet à l'assisteur et que l'assisteur est responsable de traitement pour les données d'assistance saisies au cours de la prestation d'assistance ainsi que pour les données qu'il retransmet à l'assureur ;
- Les documents contractuels (conditions générales du contrat d'assurance) précisent l'identité de l'assisteur ;
- Sauf accord exprès de l'assuré, l'assisteur ne doit pas transmettre à l'assureur des informations récoltées lors du traitement du dossier d'assistance. Les données de santé ne seront en aucun cas transmises à l'assureur.
- Chaque responsable de traitement doit déclarer son traitement à la CNIL (ou l'inscrire sur le registre du CIL).

2.10 Envoi d'une offre de crédit proposée par un partenaire

2.10.1 Contexte. Une majorité d'assureurs proposent à leurs clients une possibilité de contracter un prêt à taux préférentiel. Ce prêt est souscrit auprès d'un organisme tiers, compétent pour accepter ou rejeter la demande. Toutefois, l'utilisation de la marque de l'assureur pour identifier le produit crée bien souvent un amalgame entre l'assureur et l'organisme prêteur.

De cette confusion peuvent naître des réclamations fondées sur la loi Informatique et Libertés susceptibles de ne pas donner lieu à une réponse adéquate, par exemple, le client va demander à son assureur pourquoi sa demande de crédit a été rejetée (cette faculté incombe en fait à l'organisme prêteur), voire se plaindre à la CNIL d'une consultation illicite par son assureur du fichier FICP tenu par la Banque de France, ce qui ne peut pas être le cas.

2.10.2 Responsabilités. Dans ce type de montage, deux traitements sont successivement mis en œuvre par deux organismes distincts, responsables de leur propre traitement, l'un ayant pour finalité la « *gestion d'un fichier de clients et prospects, opérations de prospection sur les produits et services de l'organisme et de ses partenaires* », l'autre ayant pour finalité la « *gestion des demandes de crédit* ».

Dans les deux cas, la donnée client vient du client lui-même, qui la transmet spontanément aux deux organismes dans le cadre de deux traitements clairement identifiés :

- le client ou le prospect adresse ses données à l'assureur, qui en contrepartie l'informe sur ses propres produits ou services ou sur ceux de ses partenaires (en l'occurrence organisme prêteur), sans cession de données à celui-ci,
- ce même client ou prospect renvoie ses données à l'organisme prêteur mais à une adresse identifiable comme celle de l'assureur[31] (principe de la « marque blanche »).

Bien que les responsabilités soient sur le plan juridique très clairement établies, l'information donnée au client est parfois trop confuse pour lui permettre d'exercer correctement ses droits Informatique et Libertés.

Recommandations de l'AFCDP

- les courriers adressés par l'assureur au client, et par lesquels il lui transmet une information concernant les produits et services d'un organisme prêteur doivent être clarifiés au maximum pour préciser les responsabilités de chacun,
- il est très important de convenir d'une procédure entre l'assureur et l'organisme prêteur afin de traiter de manière adéquate les demandes des clients liées à la loi Informatique et Libertés. Cette procédure fera notamment état :
  - des modalités d'information (canal, délai, interlocuteurs…) réciproque,
  - du contenu du courrier d'attente adressé par le destinataire de la réclamation au client.

2.11 Opérations commerciales de plusieurs partenaires sur une même cible

2.11.1 Contexte. Lorsqu'une société commerciale communique avec ses clients, elle peut être amenée à les solliciter pour des produits et services complémentaires proposés par ses partenaires commerciaux. Trois principaux cas de figure peuvent être envisagés :

- la société adresse elle-même à ses clients et prospects des informations concernant les produits et services de ses partenaires,
- la société cède le fichier à ses partenaires qui sont en charge de la prospection. Cette cession peut être réciproque et prendre la forme d'une mutualisation des données clients, centralisées dans un seul et unique fichier,
- la collecte des données prospect est réalisée par l'intermédiaire d'une plate-forme de VAD en ligne proposant les produits de tous les partenaires.

2.11.2 Responsabilités. Il convient d'étudier chacun des trois cas mentionnés ci-dessus pour déterminer leur degré de responsabilité dans chacune des démarches :

2.11.2.1 Distribution des produits des partenaires : dans ce contexte, la société qui prend contact avec ses clients est simplement responsable de la gestion de son fichier de clients et prospects, elle n'est pas responsable de la gestion contractuelle qui pourrait découler d'une éventuelle souscription

[31] À noter dans ce dernier cas qu'il peut arriver que l'assureur récolte les données auprès de son client pour les demandes de crédit pour le compte de l'organisme de crédit

subséquente à son opération de prospection. Une question se pose toutefois sur l'étendue du retour que cette société peut recevoir de l'organisme dont elle diffuse les produits : elle n'a en effet aucune légitimité à être informée de la vie du contrat souscrit.

Ainsi, en dehors des informations strictement nécessaires au calcul des commissions dues à la société distributrice, aucune donnée personnelle n'a vocation à lui être adressée pour ses propres besoins commerciaux. Toutefois, une telle transmission d'informations reste possible si, à l'occasion de la souscription du produit, les mentions légales faisaient bien apparaître cette société comme destinataire potentiel des données et laissaient au souscripteur la possibilité de s'opposer à une telle communication d'informations.

2.11.2.2 Cession d'un fichier client à des partenaires : dans ce cas de figure, chaque organisme utilise les données personnelles des clients de la première structure à ses propres fins commerciales. Ainsi, la responsabilité de la mise en œuvre du traitement pèse uniquement sur le partenaire rendu destinataire des données, la seule obligation résiduelle pour l'organisme « fournisseur » étant la transmission des réclamations de ses clients aux partenaires qu'il a rendus destinataires des données, par ricochet.

2.11.2.3 VAD multiproduits via une interface de vente en ligne : ce montage repose sur un principe de mutualisation de la ressource informatique par plusieurs sociétés commerciales pour promouvoir et distribuer leurs produits et services, en s'appuyant sur un seul et unique portail (ou galerie commerciale).

Cette configuration fait donc apparaître deux catégories d'acteurs :

a) l'organisme en charge de la supervision technique de la plate-forme (généralement le groupement de moyens au sein du groupe ou un prestataire extérieur, en charge du développement et de la maintenance) est nécessairement le sous-traitant des sociétés dont il fait figurer les offres sur la plate-forme. Il n'est donc pas le responsable des traitements qui sont mis en œuvre à partir de celle-ci, et n'agit que sur instruction des sociétés, responsables des traitements, sauf pour le traitement des données de connexions des visiteurs du site dont il est responsable de traitement ;

b) chaque société est responsable des traitements concernant ses propres clients et prospects. Plusieurs cas de figure peuvent se présenter :

- le client/prospect souscrit en ligne à une ou plusieurs offres proposées par le portail. Chaque société concernée est responsable du traitement découlant de la demande de souscription, sans interdépendance avec les autres sociétés ;

- le client/prospect utilise un espace client unique en ligne lui permettant de consulter ou de gérer tous ses contrats et demandes de devis : cet espace est une faculté offerte par chaque société, responsable de traitement, à son client/prospect. La mutualisation de cet espace ne représente qu'une modalité technique de mise en œuvre d'un traitement relatif à la consultation ou à la gestion du contrat et des devis, dont la responsabilité incombe à chaque société ;

- la constitution d'une base de données « prospects » peut présenter un réel problème d'identification lorsque les données sont collectées par la plate-forme de VAD et vouées à une prospection ultérieure pour tout autre type de produit, soit par les sociétés utilisatrices de la plate-forme, soit par leurs partenaires commerciaux. Dans cette configuration, et en gardant à l'esprit que le prestataire technique ne peut pas juridiquement être responsable de tels fichiers parce qu'il ne peut agir que sur instruction pour le constituer, il conviendrait peut-être de remonter à l'organisme signataire du contrat de développement et de maintenance, légitimement habilité à collecter des données à des fins d'exploitation commerciale. À ce stade, deux possibilités sont envisageables :
    - le signataire du contrat est une société commerciale, auquel cas celle-ci sera responsable en premier lieu de la base de données ainsi constituée, et ses

partenaires à leur tour responsables en tant que destinataires de données en vue de la mise en œuvre de traitements relevant de leur propre responsabilité ;

- le signataire du contrat est un autre interlocuteur technique (autre prestataire, groupement de moyens…), auquel cas il faut rechercher en amont quel est l'organisme qui a mandaté en cascade ces prestataires pour en déduire la responsabilité.

Recommandations de l'AFCDP

Adopter une mention légale *ad hoc* qui consignera l'information de la personne préalablement à toute forme de prospection, et la faculté dont dispose le responsable du traitement pour communiquer les données personnelles à un organisme tiers (voir à ce titre les modèles de mentions légales proposées sur le site de la CNIL[32])

- Dans le cas du recours à un système susceptible de proposer au client une pluralité d'organismes responsables de traitements (plate-forme de VAD par exemple), la possibilité pour celui-ci de faire appel à un seul et unique interlocuteur pour l'exercice de ses droits Informatique et Libertés est fortement recommandée, pour des raisons évidentes de lisibilité. De manière générale, il conviendra de simplifier au maximum les procédures d'accès reconnues au client,
- Ne pas oublier que conformément aux obligations découlant de la LCEN[33], l'adresse mail collectée par une société ne peut pas être cédée à une autre société sauf accord explicite et éclairé de la personne, ni être utilisée par la société responsable du traitement pour proposer des services qui ne seraient pas considérés comme « analogues[34] ». Toute société extérieure à celle qui doit être considérée comme responsable d'un traitement est considérée comme tiers, quand bien même elle ferait partie d'un même groupe (société partenaire, filiale…). Ainsi, il n'est pas possible pour la société légitimement détentrice de l'adresse mail de proposer des produits et services analogues qui seraient fournis par l'un de ses partenaires (voir en ce sens la jurisprudence Amazon, qui rappelle que le produit ou service analogue doit impérativement être « fourni » par la même personne, et non pas simplement « distribué »[35]),
- Rappeler à tout sous-traitant qu'il n'est autorisé à utiliser les données qui lui sont confiées que dans le cadre d'une finalité déterminée et sur instruction du responsable du traitement, et qu'il ne dispose d'aucune latitude, sauf stipulation contractuelle spécifique, pour procéder à des opérations de prospection commerciale pour ses propres produits,
- Convenir d'une procédure pour répercuter « par ricochet » une demande d'opposition (notamment à toute forme de prospection) ou de suppression des données afin que tous les acteurs de la chaîne prennent en compte la demande, conformément aux obligations qui leur incombent en tant que responsables de traitement autonomes[36].

NB : Nous pensons qu'un client qui serait démarché par plusieurs interlocuteurs liés dans le cadre d'un partenariat commercial dispose *a priori* de quatre modes opératoires pour faire valoir ses droits :

- soit se retourner contre tous les responsables de traitements pour faire valoir ses droits, mais cela implique qu'il soit informé de l'identité de chaque organisme qui se serait vu communiquer des

[32] http://www.cnil.fr/vos-responsabilites/informations-legales/
[33] Notamment article L34-5 du Code des postes et des communications électroniques
[34] Il est possible de trouver une ébauche de réflexion sur cette « analogie » dans la charte de l'emailing qui considère que les services analogues sont ceux pour lesquels la personne concernée pouvait raisonnablement s'attendre à recevoir des prospections directes de la part du vendeur ou du prestataire ayant recueilli les coordonnées.
[35] « *Attendu que la clause susvisée qui emploie le terme général d'offres commerciales ou services, sans aucune spécification de l'objet et qui introduit un tiers dans la prospection, est contraire aux dispositions de l'article susvisé et sera donc qualifiée de clause illicite* » (TGI Paris 28 octobre 2008)
[36] Articles 97 et 99 du décret n°2005-1309 du 20 octobre 2005

informations le concernant (ce qui semble très difficile et particulièrement contraignant - voir dissuasif - pour le client) ;

- soit se retourner contre l'organisme qui était le destinataire initial des données afin qu'il répercute la demande « par ricochet » (mais cette démarche peut prendre du temps avant que la demande soit pleinement satisfaite, de plus il est nécessaire qu'une procédure de transmission de la demande ait été définie entre les différents responsables de traitements) ;
- soit se retourner contre le prestataire technique s'il ne dispose d'aucun autre moyen pour faire valoir ses droits (mais cela implique qu'une procédure de remontée d'information ait été définie entre le sous-traitant et le responsable de traitement) ;
- soit faire valoir ses droits auprès du dernier organisme entré en contact avec lui en lui demandant de répercuter sa demande auprès de tous ses partenaires (c'est-à-dire aussi bien ceux qu'il a rendus destinataires des données que ceux qui lui ont transmis, ce qui pose un problème d'interprétation du décret du 25 mars 2007 qui prévoit comme seule obligation l'information des destinataires des données, et non des émetteurs[37]).

La quatrième solution, bien qu'elle excède les dispositions réglementaires imposées aux responsables de traitements de données à caractère personnel, est de loin la plus confortable pour la personne, et devrait par conséquent peut-être faire l'objet de préconisations d'ordre déontologique.

Attention toutefois dans ce cas spécifique à bien cerner la demande de la personne (mécontentement contre le responsable de traitement ciblé qui va impacter tous les autres responsables de traitement, y compris émetteurs, ou encore souhait de ne plus recevoir d'information concernant un type de produit spécifique…) et ne pas oublier que la vision du client est généralement confuse lorsqu'il s'agit de déterminer correctement les responsabilités.

2.12 Accompagnement du retour à l'emploi des personnes en arrêt de travail

2.12.1 Contexte. Avec l'accord de son employeur, l'organisme assureur propose à un salarié en situation d'arrêt de travail et bénéficiant d'indemnités journalières versées par l'assureur de participer à un programme de réhabilitation dans son emploi, et confie à un prestataire l'intégralité de la mise en œuvre des opérations correspondantes.

2.12.2 Responsabilités. Les trois acteurs sont susceptibles d'endosser une partie de la responsabilité, mais pour des traitements très distincts.
Elle incombe en effet :

- à l'assureur, mais seulement en ce qui concerne l'opération consistant à proposer au salarié de l'entreprise cliente un programme de reprise du travail, le cas échéant pris en charge par l'assureur (démarche informative exclusivement), cette information pouvant éventuellement être déléguée (sous-traitée) au partenaire,
- au partenaire, pour l'ensemble des traitements nécessaires à la mise en œuvre des prestations (l'assuré devient client du partenaire). Dans le cadre de ces prestations, le partenaire peut être amené à collecter de l'information relative à la santé de l'assuré, en s'appuyant notamment sur une cellule médicale dédiée et soumise au secret médical,
- à l'employeur, qui peut se voir communiquer par le prestataire des informations relatives aux mesures administratives, organisationnelles ou logistiques à adopter pour optimiser la réadaptation de son salarié. L'assureur peut également se voir communiquer des informations sous forme de reporting, limitées aux seules données nécessaires à la facturation des prestations réalisées au profit de son assuré.

[37] Voir articles 97 et 99 du décret susmentionnés

Recommandations de l'AFCDP

- Le contrat avec le prestataire doit explicitement mentionner les traitements qui relèvent de sa responsabilité et ceux qui incombent à l'employeur.
- Exiger contractuellement du prestataire qu'il soit à jour de ses déclarations CNIL ou ait désigné un CIL. Le cas échéant, lui demander de produire le détail de sa déclaration et de son récépissé, ou un extrait du registre du CIL.
- Ne pas hésiter à rappeler dans le contrat que le prestataire dispose d'une autonomie totale dans la réalisation de la prestation, et que les informations concernant l'assuré qui pourraient lui être adressées doivent se limiter à un reporting technique ou administratif nécessaire à la facturation des prestations par le partenaire à l'assureur.
- Vérifier que le contrat liant le prestataire à l'assuré soit sans équivoque quant aux responsabilités des trois acteurs, et fasse apparaître les modalités d'exercice des droits des personnes auprès du seul prestataire.
- Si la démarche d'information est déléguée au prestataire, exiger de celui-ci qu'il détruise les données d'identification relatives à toute personne figurant dans le fichier des assurés démarchés qui auraient refusé la prestation.

NB : Il est possible de recourir à une sous-traitance totale pour l'ensemble du périmètre, mais si tel est le cas, les traitements de données mis en œuvre par le prestataire seront réputés être faits sur instruction de l'assureur, qui devra mettre à jour ses déclarations CNIL en conséquence (notamment en ce qui concerne la finalité du traitement et la collecte des données de santé), et procéder à des audits pour contrôler le respect par le prestataire de la confidentialité médicale.

2.13 Gestion de la vidéosurveillance

2.13.1 Contexte. Dans un même bâtiment cohabitent plusieurs sociétés, colocataires, qui bénéficient d'un système de vidéosurveillance sur l'ensemble du site, ou du moins dans ses parties communes.

2.13.2 Responsabilités. Plusieurs cas peuvent se présenter :

1) le propriétaire a installé un système de vidéosurveillance pour sécuriser son bâtiment. Un Poste central de sécurité peut accéder aux enregistrements. La solution s'impose à tout nouveau locataire. C'est bien le propriétaire qui décide de la mise en œuvre du traitement. Il est donc responsable de traitement et doit accomplir les formalités préalables (préfecture, CNIL).

2) les locataires souhaitent mettre en œuvre un système de vidéosurveillance des parties communes (accès). La tentation est grande, dans ce contexte, de faire peser sur les épaules de l'entité signataire du contrat avec l'installateur du système de vidéosurveillance la responsabilité de l'ensemble du traitement. Nous pensons cependant qu'il est utile dans ce type de traitement de recourir à un critère spécifique, celui de la **destination** des informations collectées par le système : deviendrait coresponsable d'un traitement de vidéosurveillance tout organisme susceptible de s'appuyer sans l'autorisation d'un tiers sur les images de la vidéosurveillance dans l'établissement pour la défense de ses propres intérêts, qu'il soit ou non propriétaire du système. L'installation et la gestion du système peuvent être considérées dans cette perspective comme mutualisées, et chaque locataire comme responsable du traitement à part entière.

Dans tous les cas, il revient à chaque entreprise occupant les lieux d'assurer l'information préalable de ses salariés, prévue par le code du travail, et de procéder à l'information du Comité d'entreprise. Les visiteurs seront informés par une affichette dans les halls d'entrée. Les droits d'accès s'exerceront quant à eux par défaut auprès de la société chargée de la vidéosurveillance des locaux, en vertu d'une procédure convenue entre les entités bénéficiaires de la vidéosurveillance.

La démarche de conformité au regard de la CNIL décrite ci-dessus doit être selon nous distinguée de celle qui doit être effectuée au niveau de la préfecture.

Explications :

a) tout « **système »** de vidéosurveillance installé dans un espace recevant du public ou sur la voie publique doit faire l'objet d'une demande d'autorisation préalable en préfecture, que les séquences filmées soient enregistrées ou non. Il s'agit en quelque sorte de la conformité juridique de l'équipement utilisé pour filmer, de l'aspect « matériel » de la vidéosurveillance indépendamment de tout enregistrement des séquences vidéo, sous réserve toutefois qu'existe au moins un moniteur pour la retransmission des images.

À ce titre, l'article 1384 du Code civil[38] nous donne une piste intéressante si l'on prête attention aux critères de la « garde de la chose » : la responsabilité est liée à **l'usage** qui est fait de la chose ainsi qu'aux pouvoirs de **surveillance** et de **contrôle** exercés sur elle. Généralement, le système de vidéosurveillance fera l'objet d'un contrat d'installation et de maintenance avec une société tierce. Celle-ci agira sur instruction de l'organisme responsable du système, seul à répondre aux trois critères énoncés ci-dessus. Ainsi, seule la société qui ferait contractuellement procéder à la mise en service du système de vidéosurveillance serait considérée comme « exploitant » au sens de la loi n°95-73 du 21 janvier 1995 et de son décret d'application n°96-926 du 17 octobre 1996.
Il incombe donc uniquement à celle-ci d'effectuer les démarches en préfecture obligatoires, et non par défaut ou concomitamment au revendeur du matériel, à l'installateur du système, ou au propriétaire de l'établissement visé (si celui-ci est différent)[39].

b) tout « **traitement** » de vidéosurveillance impliquant un stockage des séquences vidéo est soumis à la loi Informatique et Libertés. Responsable du traitement en premier lieu, l'exploitant du système doit répondre aux obligations découlant de la loi Informatique et Libertés. Toutefois, les autres personnes morales qui partagent les locaux pourraient exiger, le cas échéant, communication des enregistrements afin de défendre leurs propres intérêts (par exemple en cas d'intrusion ou de dégradation). À ce titre, elles deviendront responsables de traitement par destination, ce qui implique l'accomplissement en amont des formalités obligatoires auprès de la CNIL.

	Formalités préfecture	Formalités CNIL
Revendeur	Non	Non
Installateur	Non. Doit juste délivrer une attestation de conformité si certifié	Non
Prestataire sécurité	Non	Non. Mentions CNIL obligatoires dans contrat avec exploitant
Propriétaire établissement	Oui, s'il est aussi propriétaire des équipements de vidéosurveillance	Oui, s'il exploite le système pour ses propres besoins
Locataire titulaire du contrat de bail	Oui, s'il est propriétaire des équipements de vidéosurveillance	Oui, s'il exploite le système pour ses propres besoins
Colocataire	Non	Oui, s'il exploite le système pour ses propres besoins

[38] « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde* ».

[39] La notice d'information relative au formulaire CERFA n° 13806*01 de demande d'autorisation d'un système de vidéosurveillance dispose que « l'*autorisation de mise en œuvre d'un système de vidéosurveillance est délivrée à la personne responsable du système, c'est-à-dire à celle qui, ayant la capacité juridique pour ce faire, estime nécessaire de recourir à la vidéosurveillance. L'obligation de déclaration des systèmes entrant dans le champ d'application de la loi du 21 janvier 1995 incombe à l'exploitant des lieux où sont installées les caméras, qu'il soit ou non le propriétaire des lieux et même lorsque le système de vidéosurveillance n'est installé que pour une durée limitée. Le responsable n'est donc pas l'installateur* ».

Recommandations de l'AFCDP

- Le responsable du traitement (soit le propriétaire, soit les locataires) doit :
  - Le cas échéant, contractualiser avec la société de gardiennage qui assure la sécurité des locaux (PC Sécurité). Le contrat de vidéosurveillance doit intégrer la définition de la sécurité et de la confidentialité, l'obligation d'agir uniquement sur instruction du responsable de traitement ;
  - Accomplir les formalités préalables adéquates (démarche auprès de la Préfecture, déclaration du traitement à la CNIL ou inscription sur le registre du CIL) ;
  - Afficher clairement à destination des visiteurs le nom et la qualité du responsable de traitement ainsi que les modalités permettant d'exercer son droit d'accès ;
  - Définir une procédure d'accès aux images de la vidéosurveillance (qui est habilité à accéder aux images, comment « tracer » la demande d'accès etc..).
- En cas de traitement soumis à autorisation préfectorale et stockant des images exploitées par plusieurs sociétés, la personne habilitée à accéder aux enregistrements (et déclarée à la préfecture) devra être mandatée (directement ou non) pour y accéder pour le compte de toutes les sociétés concernées.

2.14 Organisation des déplacements professionnels des salariés

2.14.1 Contexte. Une société confie à un prestataire la mise en œuvre des opérations de réservation, au profit de son personnel, de titres de transport et de chambres d'hôtels, et lui transmet à cette fin un fichier permettant d'identifier les salariés bénéficiant de ces services. Ce même prestataire alimente par ailleurs sa propre base de données à partir des préférences de voyage renseignées spontanément par les utilisateurs afin de leur proposer des offres commerciales complémentaires diverses.

2.14.2 Responsabilités. Ce traitement permet de discerner assez clairement deux responsabilités. La difficulté est d'identifier la frontière entre les deux traitements :

- le sous-traitant n'a aucune autonomie dans la mise en œuvre des missions de recherche de prestataires tiers et de réservation de titre de transport. Il agit sur mandat de l'employeur et ne peut utiliser les données des utilisateurs à d'autres fins que celles qui lui ont été confiées. À ce niveau, l'employeur autorise le sous-traitant à procéder à des traitements de ciblage marketing pour ses propres besoins et de manière autonome, sous réserve que le salarié accepte explicitement cette démarche de la part du prestataire, et que ce dernier se limite à certains types de propositions commerciales très limitées[40].
- après acceptation expresse du salarié, celui-ci transmet directement au prestataire des informations complémentaires (préférences de voyages ou d'alimentation notamment) en vue de recevoir de l'information sur des prestations analogues proposées librement par le prestataire. Il y a ainsi enrichissement d'une base de données qui échappe au contrôle de l'employeur, ce qui induit par conséquent un traitement différent dont le prestataire est seul responsable.

Recommandations de l'AFCDP

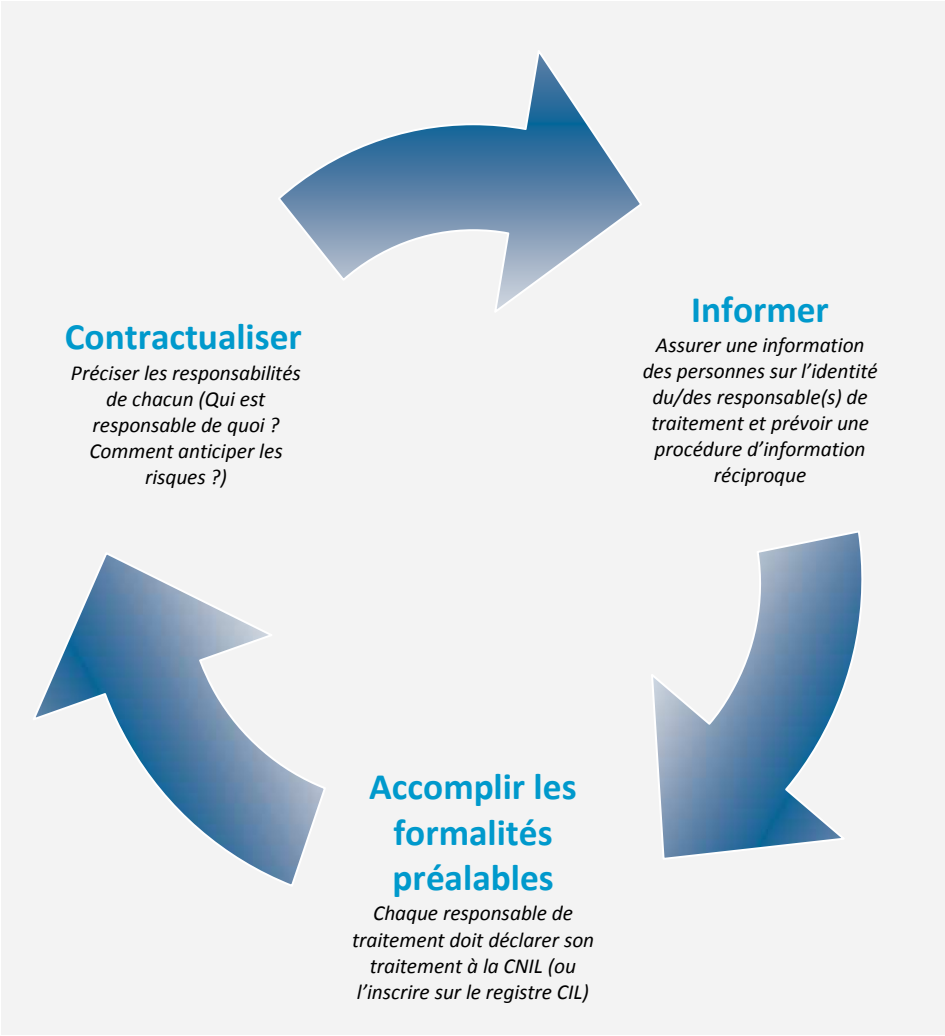
- le contrat liant l'employeur au prestataire doit indiquer les responsabilités de chacun et notamment rappeler que dans la première phase du traitement le sous-traitant n'agit que sur instruction de

[40] Le passage du statut de « sous-traitant » à celui de « partenaire indépendant » est très délicat à appréhender et doit donc être décrit avec précision dans le contrat de prestations de services.

l'employeur (à ce niveau le prestataire est sous-traitant), et que la seconde phase de collecte de données échappant totalement à l'employeur, celui-ci n'endosse aucune responsabilité dans les traitements mis en œuvre par le prestataire ;

- le prestataire doit néanmoins s'engager contractuellement sur un périmètre d'utilisation des données à ses propres fins ;
- il est souhaitable que ce nouveau type de traitement fasse l'objet d'une information préalable des salariés et du comité d'entreprise, pour clarifier le périmètre de compétence et de responsabilité de l'employeur et de son prestataire
- il importe pour chaque société de veiller à être à jour de ses déclarations CNIL ;
- il convient de définir une procédure d'information réciproque en cas de réclamation CNIL d'un utilisateur susceptible d'avoir un impact sur les traitements de l'autre partie (voir modèle en annexe).

La démarche proposée



Annexe 1 - Modèles de clauses

1) Exemple de clauses contractuelles relatives à la responsabilité

1. Au regard de l'article 3 de la loi n°78-17 du 6 janvier 1978, modifié par la loi n°2004-801 du 6 août 2004, relative à l'informatique, aux fichiers et aux libertés, il est précisé que :
   - o [PARTIE 1] est responsable du traitement consistant à [1ère finalité]
   - o [PARTIE 2], qui décide de manière autonome de [2nde finalité] et des conditions de sa mise en œuvre, est responsable des traitements qui en découlent.

2. [PARTIE 1] et [PARTIE 2] se garantissent réciproquement avoir procédé aux démarches administratives exigées par la loi (à effectuer auprès de la CNIL ou de leur Correspondant Informatique et Libertés), et veiller au respect des dispositions de celle-ci.

3. [PARTIE 1] garantit [PARTIE 2] contre toute mise en cause relative à l'exactitude des informations qui lui seront fournies. Il garantit également que toutes les informations transmises ont été collectées de manière loyale et licite auprès des personnes concernées.

2) Exemple de procédure pour le traitement des demandes clients

1. En tant que responsable du traitement, [PARTIE RESPONSABLE] s'engage à faire figurer sur les supports de collecte de données une adresse valide pour l'exercice des droits d'accès, d'interrogation, de rectification et d'opposition, et à veiller au traitement adéquat des demandes formulées par les personnes concernées. De manière plus générale, [PARTIE RESPONSABLE] répondra à toute demande émanant d'une personne physique justifiant de son identité relative à l'utilisation de ses données personnelles par [PARTIE RESPONSABLE] ou [AUTRE PARTIE].

2. Dans la mesure où une personne, dont les données personnelles sont traitées par [AUTRE PARTIE] pour le compte de [PARTIE RESPONSABLE], exercerait ses droits directement auprès de [AUTRE PARTIE], cette dernière s'engage à informer sans délai [PARTIE RESPONSABLE] de cette opposition afin que celle-ci prenne immédiatement les dispositions nécessaires.

3. Chaque partie est responsable envers les personnes concernées des dommages qu'elle cause par suite d'une violation des droits de ces personnes. Les PARTIES ne sont pas solidairement responsables des préjudices éventuellement subis par les personnes dont les droits ont fait l'objet de manquements.

4. Dans les cas impliquant des allégations de manquement par [AUTRE PARTIE], la personne concernée doit d'abord demander à [PARTIE RESPONSABLE] de prendre les mesures appropriées pour faire valoir ses droits à l'encontre de [AUTRE PARTIE]. Si [PARTIE RESPONSABLE] ne prend pas ces mesures dans des délais raisonnables (un mois maximum), la personne concernée peut faire valoir ses droits directement à l'encontre de [AUTRE PARTIE].

Annexe 2 – Documentation

(Cliquez sur les titres pour activer le lien hypertexte correspondant)

1) **Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, 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**

PREAMBULE
(47) considérant que, lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message; que, toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service;

CHAP 1 ART 2
d) «**responsable du traitement**»: 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;

e) «**sous-traitement**»: 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;

f) «**tiers**»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données;

g) «**destinataire**»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires;

2) **Loi (fra) Informatique et Libertés du 6 janvier 1978 modifiée**

Article 3
I. - 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.

II. - Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

Article 35

Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.
Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.
Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.
Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

3) Loi (lux) du 2 août 2002 modifiée relative à la protection des personnes à l'égard du traitement des données à caractère personnel

(d) «***destinataire***»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre de l'exécution d'une mission légale d'enquête ou de contrôle ne sont pas considérées comme des destinataires;

(n) «***responsable du traitement***»: 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 ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales;

(o) «***sous-traitant***»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement;

4) Loi (ger) fédérale sur la protection des données du 27 janvier 1977 modifiée

(7) On appelle service ou organisme responsable toute personne ou organisme collectant, traitant ou utilisant des données personnelles ou bien les faisant collecter, traiter ou utiliser par un tiers par mandat pour ses propres besoins.

(8) On appelle destinataire toute personne ou organisme recevant les données. On appelle tiers toute personne ou organisme autre que le service responsable. Les tiers ne sont ni la personne concernée, ni les personnes, services ou organismes collectant, traitant ou utilisant des données personnelles par mandat à l'intérieur du pays, dans un autre Etat membre de l'Union européenne ou dans un autre Etat contractant de l'Accord sur l'Espace économique européen.

5) Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite « Convention 108 »

Article 2

d) «**maître du fichier**» signifie: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations

6) **Avis du G29 du 16 février 2010 sur les notions de Responsable de traitement et de sous-traitant**

Extrait :

« la Commission prévoit la possibilité que «pour un même traitement, il peut y avoir plusieurs coresponsables décidant conjointement de la finalité du traitement et des moyens à mettre en œuvre pour l'effectuer» et que «dans un tel cas, chacun des coresponsables doit être considéré comme tenu au respect des obligations posées par la directive en vue de protéger les personnes physiques dont les données sont traitées».
L'avis de la Commission ne rendait pas totalement compte des complexités de la réalité actuelle du traitement des données, puisqu'il n'envisageait que le cas où tous les responsables du traitement décident de façon égale et sont responsables de façon égale d'un même traitement. Or la réalité montre qu'il ne s'agit là que d'une des facettes de la «responsabilité pluraliste». Dans cette optique, «conjointement» doit être interprété comme signifiant «ensemble avec» ou «pas seul», sous différentes formes et associations ».

7) **Délibération n°2007-044 de la CNIL et date du 8 mars 2007**

Extrait :

« *Les données sont traitées dans des fichiers informatisés distincts en fonction de l'établissement qui les a transmises à la société Experian, mais qui ont vocation à être mis en relation à tout moment pour permettre l'élaboration des rapports de crédit. Dès lors, ce projet constitue un traitement automatisé de données personnelles, caractérisé par des finalités et des moyens informatiques déterminés par la société Experian, qui, conformément au 1 de l'article 3 de la loi du 6 janvier 1978 susvisée, en est ainsi le responsable* ».

8) **Jurisprudence Numéricâble (TGI Paris 15 septembre 2009)**

Extrait :

« *La clause permettant ainsi au professionnel de transférer des informations concernant la vie privée du client ou ayant un caractère confidentiel (coordonnées bancaires notamment) à des tiers que n'a pas choisi l'abonné, pour des opérations qu'il ne connaît pas, sans aucune contrepartie pour le consommateur, emporte manifestement déséquilibre ; que le fait de permettre au client de s'opposer à ce transfert, opposition par ailleurs uniquement prévue pour la communication de ses adresses e-mail ou numéros de fax, n'est pas de nature à ôter le caractère déséquilibré de la clause* »

9) **Jurisprudence Amazon (TGI Paris 28 octobre 2008)**

Extrait :

« *Attendu que le principe posé par l'article L. 121-20-5 du code de la Consommation est le suivant "est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen" ;*

Que l'exception prévue au 5ème alinéa autorise la prospection directe pour "des produits ou services analogues fournis par la même personne physique ou morale" ;

Attendu que la clause susvisée qui emploie le terme général d'offres commerciales ou services, sans aucune spécification de l'objet et qui introduit un tiers dans la prospection, est contraire aux dispositions de l'article susvisé et sera donc qualifiée de clause illicite ».

10) Jurisprudence Pages jaunes / FREE (TI d'Issoire, 23 décembre 2009)

Extrait :

« *Les deux fautes, l'une de nature contractuelle imputée à FREE, et l'autre de nature délictuelle commise par la société PAGES JAUNES ont produit le dommage consistant dans la publication de la mention dans l'annuaire* ».

11) Délibération CNIL n°2010-113 du 22 avril 2010 (AIS2)

Extrait :

« *Il apparaît ainsi que la société AIS 2, qui dispose d'un véritable contrôle sur les bases de données précitées et sur leur contenu, détermine de manière autonome la manière dont sont traitées les informations qu'elle reçoit dans le cadre de son activité. En particulier, la Commission relève que la société AIS 2 exerce un contrôle sur les données concernant les candidats qu'elle sélectionne, les enseignants auxquels elle attribue des cours ainsi que les clients et prospects sollicitant ses services.*

Il ressort de ce qui précède que la société AIS 2 détient la faculté, à tout le moins partielle, de déterminer les finalités et les moyens des traitements mis en cause. La Commission se trouve donc fondée à lui attribuer la qualité de responsable de traitement dans cette affaire. »

12) Guide CNIL 2009 pour l'enseignement supérieur et la recherche

Extrait :

« *Les responsables du traitement sont d'une part l'université et d'autre part l'organisme de recherche puisque les deux assument la tutelle de l'unité. Cependant afin d'assurer la cohérence des politiques menées, il leur reviendra de définir dans les conventions qui les lient celui d'entre eux qui aura à s'assurer de la bonne application des dispositions "Informatique et Libertés" et donc à remplir le rôle de responsable pilote de traitement, unité par unité.*

[…]

Une problématique analogue est susceptible d'apparaître dans le cadre des pôles de recherche et d'enseignement supérieur (PRES) dans la mesure où certains mutualiseront des applications informatiques. Dans ce cas, il faudra explicitement déterminer si la responsabilité du traitement incombe à chaque établissement ou au PRES. »

13) Guide CNIL « *Transfert de données à caractère personnel vers des pays tiers à l'UE* »

Extrait :

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.*

14) Rapport d'étape de la CNIL (2003) sur l'application de la loi I&L par les communes

Extrait :

« La mise en œuvre de fichiers par les établissements publics de coopération intercommunale (EPCI) est parfois source de confusion quant à la détermination du responsable juridique de ces fichiers, au regard de la loi du 6 janvier 1978. Tel est le cas lorsque la commune et l'EPCI disposent d'un service informatique commun ou encore lorsque des applications développées par l'EPCI sont accessibles en ligne aux communes du territoire.
Si l'EPCI intervient seulement comme prestataire technique de la commune, seule la commune reste responsable du fichier et doit en conséquence le déclarer auprès de la CNIL. Il en est ainsi par exemple si la gestion technique du fichier du personnel d'une commune est confiée à la direction informatique d'un EPCI qui agit alors comme sous-traitant, la responsabilité du fichier continuant de reposer sur le maire. Si, en revanche, l'EPCI, dans le cadre d'un transfert de compétences, s'est vu confier la gestion administrative du service des ressources humaines de la commune et à cet effet la tenue du fichier du personnel (tel était le cas pour une des communes visitées), la responsabilité de ce traitement reposera sur le président de l'EPCI.
Par conséquent, les statuts de l'EPCI2 doivent explicitement prévoir que les transferts de compétences entraînant transferts de fichiers nominatifs conduisent à transmettre à cet établissement public la responsabilité de ces fichiers et notamment à effectuer les déclarations nécessaires auprès de la CNIL. »

15) Réflexion de la CNIL sur « *Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques* », CNIL, oct. 2010

Extrait :

« 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. » (Voir critères directement sur le site de la CNIL).

16) Rapport n°218 réalisé à l'issue de la réunion de la commission des lois en date du 19 mars 2003 (dans le cadre de la réforme de la loi Informatique et Libertés), présidée par M. Garrec

Extrait :

« L'article 2 paragraphe d) de la directive 95/46 et le présent projet de loi définissent le responsable du traitement comme 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.
Le responsable ne doit pas être confondu avec les personnes qui, tels les employés ou les sous-traitants, mettent en œuvre des traitements pour son compte.
L'Assemblée nationale a adopté, sur proposition de son rapporteur de la commission des Lois, M. Gérard Gouzes, et avec l'avis favorable du Gouvernement, un amendement supprimant les termes « seul ou conjointement avec d'autres », estimant imprécise cette notion de co-responsabilité. En effet, la notion de responsable détermine notamment le droit national applicable ; or, il s'agit d'éviter des conflits de lois en cas de pluralité des responsables, ou la répartition d'office de la présomption de responsabilité entre plusieurs personnes. »

17) Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Extrait :

Art. 97 : *Le responsable du traitement auprès duquel le droit d'opposition a été exercé informe sans délai de cette opposition tout autre responsable de traitement qu'il a rendu destinataire des données à caractère personnel qui font l'objet de l'opposition.*

Art. 99 : *Lorsque des données à caractère personnel ont été transmises à un tiers, le responsable du traitement qui a procédé à leur rectification en informe sans délai ce tiers. Celui-ci procède également sans délai à la rectification.*

18) Code des postes et des communications électroniques

Extrait :

Art. L34-5 (extrait)

[…] la prospection directe par courrier électronique est autorisée si les coordonnées du destinataire ont été recueillies directement auprès de lui […] à l'occasion d'une vente ou d'une prestation de services, si la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale […].

19) Charte de l'Emailing de l'Union Française du Marketing Direct

Extrait :

Art. 10 (extrait)

« Par produits ou services analogues, on entend des produits ou services pour lesquels la personne concernée pouvait raisonnablement s'attendre à recevoir des prospections directes de la part du vendeur ou du prestataire ayant recueilli les coordonnées. Ainsi, à titre d'exemple, une personne qui commande un livre auprès d'un site Internet proposant une grande diversité de produits et services culturels, peut s'attendre à recevoir des propositions commerciales pour tous les produits et services culturels que propose habituellement l'enseigne ».