



La gestion des données à caractère personnel dans les projets d'externalisation Offshore

décembre 2010

PRÉFACE

BRUNO MÉNARD / Directeur des Systèmes d'Information - Sanofi-aventis

C'est avec un réel plaisir que j'ai accepté de préfacer le Livre Blanc de l'EOA France sur la gestion des données à caractère personnel dans les opérations d'externalisation car il répond, de manière pratique et originale, à un vrai besoin des entreprises.

En effet, cet ouvrage ne se contente pas d'expliquer de manière claire et intelligible la problématique du transfert de données personnelles dans les opérations d'externalisation et comment ce problème, s'il est mal appréhendé, peut paralyser la mise en œuvre de ces opérations.

En formulant toute une série de recommandations pratiques, l'EOA France va bien au-delà et donne aux acteurs de l'externalisation (clients utilisateurs, prestataires de services et conseils spécialisés) un véritable mode opératoire de ce qu'il convient de faire, aux diverses étapes d'un projet, pour bien le structurer et le sécuriser.

Et ce qui donne un intérêt particulier à cet ouvrage, c'est que les recommandations qu'il formule expriment la synthèse sur laquelle se sont rejointes les trois composantes de l'EOA France : clients utilisateurs, prestataires de services et conseils spécialisés. Il ne s'agit donc pas d'un ouvrage à sens unique, à destination d'une seule de ces composantes, mais, et c'est là la nouveauté, d'une vraie synthèse des positions des trois parties prenantes, alors même que leurs intérêts ne coïncident pas toujours, comme chacun le sait.

Cet ouvrage montre qu'au-delà de l'intérêt particulier de chaque partie prenante, tout le monde gagne à s'assurer qu'une opération d'externalisation offshore est bien montée et sa sécurité juridique assurée. Il démontre aussi qu'en partageant un même référentiel des choses à faire, on se facilite grandement l'atteinte de l'objectif commun.

Je suis donc convaincu que ces recommandations pratiques feront gagner beaucoup de temps aux acteurs de l'externalisation et je félicite l'EOA France pour son travail original.

J'invite tous ceux qui sont confrontés à ce type de problématique à lire cet ouvrage et à mettre en œuvre les recommandations qu'il édicte.

Bonne lecture !

Bruno Ménard

A stylized white signature on a blue background, consisting of a large loop followed by a horizontal line that ends in a small upward-pointing arrow.

SOMMAIRE

Section n°1	La problématique du transfert offshore de données personnelles	p6
	1.1 Clefs de lecture juridique	p6
	1.2 Les moyens juridiques de sécuriser les transferts offshore	p9
Section n°2	Recommandations pratiques : de la préparation de l'opération au contrat	p16
	2.1 Étude d'opportunité	p16
	2.2 Cahier des charges	p17
	2.3 Réponse du prestataire	p18
	2.4 Due diligence	p18
	2.5 Choix du ou des prestataire(s) pressenti(s)	p18
	2.6 Négociation / signature du contrat	p19
Section n°3	Recommandations pratiques : la phase de mise en œuvre	p20
	3.1 La transition	p20
	3.2 La transformation	p20
	3.3 Mode stabilisé ou récurrent	p21
	3.4 Déclenchement de la réversibilité	p21
Section n°4	Souhaits d'évolution	p22
	Tableau récapitulatif des recommandations	p24

INTRODUCTION

En octobre 2009, l'EOA France présentait les conclusions de son enquête relative à la gestion des données personnelles dans les opérations d'externalisation offshore¹.

Les résultats traduisaient une connaissance assez approximative de la législation par les acteurs² et, en conséquence, une prise en compte souvent tardive de la problématique des données personnelles dans ces opérations, susceptible d'engendrer retards, surcoûts, frustrations et parfois, infractions à la réglementation.

Cette situation était d'autant plus alarmante que la méconnaissance des règles applicables est pénalement sanctionnée³ et peut impacter négativement l'image de marque des entreprises impliquées.

Témoin du développement des opérations d'externalisation offshore, l'EOA France ne pouvait rester sans réagir et a choisi de rédiger le présent Livre Blanc à l'attention de ses membres et des acteurs de l'externalisation.

L'objet de ce Livre Blanc est d'informer et de préparer les décideurs qui envisagent une opération d'externalisation offshore, à bien appréhender, en temps utile, la question des données personnelles afin qu'elle ne constitue pas un facteur de risque ou de blocage. Il se veut un guide pratique, destiné à éclairer les acteurs de l'externalisation sur leurs responsabilités, tout en proposant un certain nombre de meilleures pratiques.

Il s'inscrit dans la suite du rapport publié par la CNIL le 11 octobre 2010, intitulé « les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques », qui apporte quelques éléments de réponse sur ces mêmes questions.

¹ Enquête réalisée auprès de 100 « décideurs », représentant les trois catégories d'acteurs du marché : clients, prestataires, conseils. Les résultats de l'enquête sont disponibles pour les membres de l'EOA France.

² Le sujet reste assez méconnu, puisque seuls 21 % des clients utilisateurs et 30 % des prestataires déclarent avoir procédé aux formalités requises par la réglementation de protection des données personnelles.

³ La loi française prévoit des sanctions pénales délictuelles allant jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende pour une

personne physique et jusqu'à 1 500 000 euros d'amende pour une personne morale (articles 226-16 et suivants du code pénal). En vertu du décret 2005-1309 du 20 octobre 2005, la CNIL a un pouvoir de sanctions pécuniaires allant jusqu'à 300 000 euros ou 5 % du chiffre d'affaires pour des violations répétées.

SECTION N°1

La problématique du transfert offshore de données personnelles

1.1 Clefs de lecture juridique

L'externalisation offshore des activités d'une entreprise est susceptible de porter sur diverses parties de son activité (opérations de type ITO pour « Information Technology Outsourcing », ou BPO pour « Business Process Outsourcing »). Ces opérations peuvent ainsi concerner les services financiers et de comptabilité, les services de paie, la gestion des ressources humaines, les centres d'appels, ou encore la sous-traitance de processus de connaissances (KPO pour « Knowledge Process Outsourcing »), notamment dans les domaines juridiques, de la R&D, de la recherche médicale, des essais cliniques, etc.

Le cloud computing apporte une problématique complémentaire en permettant aux entreprises d'externaliser ces services « dans les nuages », c'est-à-dire sans savoir précisément où seront réparties les ressources et capacités des prestataires impliqués.

Lorsqu'elles portent sur des traitements impliquant des données personnelles et sont réalisées offshore, ces opérations doivent s'attacher à satisfaire les exigences portant sur la conformité des traitements et le transfert des données personnelles hors de l'Union européenne⁴ (ci-après « UE »). En effet, dans la quasi-totalité des cas, le pays offshore de traite-

ment ne dispose pas d'une législation protectrice des données équivalente à la législation française transposant la Directive européenne⁵.

1.1.1 Conformité des traitements de données à caractère personnel

Selon la loi française⁶, constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale). Le traitement est une notion très large au sens de la loi, car il couvre « toute opération » portant sur des données personnelles, « quel que soit le procédé utilisé », et notamment la collecte, l'enregistrement, la conservation, la modification, l'utilisation et la communication des données personnelles.

Toute entreprise qui met en œuvre des traitements de données personnelles doit, en qualité de responsable de traitement, s'assurer que ces traitements sont conformes à la réglementation des données personnelles.

⁴ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995.

⁵ Le présent Livre Blanc ne traite que les opérations offshore, hors UE, et exclut les projets se limitant géographiquement aux pays de l'UE dans la mesure où la Directive européenne « Données personnelles » permet la libre circulation des données personnelles au sein de l'UE.

⁶ La loi « Informatique et Libertés » de 1978 (loi 78-17 du 6 janvier 1978 modifiée le 6 août 2004), transposant la directive 95/46/CE de l'UE (la « Règlementation des Données Personnelles »).

POUR ÊTRE CONFORMES, CES TRAITEMENTS DOIVENT VÉRIFIER LES CONDITIONS SUIVANTES

- **Les personnes concernées dont les données personnelles sont traitées par l'entreprise** (qu'ils soient salariés, clients, fournisseurs, partenaires, etc.) **doivent avoir été clairement informées** de la finalité des traitements les concernant, des destinataires des données collectées sur elles, des conséquences à l'égard de tout refus de fournir leurs données et de leurs droits d'accès et rectification aux données les concernant et détenues par l'entreprise.
- **Les données collectées doivent être adéquates, pertinentes et non excessives** eu égard à la finalité du traitement⁷.
- **Les données doivent être traitées avec des mesures de sécurité et de confidentialité adéquates.** La réglementation des données personnelles exige ainsi que tout responsable de traitement de données personnelles adopte des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information – mot de passe, firewall, etc.) et adaptées à la nature des données et aux risques présentés par le traitement et que seules les personnes autorisées puissent accéder aux données personnelles contenues dans un fichier.
- **Les données traitées doivent être conservées pour une durée limitée,** conformément à la réglementation applicable.
- **Enfin, le traitement doit avoir fait l'objet d'une déclaration à la Commission Nationale de l'Informatique et des Libertés (CNIL)** par l'entreprise responsable de traitement.

1.1.2 Les problématiques liées à un transfert de données offshore

Un transfert de données vers un destinataire situé dans un pays hors de l'UE, ne bénéficiant pas d'une législation protectrice des données équivalente à la législation française, impacte sensiblement la nature des obligations de l'entreprise, telles que résumées ci-dessus.

Pour la CNIL, « constitue (...) un transfert de données vers un pays tiers toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel

que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire ».

Constitue également un transfert, l'accès à distance à des serveurs situés dans l'UE, par des prestataires situés en dehors de l'UE.

Dès lors qu'un transfert de données doit intervenir, l'entreprise concernée engage sa responsabilité envers les personnes concernées et la CNIL et doit en conséquence s'assurer qu'elle a pris les mesures nécessaires pour sécuriser ce transfert.

⁷A noter que la Réglementation des Données Personnelles prévoit un principe général d'interdiction de collecter ou de traiter des données dites « sensibles » c'est-à-dire les données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. Il est interdit d'externaliser des traitements de données sensibles, sans le consentement exprès de la personne concernée.

L'ENTREPRISE QUI TRANSFÈRE DES DONNÉES DOIT PRENDRE LES MESURES SUIVANTES

- Identifier et modifier les documents impactés par l'opération : notices d'information ou chartes de protection des données, déclarations effectuées auprès de la CNIL, etc.
- Obtenir l'autorisation de la CNIL pour le transfert des données résultant du projet d'externalisation. Cette autorisation est en principe délivrée lorsque les mesures contractuelles prises sont conformes à celles préconisées par la réglementation des données personnelles sans aucune modification⁸ (contrats de transfert sur la base des modèles de la Commission européenne, Binding Corporate Rules⁹, certification Safe Harbor en cas de transfert vers les États-Unis).
- S'assurer qu'elle demeure bien « responsable du traitement » au sens de la réglementation des données personnelles. Le « responsable de traitement » est celui qui détermine les finalités et les moyens de traitement des données, c'est-à-dire l'entreprise qui décide à quelle fin elle entend traiter les données et avec quels outils / ressources. Or, l'opération d'externalisation n'est souvent pas neutre sur ces plans, car dans certains cas, le prestataire sort de son rôle de simple « sous-traitant », c'est-à-dire une personne agissant sous l'autorité du responsable du traitement ou sur instruction du responsable du traitement, et acquiert lui-même la qualité de responsable du traitement¹⁰. Selon le cas, l'entreprise ne devra pas utiliser le même type de contrat de transfert (Cf. 1.2 ci-après). A noter que cette question est mal maîtrisée par les entreprises, puisque l'enquête EOA a pu montrer que 14 % des clients et 15 % des prestataires pensent (de façon erronée) que le client et le prestataire sont tous les deux responsables de traitement, chacun sur la partie qu'il contrôle.

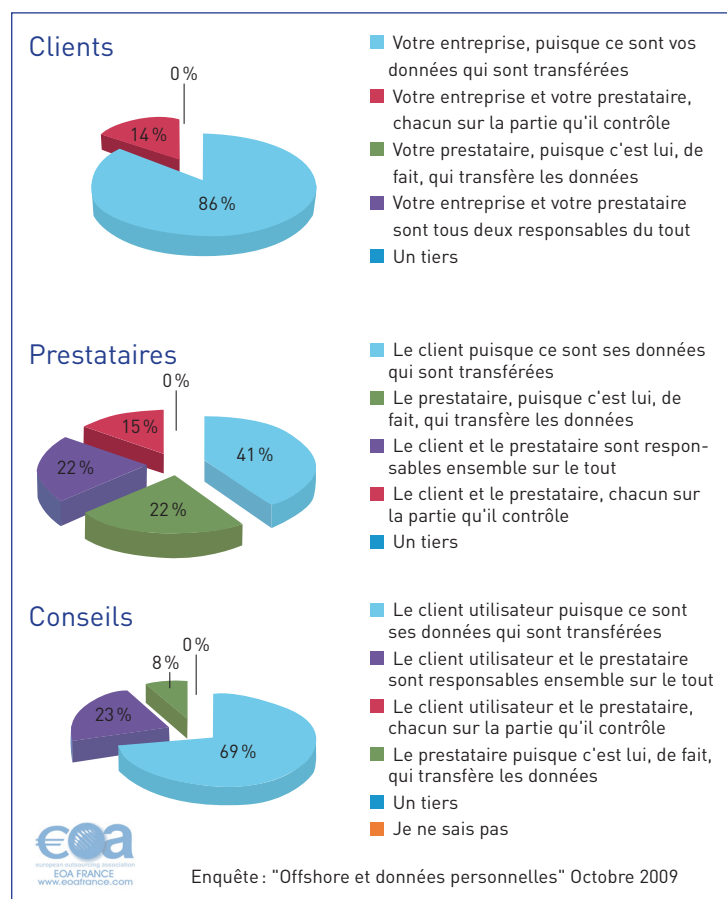
⁸ L'article 69 de la loi Informatique et Libertés et la Directive européenne 95/46/CE précitée prévoient également des exceptions en matière de transferts. On peut citer notamment le consentement exprès de la personne concernée pour autoriser les transferts, lorsque le consentement résulte d'une manifestation claire, libre et informée de la volonté. A noter cependant que le champ d'application des dispositions doit être limité à des cas ponctuels et exceptionnels, ce qui rend l'usage de cette exception rare et difficilement applicable en matière d'externalisation offshoring.

⁹ Les Binding Corporate Rules (BCR) ou règles internes d'entreprise constituent un code de conduite, définissant la politique d'une entreprise en matière de transferts de données au sein d'un même groupe

de sociétés. Ils permettent d'offrir une protection adéquate des transferts hors UE.

¹⁰ Dans le cadre de son guide des transferts de données à caractère personnel vers des pays tiers à l'UE, la CNIL a dégagé des critères qui permettent d'identifier quand le prestataire peut être qualifié de sous-traitant ou de responsable de traitement. Le guide est disponible ici : http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/GUIDE-transferts-integral.pdf. Ces critères sont : la transparence, le degré d'instruction du client, le niveau de contrôle, l'expertise.

Perception de la responsabilité de chacun, qui est responsable ?



1.2 Les moyens juridiques de sécuriser les transferts offshore

Les transferts de données personnelles en dehors de l'UE sont interdits sauf s'ils sont sécurisés par des mesures juridiques appropriées¹¹.

1.2.1 L'anonymisation des données

Les données anonymisées peuvent être librement transférées. Encore faut-il que l'anonymisation soit effective, ce qui écarte les solutions techniques non fiables, et les cas où l'anonymisation n'a pas de sens parce que le traitement suppose, par essence, de manipuler des données non-anonymisées.

Il s'agit là d'une solution essentiellement technique, dont le coût de mise en œuvre et les contraintes opérationnelles doivent être évalués et validés avec soins. Dans certains cas en effet ces coûts

sont susceptibles de gommer tout l'avantage financier recherché avec l'externalisation. Dans certains autres cas, les contraintes opérationnelles sont telles qu'elles disqualifient, pratiquement, le recours à ce procédé.

1.2.2 Les clauses contractuelles types de la Commission européenne

La Commission européenne a rédigé des modèles de contrats de transfert de données personnelles comportant des engagements à la charge de l'exportateur des données personnelles, localisé dans un pays de l'Union, et à la charge de l'importateur de ces données, localisé hors de l'Union. Ces modèles peuvent donc être utilisés par les entreprises pour sécuriser leurs transferts de données. Ces modèles de contrats, composés de clauses contractuelles types, sont :

- Les clauses du 27 décembre 2004 et du 15 juin 2001 encadrant le flux transfrontière de données entre deux responsables de traitement.
- Les clauses du 5 février 2010 encadrant le flux transfrontière de données entre un responsable de traitement et un sous-traitant (« Modèle 2010 »).

Ces modèles peuvent d'ailleurs être combinés selon les flux générés par le projet d'externalisation. Si ces modèles ont le mérite d'exister et de permettre le transfert dans des cas simples, ils présentent néanmoins des insuffisances dans la mesure où ils ne permettent pas toujours d'appréhender la subtilité des flux transfrontières liés aux projets d'externalisation, lesquels sont souvent plus complexes comme nous l'illustrons ci-après.

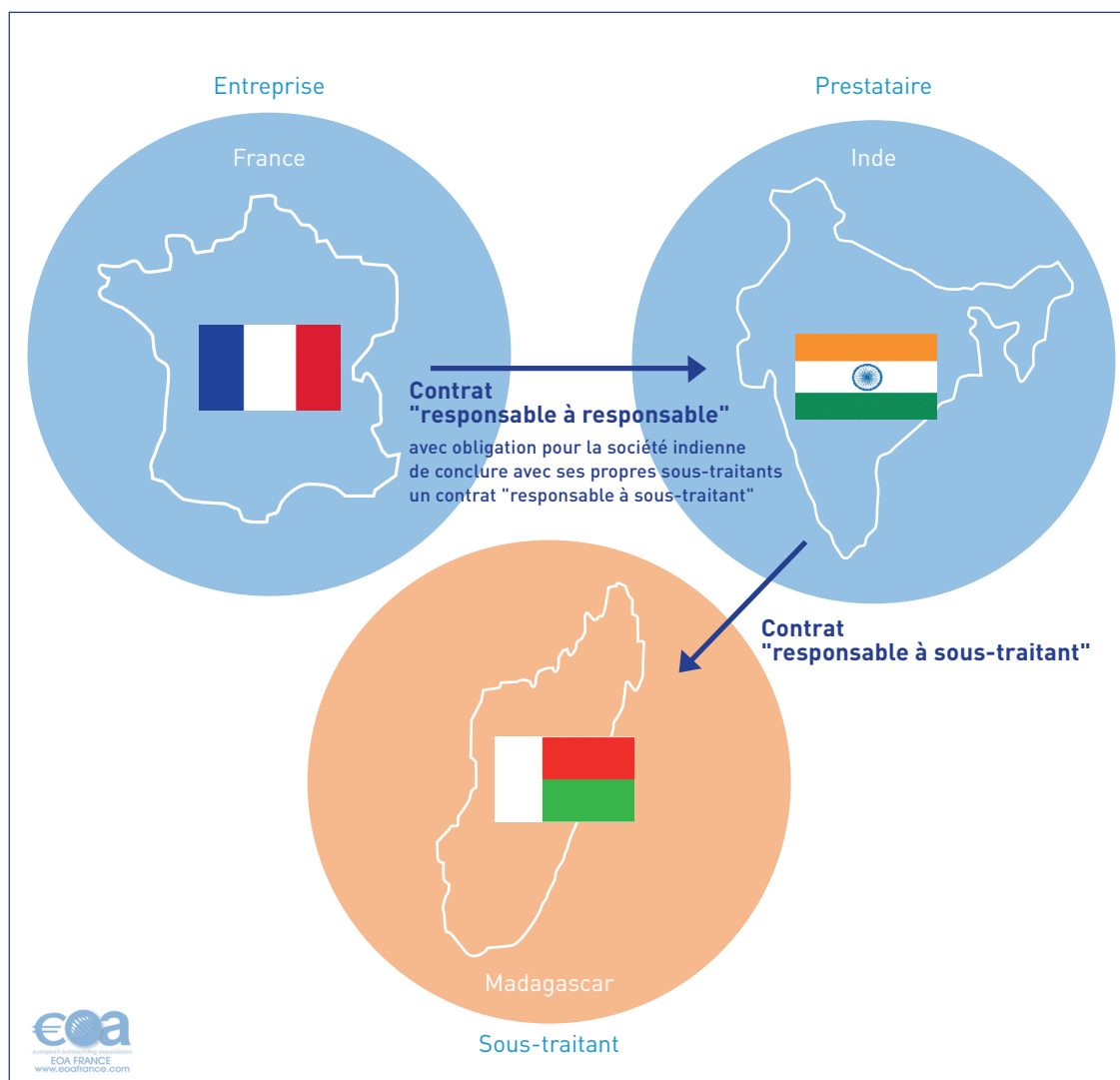
¹¹ A l'exception des transferts vers un pays reconnu comme « adéquat » par la Commission européenne, tel que le Canada, la Suisse, l'Argentine, Guernesey, Jersey et l'Isle de Man et plus récemment l'Uruguay et Israël. Les transferts vers les Etats-Unis disposent d'un régime spécifique : ils sont autorisés dès lors que la société destinataire aux Etats-Unis a adhéré au « Safe Harbor », c'est-à-dire à des principes de protection des données personnelles négociés entre les autorités américaines et la Commission européenne en 2001. Les entreprises établies aux États-Unis peuvent adhérer à ces principes auprès du Département du Commerce américain ; cette adhésion les autorise alors à recevoir des données en provenance de l'UE.

A. Cas du prestataire situé hors UE qui sous-traite à un tiers situé hors UE

A.1. Cas simple, mais peu courant: le prestataire agit également en responsable de traitement. Le prestataire agit comme responsable de traitement sur les données qui lui sont transférées car il détermine les moyens et les finalités du traitement. Il devra donc assumer la responsabilité du traitement effectué en aval par son sous-traitant, qu'il est

le seul à contrôler et à maîtriser, et donc conclure avec lui un contrat qui devra, pour être acceptable, être conforme aux clauses types. A défaut, le transfert de données vers le sous-traitant ne pourra intervenir et, s'il intervient quand même, constituera une infraction manifeste.

Prestataire qui agit en responsable de traitement

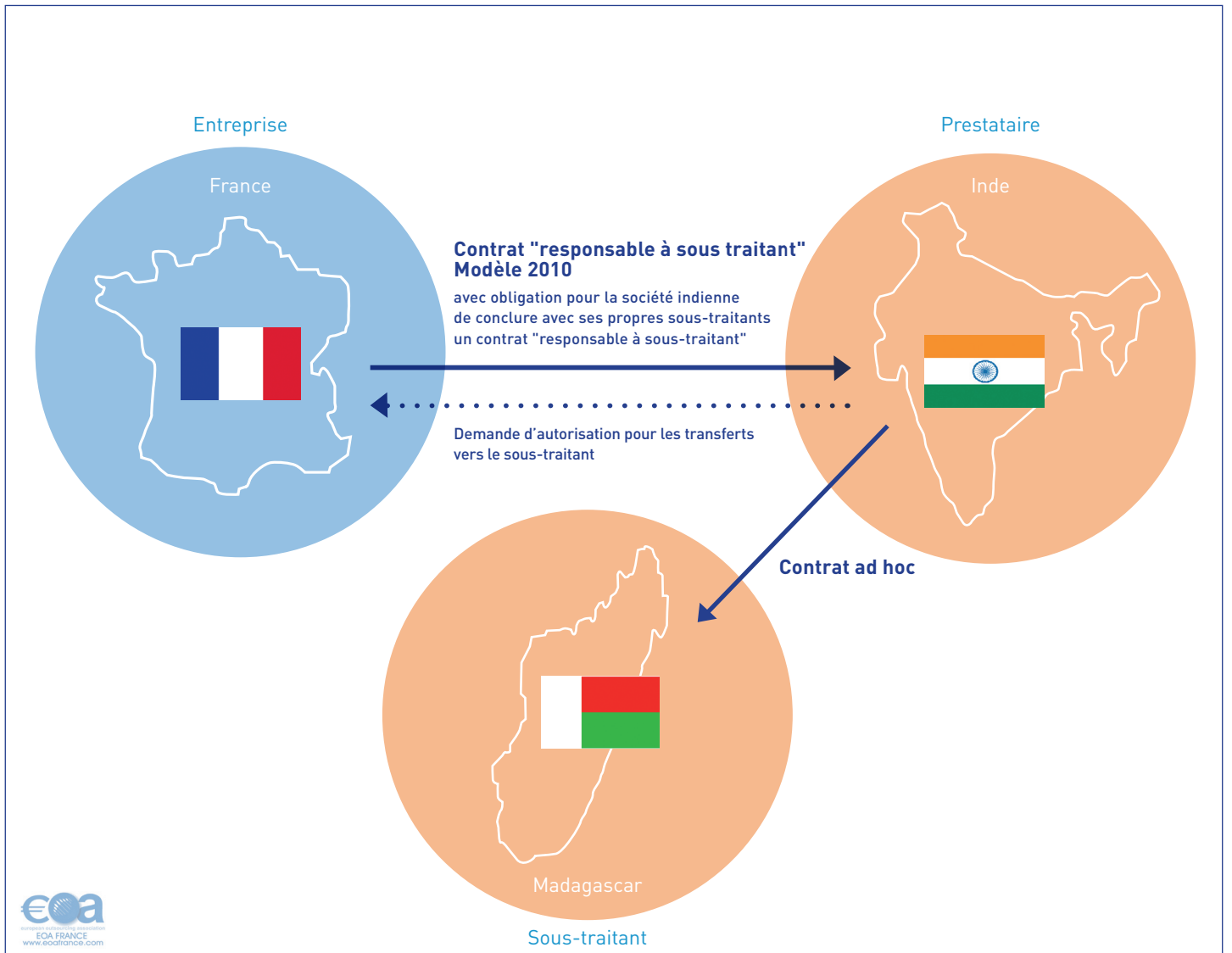


➔ Transfert hors UE

● Responsable de traitement

● Sous-traitant de données

Prestataire qui agit en véritable sous-traitant



➔ Transfert hors UE

● Responsable de traitement

● Sous-traitant de données

A.2. Cas complexe, mais plus courant : le prestataire agit en véritable sous-traitant. Agissant comme sous-traitant, le prestataire ne pourra lui-même transférer les données à un sous-traitant qu'à condition (i) d'avoir obtenu en amont l'accord écrit de l'entreprise externalisatrice (qui conserve en effet la responsabilité première du responsable de traitement) et (ii) d'imposer à son propre sous-traitant les mêmes obligations que celles qu'il aura lui-même contractées dans son contrat de transfert de données avec l'entreprise externalisatrice.

Le Modèle 2010 est normalement celui qui convient à ce type de situation. Attention toutefois : si l'entreprise externalisatrice ne dispose pas d'une visibilité effective sur les flux de données entre son prestataire et les éventuels sous-traitants de celui-ci, elle prendra un risque en signant le Modèle 2010 puisqu'elle assumera dans ce cas, seule, la respon-

sabilité de flux transfrontaliers de données dont elle ne contrôle ni le traitement, ni les sous-traitements. Pour assurer une visibilité effective à l'entreprise externalisatrice, il conviendra d'imposer, sur toute la chaîne contractuelle, au moyen d'un contrat ad hoc, la reproduction à l'identique des engagements pris par le prestataire envers l'entreprise externalisatrice.

Restent en outre certaines difficultés pratiques : le contrat « responsable à sous-traitant » Modèle 2010 prévoit que le contrat entre le prestataire et ses sous-traitants successifs doit être régi par la loi du pays de l'entreprise externalisatrice, dans notre cas la loi française. Mais est-il réaliste d'imposer à un prestataire basé en Inde qu'il applique la loi française dans un contrat qu'il va conclure avec son sous-traitant à Madagascar ?

B. Prestataire situé au sein de l'UE qui sous-traite à un tiers situé hors UE

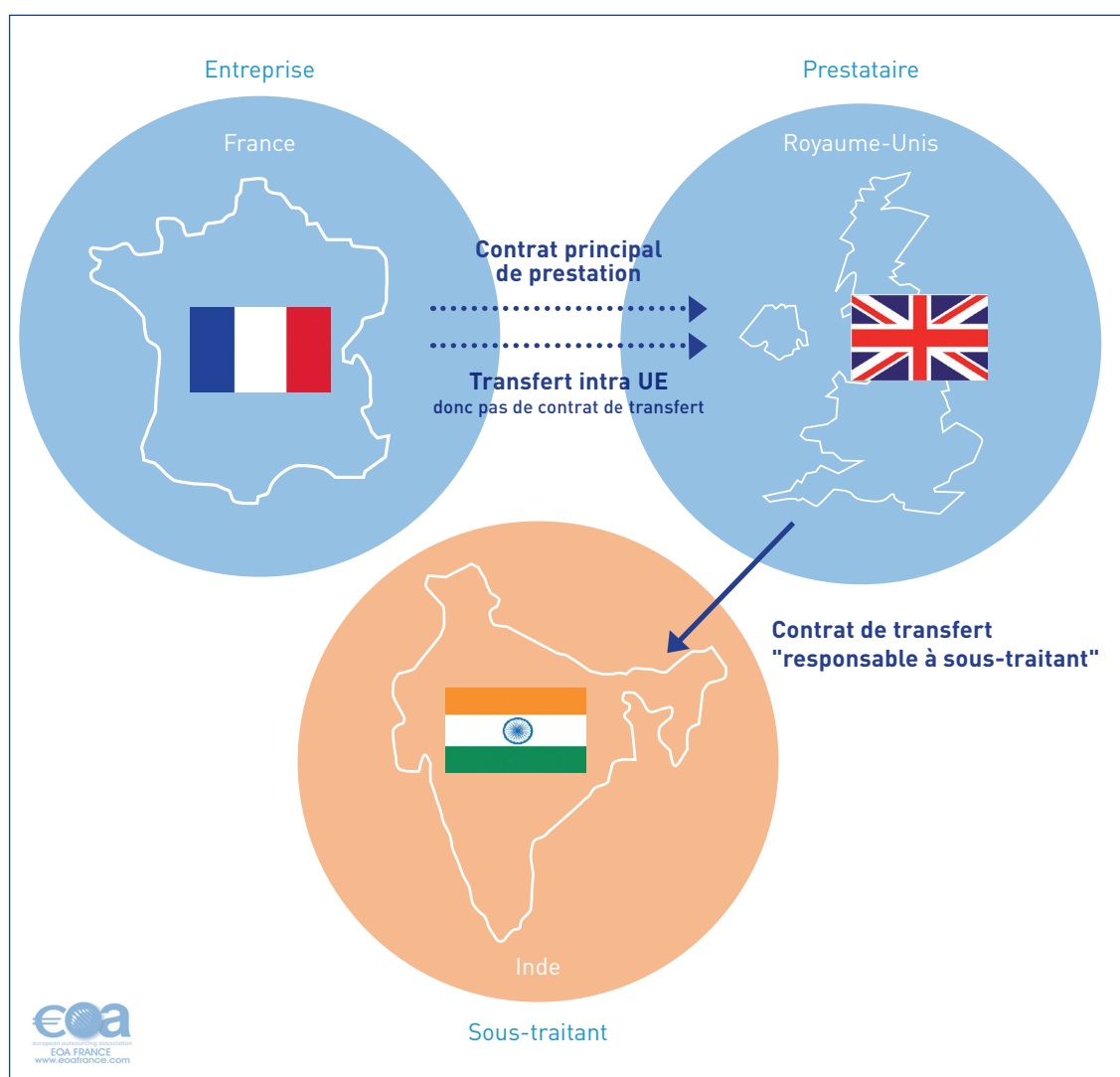
Ce scénario est fréquent car l'entreprise française recourt souvent à un prestataire installé en France ou dans un autre pays européen, qui dispose de filiales étrangères appelées à participer au projet d'externalisation. Or, les modèles de clauses types ne couvrent pas ces situations et le rapport du 11 octobre 2010 de la CNIL ne détaille pas les solutions pour couvrir ce scénario. Pourtant, en tant que responsable de traitement, l'entreprise se doit d'obtenir de son prestataire, même situé en Europe, des garanties que les données qui seront transférées dans le cadre d'une chaîne de sous-traitance maîtrisée par le prestataire, seront protégées conformément à la Règlementation des Données Personnelles.

B.1 Lorsque le prestataire basé en Europe sous-traite à une société hors-groupe se situant dans un pays en dehors de l'UE, il n'est pas nécessaire de

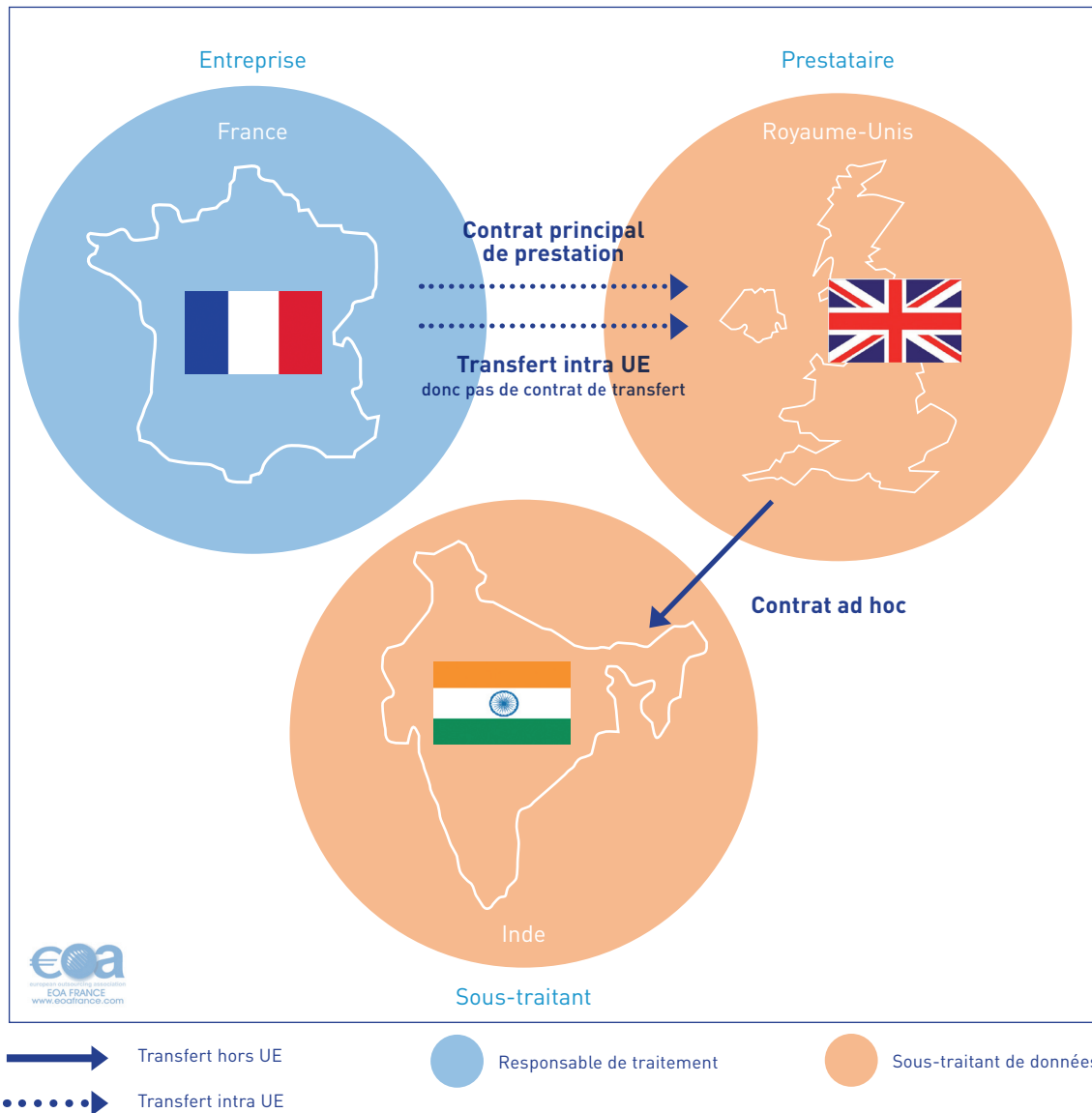
conclure les clauses types « Modèle 2010 » avec le prestataire puisque le transfert, en tant que transfert intra UE, est déjà couvert par la Directive européenne. Se pose néanmoins la question de la protection des transferts vers le sous-traitant en Inde.

Lorsque le prestataire intermédiaire agit comme responsable de traitement, un contrat Modèle 2010 devra être mis en place par celui-ci avec ses sous-traitants. Puisqu'il n'existera alors aucun lien entre l'entreprise externalisatrice et le sous-traitant hors UE, il importera, dans ce cas, d'organiser dans le contrat principal entre l'entreprise externalisatrice et le prestataire intermédiaire, les modalités pratiques permettant à celle-ci d'assumer ses responsabilités premières de responsable de traitement.

Transfert hors UE par un prestataire responsable de traitement



Transfert hors UE par un prestataire sous-traitant



B.2 Lorsque le prestataire intermédiaire agit comme simple sous-traitant, l'entreprise externalisatrice va demeurer seule responsable de traitement et devra donc s'assurer de pouvoir assumer les obligations correspondantes. Dans ce cas de figure, les « CNIL » européennes réunies au sein du « Groupe 29 » (ou « G29 »)¹², ont pris position sur l'utilisation des clauses contractuelles types Modèle 2010¹³ et proposent les options suivantes à mettre en place par un contrat ad hoc :

- **La conclusion d'un contrat direct**, conforme au Modèle 2010, entre l'entreprise externalisatrice et le(s) sous-traitant(s) établi(s) hors de l'UE. Ceci pose généralement le problème d'établir une relation directe entre deux parties qui ne sont pas contractuellement liées et potentiellement ne se connaissent pas.

- **La conclusion d'un contrat tripartite**, construit sur la base du Modèle 2010 mais non strictement conforme (car tripartite). Là encore, le problème de l'établissement d'un lien contractuel direct entre l'entreprise et le sous-traitant hors UE se trouve posé.

- **Enfin, l'entreprise peut donner mandat à son prestataire** de signer un contrat conforme au Modèle 2010 avec son propre sous-traitant, au nom et pour le compte de l'entreprise externalisatrice. Un lien contractuel sera alors établi, alors même que l'entreprise externalisatrice et le sous-traitant hors UE ne se connaissent pas. C'est la solution la plus facile à mettre en œuvre en pratique.

¹²Les « CNIL » européennes se rassemblent au sein d'un groupe dit de l'article 29 ou « G29 », qui est un organe consultatif européen indépendant sur la protection des données personnelles.

¹³Cette position se présente sous la forme d'une « Foire aux questions », ou FAQ, disponible ici : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_fr.pdf

C. Le prestataire est basé au sein de l'UE et sous-traite à d'autres sociétés de son groupe

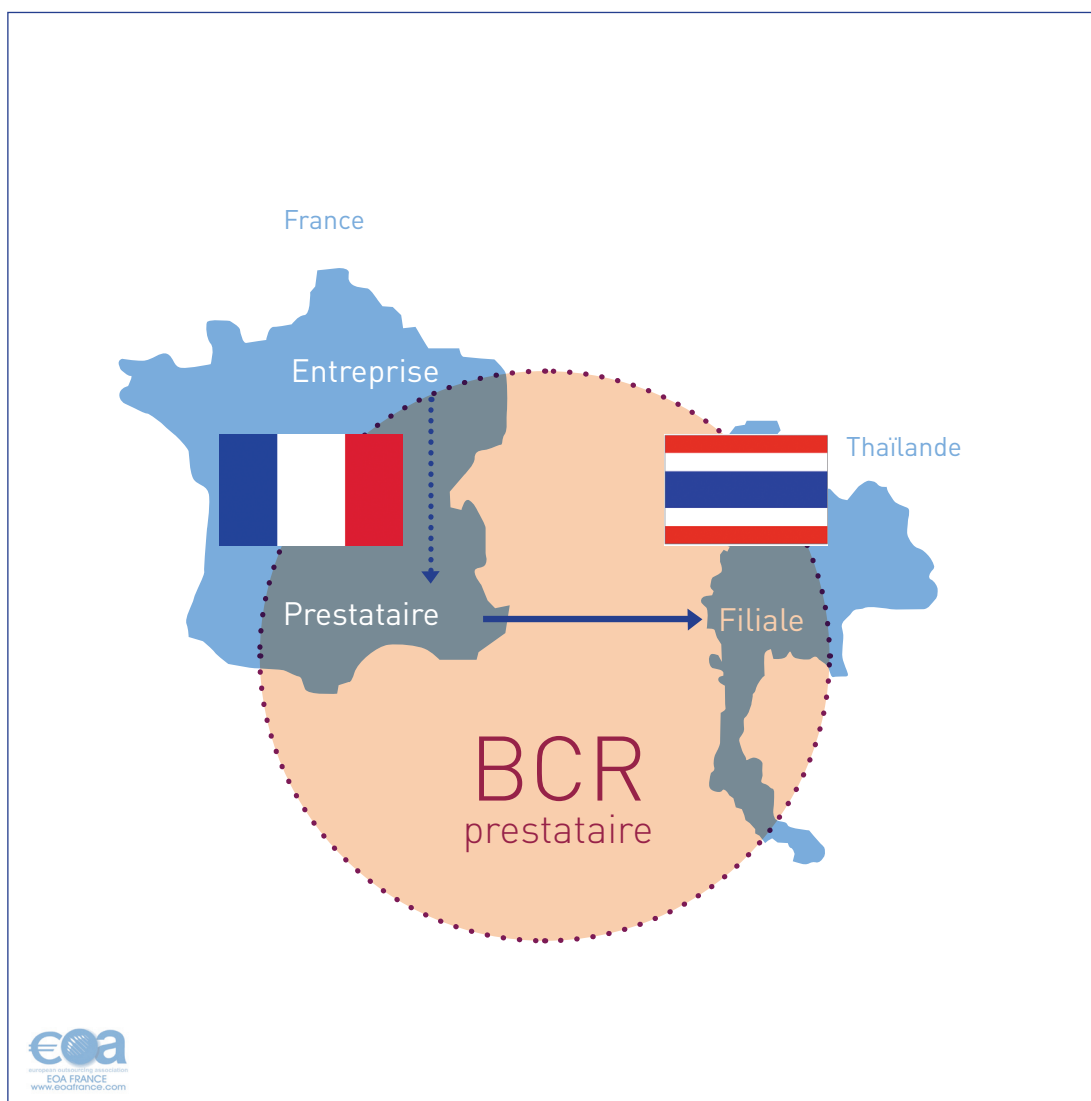
Dans un tel cas de figure, outre les solutions ci-dessus, la possibilité pour le prestataire de mettre en place, au niveau de son groupe, des BCR couvrant les transferts de données entre entreprises soumises au même contrôle (v. 2 ci-après), est susceptible de simplifier grandement les choses pour l'entreprise externalisatrice. De fait, plusieurs grands prestataires de services d'externalisation

ont entamé une démarche afin de mettre en place des BCR au sein de leur groupe.

1.2.3 L'attrait des BCR (Binding Corporate Rules)

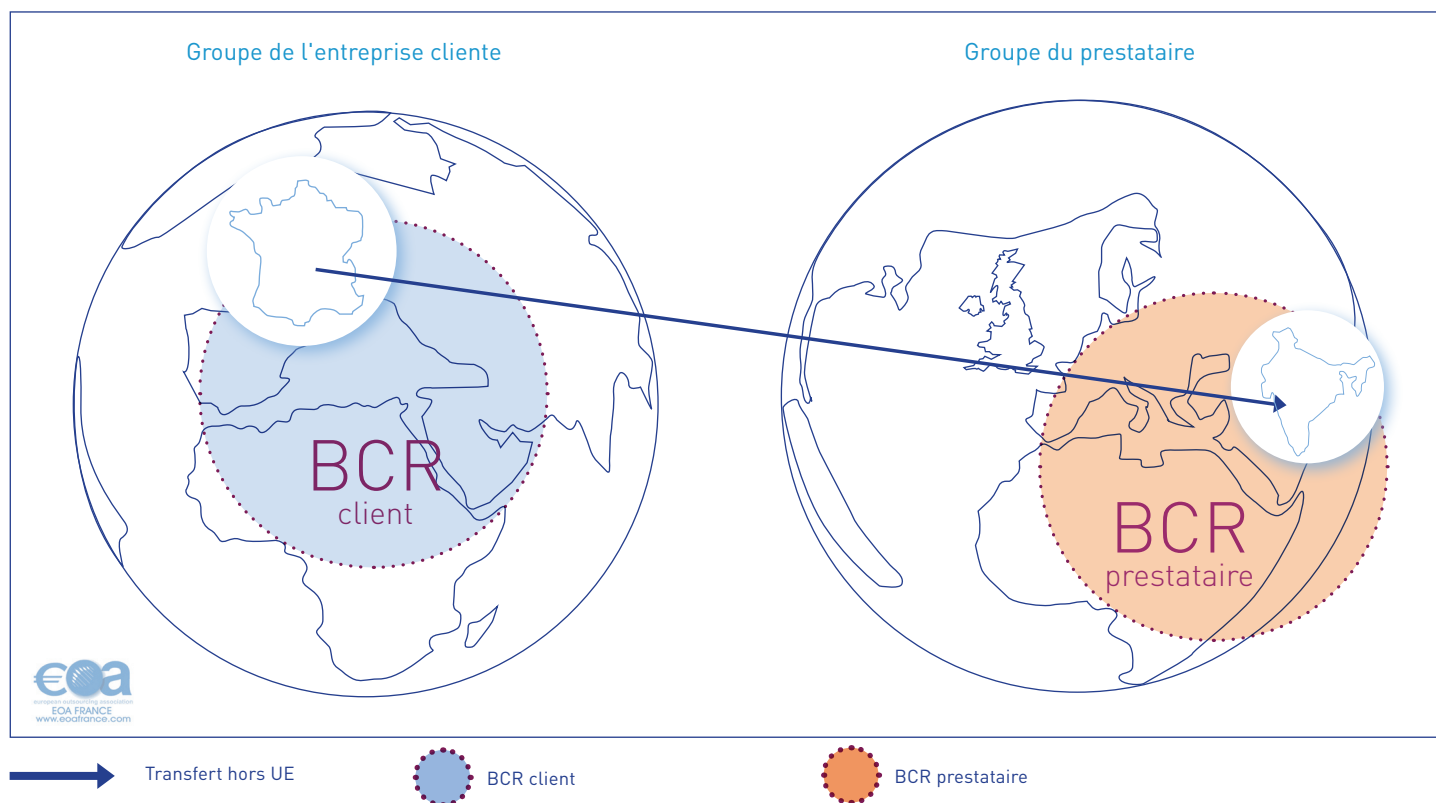
Le recours à un prestataire basé au sein de l'UE ou en dehors de l'UE et sous-traitant des prestations à ses filiales situées en dehors de l'UE peut être facilité si le prestataire fait partie d'un groupe ayant mis en place des Binding Corporate Rules (BCR).

Utilisation des BCR par le prestataire au sein de son groupe



- Transfert hors UE
- Transfert intra UE
- BCR prestataire

L'entreprise et son prestataire disposent de BCR



Les BCR¹⁴ correspondent à un code de conduite que se fixent toutes les sociétés d'un même groupe pour le traitement des données transférées au sein du groupe. Une fois élaborées, les BCR doivent être soumises à l'examen d'une autorité de protection des données de l'UE pour validation, afin d'être reconnues comme apportant un niveau de protection suffisant.

Dans le schéma le plus efficace ci-dessus, tant l'en-

treprise externalisatrice que le prestataire appartiennent à des groupes internationaux ayant mis en place des BCR: seuls les transferts initiaux de données entre les deux organisations sont alors à organiser, selon les modalités applicables et selon que ces transferts interviennent à l'intérieur de l'UE ou hors UE. Les transferts avals n'ont pas à être pris en compte car ils sont alors régis par les BCR du prestataire. ●

- On le constate, de nombreuses règles doivent être prises en compte et les situations à couvrir sont nombreuses et parfois complexes à bien traiter. Il est donc facile de commettre une erreur.
- Pour faciliter ce travail, le présent Livre Blanc propose une série de recommandations dont l'objet est de baliser, de manière chronologique, les différentes étapes d'un projet d'externalisation, en identifiant, pour chacune, les réflexes à avoir pour appliquer correctement les principes de protection des données à caractère personnel.

¹⁴ La rédaction des BCRs est régie par un ensemble de textes établis par le Groupe européen de l'article 29 (dit Groupe 29), et disponibles en ligne sur le site de la CNIL à l'adresse : <http://www.cnil.fr/vos-responsabilites/transferer-des-donnees-a-letranger/les-bcr/>

SECTION N°2

Recommandations pratiques : de la préparation de l'opération au contrat

Il résulte de l'enquête réalisée par l'EOA en octobre 2009, que 38 % des entreprises se préoccupent de la problématique liée au transfert hors UE de données personnelles au moment de la mise en œuvre du projet, c'est-à-dire après la signature du contrat avec le prestataire, ce qui est bien trop tard.

Si l'on ajoute à ce chiffre les 13 % d'entreprises pour lesquelles, de façon inquiétante, la question ne se pose jamais (!), un projet sur deux serait lancé, contrat signé et frais financiers engagés, alors pourtant qu'une composante essentielle du projet a été totalement ignorée.

Dans ces cas-là, la découverte tardive de la problématique des données personnelles va bien souvent considérablement retarder le projet et en renchérir le coût.

Ce constat est désolant, car appréhendée suffisamment en amont, la problématique liée au transfert de données personnelles hors UE ne présente au demeurant aucune difficulté particulière.

Il s'agit aujourd'hui d'une contrainte incontournable qui doit donc, en tant que telle, être prise en compte, de part et d'autre, par l'entreprise externalisatrice comme par son prestataire, le plus en amont possible et le plus sérieusement possible.

Il convient donc d'intégrer cette contrainte dans le calendrier projet dès le début de la préparation de l'opération d'externalisation.

2.1 Étude d'opportunité

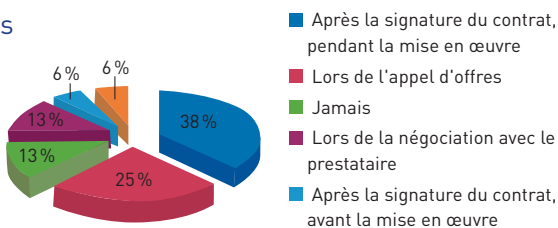
L'étude d'opportunité a pour objectif d'identifier les attentes de l'entreprise quant au projet offshore et d'en évaluer la pertinence, notamment en termes de rentabilité économique, au regard des contraintes associées. Elle permettra, ensuite, de rédiger un cahier des charges aussi fidèle que complet.

Parmi les contraintes, celle induite par les exigences de protection des données personnelles doit être envisagée. Or, pour correctement appréhender cette contrainte, il est nécessaire, dès cette phase, d'évaluer avec soin le degré de conformité existant au sein de l'entreprise à travers un rigoureux inventaire de l'existant.

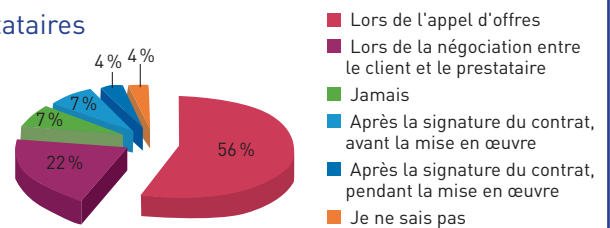
Il pourra être judicieux, pour l'entreprise qui n'est pas familière avec ces questions, de se faire conseiller, dès cette étape, par des avocats, pour les questions juridiques, et consultants, pour les aspects opérationnels, spécialisés dans ce domaine.

Quand se pose la question de la conformité ? Des perceptions contrastées

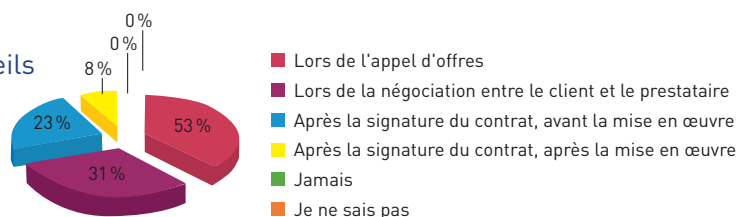
Clients



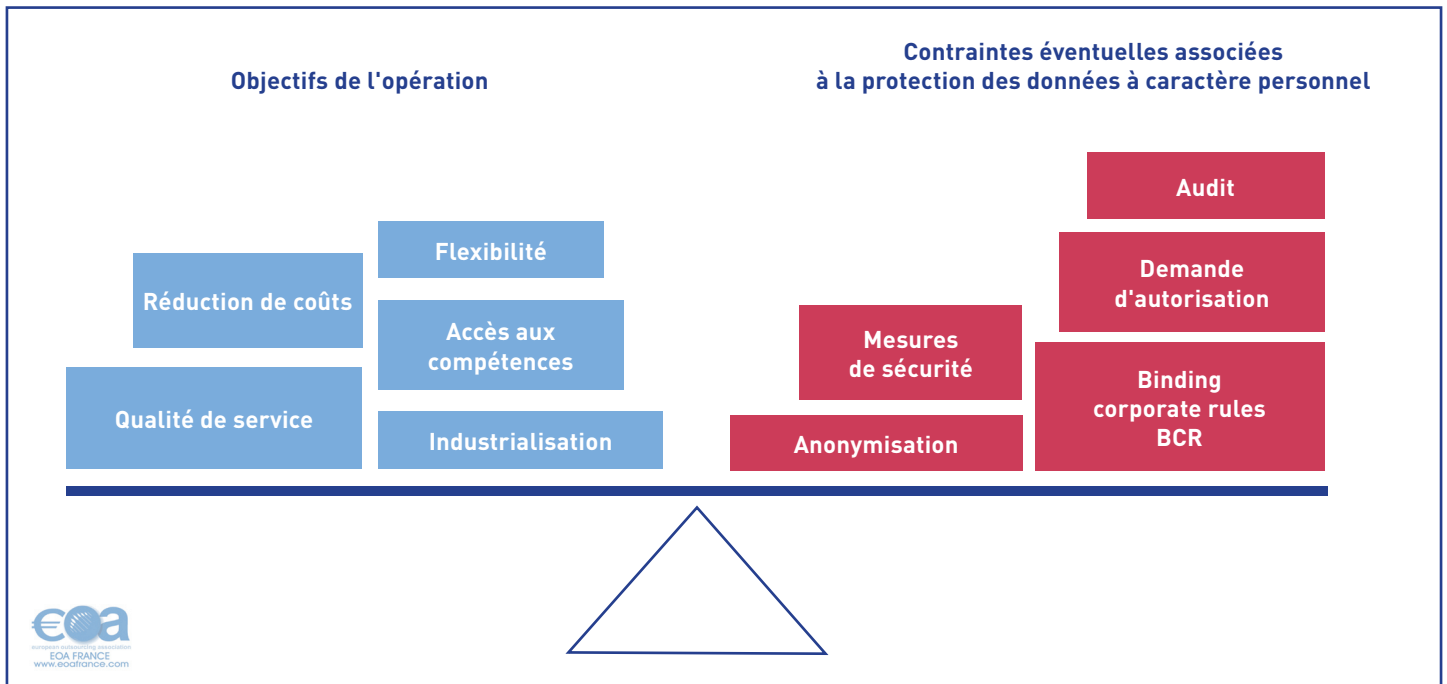
Prestataires



Conseils



Objectifs de l'externalisation versus contraintes



RECOMMANDATIONS

- 1. Réaliser un audit interne** de ses traitements de données personnelles potentiellement impactés par le projet, **en procédant à un recensement des traitements** par finalités (ressources humaines, paie, gestion client, etc.) et par flux au sein de l'entreprise. Il faut distinguer les données stratégiques à caractère personnel ou au contraire agrégées, des données dites « sensibles » au sens de la loi, car le régime de mise en conformité sera différent.
- 2. Établir sa conformité au regard de la Règlementation des Données Personnelles** en vérifiant notamment que les traitements ainsi identifiés ont bien été correctement déclarés auprès de la CNIL et en procédant, le cas échéant, aux régularisations requises (v. Section 1, §1.1.1). Attention ! la durée de délivrance des autorisations par la CNIL peut prendre entre un à six mois, selon la complexité du traitement.
- 3. Documenter soigneusement les processus internes de mise en conformité** (charte d'information, durée de conservation des documents, charte de sécurité des données, etc.) afin non seulement de pouvoir en justifier à la CNIL en cas de contrôle, mais aussi de rédiger le cahier des charges (v. §2.2) et de tenir ces documents à disposition du prestataire lors de la due diligence du prestataire (v. §2.4).

- 4. Évaluer la pertinence d'une solution d'anonymisation des données**, en mettant en balance la nécessité de transférer les données avec le coût de l'anonymisation.

2.2 Cahier des charges

La formalisation d'un cahier des charges est une étape fondamentale qui permet de transcrire et détailler les attentes de l'entreprise. Le cahier des charges doit adresser tous les aspects d'un projet d'externalisation et notamment énoncer les attentes en termes de protection des données personnelles et poser les questions sur lesquelles une réponse précise est attendue du prestataire.

- 5. Décrire précisément, dans un chapitre spécial « données personnelles », la nature et l'importance des données** à caractère personnel concernées par l'externalisation, identifier les traitements impactés et le statut de conformité de l'entreprise au regard de ses obligations. L'entreprise sera bien avisée de préciser dans ce chapitre les éventuelles spécificités induites par son activité sur le traitement des données personnelles (ex. dans le secteur bancaire ; ex. les données de santé, etc.).
- 6. Décrire la politique de sécurité** existante dans l'entreprise en identifiant, le cas échéant, les processus ou solutions mis en œuvre : nomination d'un CIL, recours au masquage ou anonymisation des données, traçabilité des données, logiciels anti-intrusion, etc. L'entreprise

demandera au prestataire de se situer par rapport à ces éléments, en indiquant si les moyens utilisés par le prestataire pour le traitement des données personnelles sont compatibles et d'un niveau supérieur, équivalent ou inférieur par rapport aux moyens mis en œuvre dans la politique de sécurité en vigueur.

7. Intégrer des questions visant à démontrer la maturité et le savoir faire du prestataire en matière de traitements de données personnelles (existence de BCR, politique vis-à-vis des sous-traitants...). Indiquer que les réponses du prestataire constitueront un critère d'évaluation et spécifier la pondération accordée à ce volet dans l'appréciation globale de la réponse du prestataire.

8. Prendre contact avec son Correspondant Informatique et Libertés (CIL)¹⁵ en interne (le cas échéant) et l'impliquer dans l'élaboration d'une stratégie de protection des données personnelles.

2.3 Réponse du prestataire

La réponse du prestataire soumissionnaire devra lui permettre de démontrer son degré de maturité sur les questions relatives au traitement des données personnelles et donc la robustesse de son offre, y compris sur ces aspects.

Cette composante de la réponse du prestataire soumissionnaire est déjà prise en compte de manière très détaillée et structurée dans le cadre de certains appels d'offres émis par l'État et sera amenée, dans les années à venir, à se développer toujours davantage dans les appels d'offres privés.

9. Proposer des solutions sur les processus de traitement des données et les moyens que le prestataire se propose de mettre en œuvre en matière de données personnelles, notamment en cas de sous-traitance.

¹⁵ Le CIL est une personne désignée volontairement par l'entreprise pour alléger les formalités de déclaration auprès de la CNIL et qui permet de veiller à la bonne application dans l'entreprise de la loi Informatique et Libertés. Voir le Guide de la CNIL ici : http://www.cnil.fr/fr/leadmin/documents/Guides_pratiques/CNIL_Guide_correspondants.pdf

10. Soulever la problématique des données personnelles si l'entreprise ne l'a pas déjà fait, relever d'autorité les problèmes potentiels susceptibles de se présenter et identifier les coûts éventuels ou les contraintes de planning pouvant résulter des problématiques identifiées.

11. Apporter expertise et conseil de manière proactive et faire part de son expérience dans le traitement de problématiques similaires.

2.4 Due diligence

Selon le type d'offshore, l'entreprise retiendra un ou plusieurs candidat(s). Le processus de sélection est une opportunité pour l'entreprise et les prestataires soumissionnaires d'apprendre à se connaître.

La phase de due diligence, ouverte aux finalistes, permettra à ceux-ci d'appréhender plus directement le contexte de l'entreprise, d'estimer leurs prises de risque et d'affiner leurs offres. Plus elle aura été préparée avec soin en amont par l'entreprise, moins cette étape sera longue et coûteuse.

12. Signer un accord de confidentialité, intégrant une clause « données personnelles » par laquelle le soumissionnaire accepte de ne traiter les données que pour les finalités de la due diligence.

13. Soulever les éventuelles non conformités et en évaluer les conséquences pour le client et le projet.

2.5 Choix du ou des prestataire(s) pressenti(s)

Il faudra à ce stade faire preuve de cohérence et ré- compenser, à travers un scoring adapté, les offres qui auront précisément appréhendé la dimension données personnelles et proposeront une solution et des processus adaptés et sécurisés.

- 14. Évaluer, et le cas échéant, auditer les solutions de sécurisation des données** proposées par le prestataire pour valider leur pertinence et leur faisabilité.

2.6 Négociation / signature du contrat

Le contrat devra documenter avec précision les options prises par les parties et les responsabilités de l'une et de l'autre en matière de données personnelles.

- 15. Insérer une clause « données personnelles » dans le contrat** : l'insertion de cette clause est obligatoire en vertu de la loi.¹⁶ Une clause d'audit des mesures de sécurité peut également être prévue par les parties.
- 16. Prévoir les moyens de sécuriser les transferts de données personnelles** : contrat de transfert de données basé sur les clauses types, BCR, consentement des personnes concernées, Safe Harbor, etc. (v. Section 1).
- 17. Prévoir les moyens techniques du droit d'accès** : l'entreprise cliente est légalement obligée de répondre à une demande de droit d'accès des personnes concernées. Pour cela, le client doit se ménager l'assistance du sous-traitant, par exemple en mettant en place une fonctionnalité spécifique, ou des procédures internes appropriées.
- 18. Décrire les mesures de sécurité à prendre et les mécanismes d'alerte** en cas d'incidents dans une annexe au contrat : les mesures de sécurité couvriront notamment (i) la protection physique des locaux, la gestion des accès des personnels aux locaux, le contrôle d'accès aux données, les mesures de confidentialité appliquées aux

personnels, les mécanismes techniques de stockage, de sauvegarde et de transfert des données, etc. et, (ii) les mécanismes d'information de l'entreprise cliente sur les manquements, violations d'accès ou incidents techniques identifiés.

- 19. Envisager des niveaux de services spécifiques** applicables aux données personnelles.
- 20. Prévoir un suivi de la montée en compétences des équipes** du prestataire sur les mesures de protection des données personnelles dans le cadre de la transition : la formation des équipes des prestataires est un des éléments clés à suivre pendant la transition. Elle pourra constituer l'un des référentiels permettant de passer en service récurrent.
- 21. Clarifier les rôles et responsabilités et les formaliser via l'utilisation d'une matrice** : les mesures de contrôle et de gestion des données à caractère personnel sont mises en œuvre par des acteurs clairement identifiés dont les types de rôles sont : en charge de l'action, en charge de la validation, contributeur.
- 22. Mettre en place la gouvernance adaptée** pour permettre un suivi effectif de la conformité des données personnelles et une réactivité immédiate en cas de problème.
- 23. Préparer toutes les déclarations et documents pour la CNIL.** Éventuellement préparer des schémas de flux internationaux de données.
- 24. En cas de difficulté importante contacter la CNIL.** ●

¹⁶ Article 35 de la loi Informatique et Libertés.

SECTION N°3

Recommandations pratiques : la phase de mise en œuvre

3.1 La transition

La transition est le processus qui permet de faire reprendre la fourniture du service à iso périmètre par le prestataire. Ce processus est piloté par un plan de transition, véritable recueil méthodologique de l'opération. La fin du processus de transition marque le véritable transfert de responsabilité du client au prestataire.

25. Intégrer dans le plan de transition, le cas échéant, la mise en conformité du traitement de données de l'entreprise (si cela n'a pas été fait en amont) avant transfert des données.

26. Effectuer la ou les demande(s) d'autorisation auprès de la CNIL et obtenir l'autorisation avant de transférer ses données offshore. C'est à l'entreprise que revient la responsabilité de réaliser les formalités préalables et obligatoires auprès de la CNIL et de sécuriser juridiquement les transferts de données par des mesures adéquates. Le récépissé d'autorisation de la CNIL doit être obtenu avant de transférer les données.

27. Mettre en œuvre des mesures de sécurité proportionnelles à la sensibilité des données. Il importera notamment :

- de mettre en place un **Plan d'Assurance Sécurité (PAS)**, s'appuyant sur un référentiel de sûreté de l'information, ainsi que sur les référentiels de sécurité issus des normes et standards reconnus (ISO 27001, ISO 27002, etc.) ;
- d'adapter la sécurité aux types de données (bancaire, santé, etc.) et donc définir des niveaux de sécurité ;
- de mettre en place les moyens de sécuriser les transferts de données (v. Section 1) ;
- de former et sensibiliser les équipes internes de l'entreprise et du prestataire sur les mesures de protection des données.

28. Avant le passage en mode stabilisé, effectuer une revue des mesures prises sur la base des prescriptions du PAS pour s'assurer que les risques sont levés et que la conformité est effective.

3.2 La transformation

La transformation regroupe les différents axes de massification correspondant aux objectifs de réduction des coûts (mutualisation, localisation) et de gain de productivité (gouvernance, industrialisation).

L'entreprise cliente demeure le responsable légal de la sécurité des données, en tant que c'est elle qui fixe les finalités des traitements et les moyens mis en œuvre. Toutefois, si le prestataire transforme ces moyens de traitement dans le cadre de la transformation, il doit en informer l'entreprise cliente de manière transparente afin de lui donner les moyens d'assumer ses responsabilités. A défaut, le prestataire risquerait d'endosser lui-même la qualité de responsable du traitement, et les responsabilités associées.

Toute modification substantielle des traitements doit faire l'objet d'une modification de la déclaration CNIL (en envoyant une lettre ou une déclaration modificative du traitement, selon les cas) et du contrat de transfert de données si les transferts sont modifiés (par exemple changement ou recours à un sous-sous-traitant). Éventuellement, la modification doit être notifiée aux personnes concernées et au Comité d'entreprise.

Dès lors, il reviendra au prestataire, s'il est l'initiateur de cette modification, d'alerter l'entreprise cliente, responsable de traitement.

29. Suivre avec attention toute modification des moyens de traitement affectant les données personnelles (par exemple le recours à un sous-sous-traitant non prévu dans le contrat initial) pour qu'elle puisse mettre à jour ses déclarations CNIL, et informer l'entreprise cliente préalablement à leur mise en œuvre.

30. Adapter, au fil de l'eau, les déclarations CNIL et autorisations obtenues en fonction des évolutions des moyens de traitement de façon à toujours conserver une parfaite conformité de l'ensemble.

31. Adapter le PAS et le rendre cohérent avec le processus interne du prestataire.

3.3 Mode stabilisé ou récurrent

Il s'agit du mode de fonctionnement dans le dispositif opérationnel nominal, avec engagement complet sur les niveaux de services contractuels et application d'un éventuel système de pénalité.

32. Effectuer, de part et d'autre, des revues régulières des mesures de sécurité et suivre, le cas échéant, les indicateurs spécifiques définis pour les données personnelles et les niveaux de service effectifs

33. Traiter avec diligence les problèmes liés aux données à caractère personnel, dans le cadre des instances de gouvernance, et en investiguer la cause.

34. Mettre à jour le PAQ / PAS pour adapter les mesures si nécessaire.

35. Réaliser des audits afin de vérifier le respect des mesures de sécurité mises en œuvre par le prestataire.

36. Intégrer la dimension protection des données personnelles dans le plan de réversibilité pour assurer son application dans le cadre du processus de réversibilité. Ce plan doit être mis à jour continuellement pendant toute la durée du contrat par le prestataire et doit être livré annuellement ou sur demande du client.

3.4 Déclenchement de la réversibilité

La réversibilité est un processus qui permet de faire reprendre la responsabilité opérationnelle d'une

prestation par celui qui reprend la fourniture du service (équipe interne du client ou équipe d'un autre prestataire). A ce processus est associé un plan de réversibilité qui en constitue le recueil méthodologique. La fin du processus de réversibilité implique l'arrêt de la prestation transférée : substitution des équipes, transfert de responsabilité de la fourniture du service, changement de locaux, restitution et destruction des données à caractère personnel...

Attention ! Le client doit vérifier sa conformité à la loi Informatique et Libertés avant la mise en œuvre de la réversibilité car en cas de non conformité le client devra attendre les autorisations adéquates de la CNIL, qui peuvent prendre jusqu'à 6 mois.

37. Mettre à jour et exécuter un plan de réinternalisation ou de transfert à un tiers des données à caractère personnel. Le prestataire restituera au client ou à un tiers désigné par le client, l'ensemble des données à caractère personnel traité dans le cadre de la gérance. Cette remise donnera lieu à l'établissement d'un procès-verbal par les deux parties. Le prestataire détruira l'ensemble des copies des données à caractère personnel encore présent sur ses systèmes informatiques après ladite restitution, et en certifiera la destruction effective. Le Plan précisera les modalités de restitution et de destruction des données à caractère personnel.

38. Mettre à jour les demandes d'autorisation et les contrats de transferts.

39. Dans le cas d'un changement de prestataire, mettre en place une gouvernance tri-partite au sein de laquelle le sujet des données à caractère personnel sera suivi.

40. En fin de réversibilité, faire un audit des installations du prestataire sortant pour s'assurer que toutes les données à caractère personnel ont été détruites (prévoir l'obligation d'établir un certificat). ●

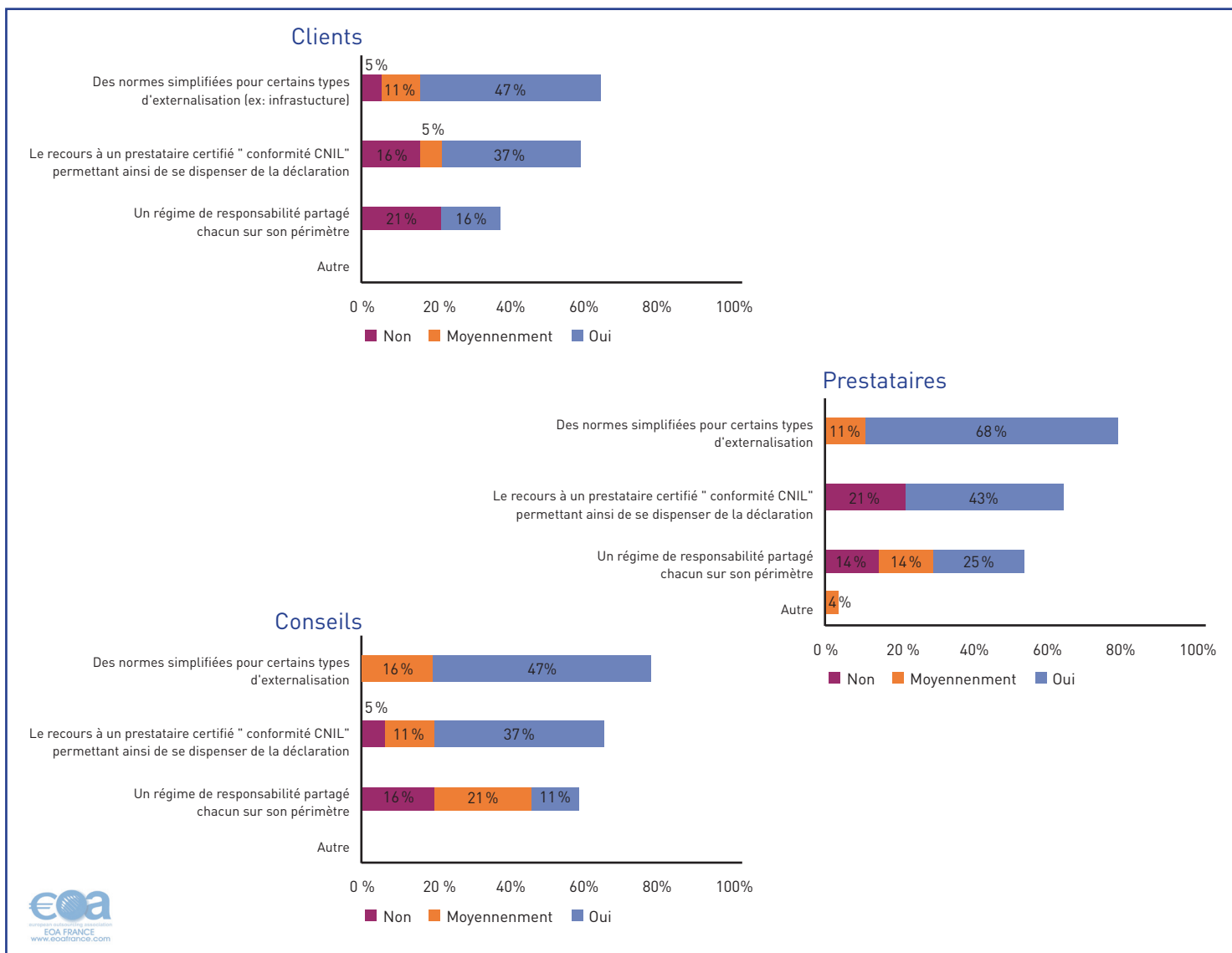
SECTION N°4

Souhaits d'évolution

La rédaction de ce Livre Blanc a permis à l'EOA France de dégager certains souhaits d'évolution, qui permettraient aux acteurs de l'externalisation de faciliter la réalisation du volet données personnelles

d'un projet d'externalisation offshore. L'enquête d'octobre 2009 avait déjà permis d'identifier les premières pistes d'évolutions souhaitées par les acteurs de l'externalisation :

Souhaits d'évolution exprimés lors de l'enquête EOA France



A partir de cette orientation initiale, l'EOA France a mené une réflexion sur cette question et formule à son tour les souhaits d'évolution suivants :

4.1 La reconnaissance d'un statut légal du prestataire

A côté du statut légal de responsable de traitement, il semblerait opportun de définir dans la loi le statut du prestataire. En effet, il a été constaté que constitue une source d'incertitude et de flou, l'absence de définition légale précise (i) des critères permettant de qualifier une entreprise comme prestataire et (ii) des obligations à sa charge. L'enquête réalisée par l'EOA a notamment montré que les acteurs de l'externalisation ont une perception divergente de leurs responsabilités respectives (v. schéma p.9).

Chaque partie bénéficierait d'avoir un statut légal clairement identifié, la responsabilisant sur la partie du traitement sous son contrôle effectif.

Il semblerait que cette préoccupation soit partagée par la CNIL, qui a indiqué étudier l'opportunité de créer un statut légal pour le sous-traitant.

4.2 Un allègement des formalités déclaratives

Fort du constat que les entreprises qui externalisent le font souvent sans s'être acquittées de leurs obligations déclaratives, l'EOA France souhaite la simplification des formalités déclaratives. A cet effet, deux solutions sont envisageables :

- La mise en place d'une norme simplifiée spécifique à l'externalisation : cette norme définirait, à l'instar des normes existantes, les finalités, catégories de destinataires, catégories de données, mesures de sécurité, délais de conservation et conditions de transfert devant être respectées pour bénéficier de l'application de cette norme simplifiée. Ces informations pourraient être simplifiées dans l'hypothèse où l'entreprise a déjà procédé à des formalités déclaratives selon les normes n° 46 (relative à la gestion du personnel) et n° 48 (fichiers clients et prospects) et que ces conditions de traitement sont maintenues dans le cadre de l'externalisation. Dans un tel cas la seule référence à ces normes et la confirmation que les prestataires en charge de l'externalisation les respectent devrait suffire. Les conditions de transfert devront être explicitées dans le cadre d'une annexe transfert simplifiée, le recours à des contrats de transferts de données non modifiés selon le

modèle de la Commission Européenne ou le recours à des BCRs devant suffire pour considérer l'entreprise comme étant en conformité. Cette proposition ambitieuse aurait le mérite de rationaliser les démarches « informatique et liberté » de l'entreprise en couvrant, par une seule déclaration, toutes les finalités des traitements de données habituellement externalisés, notamment les données clients et salariés.

- L'autre possibilité rejoint celle envisagée par la CNIL dans son avis sur « les questions posées pour la protection des données personnelles par l'externalisation hors de l'UE des traitements informatiques », à savoir une révision des normes n°46 et n°48 pour tenir compte des opérations d'externalisation. Cette solution nous semble néanmoins ne pas totalement répondre à l'objectif de simplification et de rationalisation recherché car elle ne prend pas en compte la possibilité pour le prestataire d'être parfois « responsable de traitement ». En outre, elle oblige l'entreprise à déposer une déclaration par finalité de traitement, alors qu'un projet d'externalisation peut couvrir plusieurs finalités à la fois.

4.3 La labellisation par la CNIL des systèmes informatiques et logiciels

Depuis l'entrée en vigueur de la loi du 12 mai 2009 de simplification et de clarification du droit, la CNIL dispose d'un pouvoir effectif de labellisation. Si la CNIL entend privilégier d'abord la labellisation des audits et formations « informatique et libertés », elle prévoit ensuite de mettre en œuvre un processus de labellisation des systèmes informatiques et logiciels. Cette labellisation pourrait s'appliquer aux systèmes informatiques et logiciels utilisés dans le cadre d'un projet d'externalisation, ce qui permettrait de garantir la protection des données dans le cadre de tels projets et de faciliter ainsi les démarches déclaratives auprès de la CNIL.

4.4 L'adoption de BCR par les prestataires

Il s'agit ici d'une évolution des pratiques actuelles que l'EOA France entend encourager. Les BCR s'avèrent utiles dans le cas d'une externalisation au sein d'un même groupe de sociétés. De plus, la CNIL étudie la possibilité pour les prestataires d'adopter des BCR permettant de sécuriser les transferts de données au sein de leurs organisations, y compris pour les transferts de données de leurs clients. ●

TABLEAU RÉCAPITULATIF

Tableau récapitulatif des recommandations de l'EOA France en matière de protection des données à caractère personnel dans le cadre de projets offshore

RECOMMANDATIONS	CLIENT	PRESTATAIRE
ÉTUDE D'OPPORTUNITÉ		
1. Réaliser un audit interne en procédant à un recensement des traitements	<input checked="" type="radio"/>	<input type="radio"/>
2. Établir sa conformité au regard de la Règlementation des Données Personnelles	<input checked="" type="radio"/>	<input type="radio"/>
3. Documenter soigneusement les processus internes de mise en conformité	<input checked="" type="radio"/>	<input type="radio"/>
4. Évaluer la pertinence d'une solution d'anonymisation des données	<input checked="" type="radio"/>	<input type="radio"/>
CAHIER DES CHARGES		
5. Décrire précisément, dans un chapitre spécial « données personnelles » la nature et l'importance des données	<input checked="" type="radio"/>	<input type="radio"/>
6. Décrire la politique de sécurité	<input checked="" type="radio"/>	<input type="radio"/>
7. Intégrer des questions visant à démontrer la maturité et le savoir faire du prestataire	<input checked="" type="radio"/>	<input type="radio"/>
8. Prendre contact avec son Correspondant Informatique et Libertés (CIL)	<input checked="" type="radio"/>	<input type="radio"/>
RÉPONSE DU PRESTATAIRE		
9. Proposer des solutions sur les processus	<input type="radio"/>	<input checked="" type="radio"/>
10. Soulever la problématique des données personnelles	<input type="radio"/>	<input checked="" type="radio"/>
11. Apporter expertise et conseil	<input type="radio"/>	<input checked="" type="radio"/>

RECOMMANDATIONS	CLIENT	PRESTATAIRE
DUE DILIGENCE		
12. Signer un accord de confidentialité, intégrant une clause « données personnelles »	<input checked="" type="radio"/>	<input checked="" type="radio"/>
13. Soulever les éventuelles non conformités et en évaluer les conséquences pour le client	<input type="radio"/>	<input checked="" type="radio"/>
CHOIX DU OU DES PRESTATAIRE(S) PRESSENTI(S)		
14. Évaluer, et le cas échéant, auditer les solutions de sécurisation des données	<input checked="" type="radio"/>	<input type="radio"/>
NÉGOCIATION / SIGNATURE DU CONTRAT		
15. Insérer une clause « données personnelles » dans le contrat	<input checked="" type="radio"/>	<input checked="" type="radio"/>
16. Prévoir les moyens de sécuriser les transferts de données personnelles	<input checked="" type="radio"/>	<input checked="" type="radio"/>
17. Prévoir les moyens techniques du droit d'accès	<input type="radio"/>	<input checked="" type="radio"/>
18. Décrire les mesures de sécurité à prendre et les mécanismes d'alerte	<input checked="" type="radio"/>	<input checked="" type="radio"/>
19. Envisager des niveaux de services spécifiques	<input checked="" type="radio"/>	<input checked="" type="radio"/>
20. Prévoir un suivi de la montée en compétences des équipes	<input type="radio"/>	<input checked="" type="radio"/>
21. Clarifier les rôles et responsabilités et les formaliser via l'utilisation d'une matrice	<input checked="" type="radio"/>	<input checked="" type="radio"/>
22. Mettre en place la gouvernance adaptée	<input checked="" type="radio"/>	<input checked="" type="radio"/>
23. Préparer toutes les déclarations et documents pour la CNIL.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
24. En cas de difficulté importante contacter la CNIL	<input checked="" type="radio"/>	<input checked="" type="radio"/>
LA TRANSITION		
25. Intégrer dans le plan de transition la mise en conformité	<input type="radio"/>	<input checked="" type="radio"/>
26. Effectuer la ou les demande(s) d'autorisation auprès de la CNIL et obtenir l'autorisation	<input checked="" type="radio"/>	<input checked="" type="radio"/>
27. Mettre en œuvre des mesures de sécurité proportionnelles à la sensibilité des données	<input checked="" type="radio"/>	<input checked="" type="radio"/>
28. Avant le passage en mode stabilisé, effectuer une revue des mesures prises	<input type="radio"/>	<input checked="" type="radio"/>

TABLEAU RÉCAPITULATIF

(suite)

RECOMMANDATIONS	CLIENT	PRESTATAIRE
LA TRANSFORMATION		
29. Suivre avec attention toute modification des moyens de traitement	●	●
30. Adapter, au fil de l'eau, les déclarations CNIL et autorisations obtenues	●	●
31. Adapter le PAS	○	●
MODE STABILISÉ OU RÉCURRENT		
32. Effectuer, de part et d'autre, des revues régulières	●	●
33. Traiter avec diligence les problèmes liés aux données à caractère personnel	●	●
34. Mettre à jour le PAQ / PAS	○	●
35. Réaliser des audits afin de vérifier le respect des mesures de sécurité	●	○
36. Intégrer la dimension protection des données personnelles dans le plan de réversibilité	○	●
DÉCLENCHEMENT DE LA RÉVERSIBILITÉ		
37. Mettre à jour et exécuter un plan de ré-internalisation ou de transfert à un tiers	○	●
38. Mettre à jour les demandes d'autorisation	●	○
39. Dans le cas d'un changement de prestataire, mettre en place une gouvernance tri-partite	●	●
40. En fin de réversibilité, faire un audit des installations du prestataire sortant	●	○

REMERCIEMENTS

Ce Livre Blanc a vu le jour grâce à la motivation et la participation des membres de la commission juridique de l'EOA, et notamment

• **JEAN-CLAUDE BARRIER,**
IT Operations Director,
Bombardier Transportation

• **DAVID CHARLOT,**
Juriste, Baker & McKenzie Paris

• **LAURENCE DEGHAÏE,**
Juriste, Stéria

• **FLORE DION,**
Responsable Business Development et Marketing,
Baker & McKenzie Paris

• **FRANÇOIS GOUBLET,**
Consultant indépendant

• **GLORIA HOWA,**
Juriste, HR Access Solutions

• **DENISE LEBEAU-MARIANNA,**
Avocat, Local Partner, Baker & McKenzie Paris

• **FLORIANE MANGENOT,**
Juriste, Systèmes d'Informations Critiques, Thalès

• **MARIE-HÉLÈNE MANSARD,**
Directeur du Marketing et de la Communication,
Systèmes d'Informations Critiques, Thales

• **EMMANUELLE MUNIER,**
Directeur Juridique,
Systèmes d'Informations Critiques, Thales

• **JONATHAN ROFE,**
Avocat, Bird & Bird

• **LAURENT MICHON,**
Contract manager, Atos Origin Infogérance

• **JEAN-MICHEL PÉTIN,**
Directeur Associé, Nitep Consultants

• **NICOLAS QUOY,**
Avocat, Local Partner, Baker & McKenzie Paris

• **CHRISTOPHER SOARES,**
Senior Manager, Ineum Consulting

Je les en remercie vivement

RÉMY BRICARD,
Avocat Associé, Baker & McKenzie Paris,
Président de la Commission Juridique, EOA France



EOA France
10 rue de la Paix
75002 Paris

www.eoafrance.com