GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

01037/12/FR
WP 196

Avis 05/2012 sur l'informatique en nuage

Adopté le 1er juillet 2012

Résumé

Le présent avis du groupe de travail «article 29» analyse toutes les questions intéressant les fournisseurs de services d'informatique en nuage qui exercent leurs activités dans l'espace économique européen (EEE) ainsi que leurs clients, en précisant, lorsque c'est utile, tous les principes applicables tirés de la directive de l'UE relative à la protection des données (95/46/CE) et de la directive «vie privée et communications électroniques» 2002/58/CE (modifiée par la directive 2009/136/CE).

Tout en reconnaissant les avantages indéniables que l'informatique en nuage présente pour l'économie et la société, le présent avis décrit comment son utilisation généralisée peut créer un certain nombre de risques pour la protection des données, tenant principalement à une absence de contrôle sur les données à caractère personnel et à une information insuffisante sur le mode et le lieu du traitement ou du sous-traitement des données et sur la ou les personnes qui les réalisent. Ces risques doivent être soigneusement évalués par les organismes publics et les entreprises privées qui envisagent de recourir aux services d'un fournisseur d'informatique en nuage. Le présent avis examine les questions liées au partage de ressources avec des tiers, au manque de transparence que comporte une chaîne d'externalisation composée de multiples sous-traitants, à l'absence de cadre commun mondial régissant la portabilité des données, et à l'incertitude qui entoure l'admissibilité du transfert des données à caractère personnel aux fournisseurs d'informatique en nuage établis en dehors de l'EEE. De la même façon, il souligne les graves préoccupations que suscite le manque de transparence des informations qu'un responsable du traitement doit être en mesure de présenter à une personne concernée sur la manière dont ses données à caractère personnel sont traitées. Les personnes concernées doivent[1] savoir qui traite leurs données et à quelles fins, pour être en mesure d'exercer les droits qui leur sont conférés à cet égard.

L'une des principales conclusions tirées par le présent avis est que les entreprises et les administrations qui souhaitent recourir à l'informatique en nuage devraient, dans un premier temps, procéder à une analyse de risques rigoureuse et exhaustive. Tous les fournisseurs d'informatique en nuage qui offrent des services dans l'EEE devraient communiquer à leurs clients toutes les informations qui leur sont nécessaires pour évaluer correctement les avantages et les inconvénients d'un tel service. La sécurité, la transparence et la sécurité juridique des clients devraient occuper une place essentielle dans l'offre de services d'informatique en nuage.

Les recommandations formulées dans le présent avis mettent en lumière les obligations incombant au client lorsqu'il est responsable du traitement, l'une d'elles étant de choisir un fournisseur d'informatique en nuage qui garantisse le respect de la législation européenne sur la protection des données. En ce qui concerne les garanties contractuelles appropriées, le présent avis exige que tout contrat entre un fournisseur d'informatique en nuage et son client offre des garanties suffisantes en matière de mesures techniques et

[1] «DOIT», «NE DOIT PAS», «REQUIS», «SERA», «NE SERA PAS», «DEVRAIT», "NE DEVRAIT PAS», «RECOMMANDÉ», «PEUT», et «FACULTATIF» figurant dans ce document doivent être interprétés conformément au sens qui leur est donné dans la demande de commentaires n° 2119, consultable à l'adresse: http://www.ietf.org/rfc/rfc2119.txt. Toutefois, dans un souci de lisibilité, ces mots n'apparaissent pas en majuscules dans le présent avis.

organisationnelles. Il importe également que le client vérifie si son fournisseur peut garantir la légalité des transferts internationaux de données.

Comme tout processus d'évolution, l'élévation de l'informatique en nuage au rang de modèle technologique mondial constitue un défi. Dans sa version actuelle, le présent avis peut être considéré comme une étape importante dans la définition des missions à remplir à cet égard par les instances chargées de la protection des données dans les années à venir.

Table des matières

1. Introduction

Certains voient dans l'informatique en nuage l'une des plus grandes révolutions technologiques de ces dernières années. Pour d'autres, elle ne constitue que l'évolution naturelle d'une série de technologies menant à l'informatique à la demande, longtemps attendue. Quoi qu'il en soit, nombre de parties prenantes ont accordé une place centrale à l'informatique en nuage dans le développement de leurs stratégies technologiques.

L'informatique en nuage réunit un ensemble de technologies et de modèles de services dans lesquels l'utilisation et la livraison d'applications informatiques, la capacité de traitement, le stockage et l'espace mémoire reposent tous sur l'internet. Elle peut générer des avantages économiques considérables, sachant que les ressources à la demande sont faciles à configurer et à développer sur l'internet, où elles sont par ailleurs aisément accessibles. En outre, l'informatique en nuage peut également présenter des avantages du point de vue de la sécurité; les entreprises, notamment les petites et moyennes entreprises, peuvent ainsi acquérir, à un coût marginal, des technologies de haut niveau qui normalement dépasseraient leur budget.

Les fournisseurs d'informatique en nuage offrent toute une gamme de services, allant des systèmes de traitement de données à mémoire virtuelle (qui remplacent et/ou fonctionnent conjointement avec les serveurs classiques sous le contrôle direct du responsable du traitement) aux services à l'appui du développement d'applications et aux services d'hébergement avancé, en passant par des solutions de logiciel en ligne qui peuvent remplacer les applications traditionnellement installées sur les ordinateurs personnels des utilisateurs finals. Il peut s'agir d'applications de traitement de texte, d'agendas et de calendriers, de systèmes de classement pour le stockage de documents en ligne ainsi que de solutions de messagerie externalisée. L'annexe du présent avis contient quelques-unes des définitions les plus communément utilisées pour ces différents types de services.

Le présent avis du groupe de travail «article 29» (ci-après le «GT article 29») examine le droit applicable aux responsables du traitement dans l'Espace économique européen (ci-après «l'EEE») et aux fournisseurs de services en nuage qui ont des clients dans l'EEE, ainsi que leurs obligations respectives. Il se penche plus particulièrement sur la relation entre responsable du traitement et sous-traitant, le client ayant la qualité de responsable du traitement et le fournisseur, celle de sous-traitant. Lorsque le fournisseur d'informatique en nuage intervient également en qualité de responsable du traitement, il doit satisfaire à des exigences supplémentaires. Ainsi, s'il souhaite recourir à des solutions d'informatique en nuage, le responsable du traitement doit au préalable procéder à une évaluation appropriée des risques, prenant en considération les lieux où se situent les serveurs sur lesquels les données sont traitées ainsi que les risques et les avantages du point de vue de la protection des données, conformément aux critères indiqués dans les paragraphes ci-dessous.

Le présent avis précise les principes de la directive générale sur la protection des données (95/46/CE) qui s'appliquent aux responsables du traitement et aux sous-traitants, tels que la spécification et la limitation des finalités, l'effacement des données, et les mesures techniques et organisationnelles. Il donne des orientations en ce qui concerne les exigences de sécurité, envisagées comme des garanties structurelles et procédurales. À cet égard, il insiste particulièrement sur les dispositions contractuelles qui devraient régir la relation entre un responsable du traitement et un sous-traitant. Les objectifs traditionnels de la sécurité des données sont la disponibilité, l'intégrité et la confidentialité. Toutefois, la protection des

données ne se limitant pas à leur sécurité, des objectifs spécifiques sont ajoutés, à savoir la transparence, la séparation, la possibilité d'intervention et la portabilité, pour donner corps au droit des citoyens à la protection des données, consacré à l'article 8 de la Charte des droits fondamentaux de l'Union.

S'agissant des transferts de données à caractère personnel en dehors de l'EEE, le présent avis examine divers instruments, comme les clauses contractuelles types adoptées par la Commission européenne, les constatations du niveau de protection adéquat des données, et les éventuelles futures règles d'entreprises contraignantes imposées aux sous-traitants, sans oublier les risques pour la protection des données découlant des demandes adressées par les services répressifs dans le cadre international.

Pour conclure, des recommandations sont formulées à l'intention des clients en leur qualité de responsables du traitement, des fournisseurs en leur qualité de sous-traitants, et de la Commission européenne pour ce qui concerne les modifications apportées à l'avenir au cadre européen régissant la protection des données.

Le Groupe de Berlin (groupe de travail international sur la protection des données dans les télécommunications) a adopté le *mémorandum de Sopot*[2] en avril 2012. Ce dernier examine les questions liées à la protection de la vie privée et des données à caractère personnel dans le domaine de l'informatique en nuage, en insistant sur le fait que celle-ci ne doit pas conduire à un affaiblissement des normes de protection des données par rapport au traitement conventionnel des données.

2. Les risques de l'informatique en nuage pour la protection des données

Le présent avis portant pour l'essentiel sur les opérations de traitement de données à caractère personnel déployant des services d'informatique en nuage, seuls sont examinés les risques spécifiques liés à ce contexte[3]. Ces risques relèvent dans leur grande majorité de deux grandes catégories, à savoir l'absence de contrôle sur les données et l'insuffisance des renseignements relatifs aux opérations de transformation proprement dites (absence de transparence). On retiendra, parmi les risques spécifiques liés à l'informatique en nuage examinés dans le présent avis:

L'absence de contrôle

> En confiant leurs données à caractère personnel à des systèmes gérés par des fournisseurs d'informatique en nuage, les clients pourraient perdre le contrôle exclusif de ces données et être privés de la capacité de déployer les mesures techniques et organisationnelles nécessaires pour garantir la disponibilité, l'intégrité, la confidentialité, la transparence, la séparation[4] et la portabilité des données, ainsi que la possibilité d'intervention. Cette absence de contrôle peut se manifester de la façon suivante:

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 Outre les risques liés aux données personnelles traitées «dans le nuage» expressément mentionnés dans le présent avis, tous les risques liés à l'externalisation du traitement des données personnelles doivent aussi être pris en compte.

4 En Allemagne, le concept plus général d'«indissociabilité» a été introduit. Voir infra la note de bas de page 24.

- Manque de disponibilité dû à un manque d'interopérabilité (dépendance vis-à-vis du fournisseur): lorsque le fournisseur d'informatique en nuage utilise une technologie propriétaire, il peut s'avérer difficile pour un client de déplacer des données ou des documents d'un système d'informatique en nuage à un autre (portabilité des données) ou d'échanger des informations avec des entités qui utilisent des services d'informatique en nuage gérés par plusieurs fournisseurs (interopérabilité).
- Manque d'intégrité causé par le partage des ressources: un nuage se compose de systèmes et d'infrastructures partagés. Les données à caractère personnel traitées par les fournisseurs d'informatique en nuage provenant d'une grande variété de sources, qu'il s'agisse des personnes concernées ou des organisations, des intérêts contradictoires et/ou des objectifs divergents peuvent naître.
- Manque de confidentialité concernant les demandes adressées par les services répressifs directement aux fournisseurs d'informatique en nuage: les données à caractère personnel traitées dans le nuage peuvent faire l'objet de demandes de la part des organes répressifs des États membres de l'UE et des pays tiers. Les données à caractère personnel risquent d'être communiquées à des organes répressifs (étrangers) sans que cette communication ne soit fondée sur une base juridique en vigueur dans l'UE, ce qui entraînerait une violation de la législation de l'Union européenne en matière de protection des données.
- Manque de possibilités d'intervention en raison de la complexité et des modalités de fonctionnement de la chaîne de sous-traitance: le service d'informatique en nuage offert par un fournisseur pourrait être obtenu en combinant des services provenant de toute une série d'autres fournisseurs, qui peuvent être ajoutés ou supprimés de manière dynamique pendant la durée du contrat du client.
- Manque de possibilités d'intervention (droits des personnes concernées): un fournisseur d'informatique en nuage ne fournit pas toujours les mesures et les outils nécessaires pour permettre au responsable du traitement de gérer les données, par exemple en termes d'accès, de suppression ou de correction des données.
- Manque de séparation: un fournisseur d'informatique en nuage peut contrôler physiquement les données de différents clients en vue d'établir des liens entre les données à caractère personnel. Si les administrateurs se voient accorder des droits d'accès suffisamment privilégiés (postes à risque élevé), ils peuvent établir un lien entre les données de plusieurs clients.

Le manque d'informations sur le traitement (transparence)

Le caractère insuffisant des informations sur les opérations de traitement d'un service d'informatique en nuage présente un risque pour les responsables du traitement, tout comme pour les personnes concernées, car s'ils ne sont pas informés des menaces et des risques éventuels, ils n'auront pas la possibilité de prendre les mesures qu'ils jugent les mieux indiquées.

Certaines menaces potentielles peuvent survenir du fait que le responsable du traitement ignore que:

- il existe un traitement en chaîne faisant intervenir plusieurs sous-traitants;
- les données à caractère personnel sont traitées dans plusieurs zones géographiques au sein de l'EEE. Cette circonstance a un effet direct sur la législation applicable aux litiges relatifs à la protection des données qui peuvent survenir entre l'utilisateur et le fournisseur;

- Les données à caractère personnel sont transférées vers des pays tiers en dehors de l'EEE. Les pays tiers ne fournissent pas toujours un niveau de protection adéquat des données et les transferts ne sont pas toujours garantis par des mesures appropriées (clauses contractuelles types ou règles d'entreprise contraignantes, par exemple) et peuvent dès lors être illégaux.

Les personnes concernées dont les données à caractère personnel sont traitées dans le nuage doivent être informées de l'identité du responsable du traitement des données et de la finalité du traitement (cette exigence est imposée à tous les responsables du traitement par la directive relative à la protection des données 95/46/CE). Compte tenu de la complexité des chaînes de traitement dans un environnement d'informatique en nuage, il conviendrait, pour garantir un traitement loyal vis-à-vis de la personne concernée (article 10 de la directive 95/46/CE), que les responsables du traitement fournissent également de plus amples renseignements sur les sous-traitants (ou sous-traitants ultérieurs) qui offrent les services d'informatique en nuage.

3. Le cadre juridique

3.1 Le cadre régissant la protection des données

Le cadre juridique applicable est la directive relative à la protection des données 95/46/CE. Cette directive s'applique dans tous les cas où les données à caractère personnel sont traitées dans le cadre de services d'informatique en nuage. La directive «vie privée et communications électroniques» 2002/58/CE (telle que révisée par la directive 2009/136/CE) s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics (opérateurs de télécommunications) et s'applique donc si ces services sont fournis au moyen d'une solution en nuage[5].

3.2 Le droit applicable

Les critères de détermination de la législation applicable figurent à l'article 4 de la directive 95/46/CE, qui fait référence au droit applicable aux responsables du traitement[6] ayant un ou plusieurs établissements dans l'EEE, et au droit applicable à ceux qui sont établis en dehors de l'EEE mais qui utilisent des moyens localisés sur le territoire de l'EEE pour traiter des données à caractère personnel. Cette question a été analysée par le groupe de travail de l'article 29 dans son avis 8/2010 sur le droit applicable[7].

Dans le premier cas de figure, le facteur qui détermine l'application du droit de l'UE au responsable du traitement est le lieu de son établissement et les activités qu'il exerce,

---

5 Directive 2002/58/CE sur la vie privée et les communications électroniques (modifiée par la directive 2009/136/CE). Cette directive s'applique aux fournisseurs de services de communications électroniques accessibles au public, et leur impose de garantir le respect des obligations relatives au secret des communications et à la protection des données personnelles, ainsi que des droits et obligations concernant les réseaux et services de communications électroniques. Les fournisseurs d'informatique en nuage qui fournissent des services de communications électroniques accessibles au public sont soumis à cette directive.

6 La notion de responsable du traitement, examinée par le groupe de travail «article 29» dans son avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», est définie à l'article 2, sous h), de la directive.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_fr.pdf

conformément à l'article 4, paragraphe 1, sous a), de la directive, et ce, quel que soit le type de service en nuage. La législation applicable est celle du pays dans lequel le responsable du traitement qui passe des contrats de services d'informatique en nuage est établi, et non celle du lieu où les fournisseurs d'informatique en nuage sont situés.

Si le responsable du traitement est établi dans plusieurs États membres et traite les données au titre de ses activités dans ces différents pays, le droit applicable sera celui de chaque État membre dans lequel le traitement a lieu.

L'article 4, paragraphe 1, sous c)[8] fait référence à la façon dont la législation sur la protection des données s'applique aux responsables du traitement qui ne sont pas établis dans l'EEE mais qui recourent à des moyens, automatisés ou non, situés sur le territoire d'un État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit. Cela implique que si un fournisseur situé dans l'EEE est mandaté par un client établi en dehors de l'EEE, alors le fournisseur lui exporte sa législation sur la protection des données.

3.3 Les devoirs et responsabilités des différents intervenants

Comme indiqué précédemment, l'informatique en nuage implique un large éventail d'intervenants. Il est important d'évaluer et de préciser le rôle de chacun de ces acteurs afin de déterminer leurs obligations particulières au regard de la législation actuelle sur la protection des données.

Il convient de rappeler que le groupe de travail «article 29» a indiqué dans son avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» que «*le rôle premier de la notion de responsable du traitement est de déterminer qui est chargé de faire respecter les règles de protection des données, et comment les personnes concernées peuvent exercer leurs droits dans la pratique. En d'autres termes, il s'agit d'attribuer les responsabilités*». Les parties qui participent à cette analyse devraient garder à l'esprit ces deux critères généraux de conformité et de répartition des responsabilités.

3.3.1 Le client et le fournisseur de services d'informatique en nuage

Le client de services d'informatique en nuage détermine l'objectif final du traitement et décide de l'externalisation de ce traitement et de la délégation de tout ou partie des activités de traitement à une organisation externe. Le client agit donc en qualité de responsable du traitement des données. La directive définit 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 client, en tant que responsable du traitement, doit observer la législation sur la protection des données et répondre de toutes les obligations légales mentionnées dans la directive 95/46/CE. Il peut laisser au fournisseur d'informatique en nuage le choix des méthodes et des mesures techniques ou organisationnelles à utiliser pour réaliser les objectifs du responsable du traitement.

[8] L'article 4, paragraphe 1, sous c), dispose que la législation d'un État membre sera applicable dès lors que «le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté».

Le fournisseur d'informatique en nuage est l'entité qui fournit les services d'informatique en nuage sous les différentes formes évoquées plus haut. Lorsqu'il fournit les moyens et la plate-forme pour le compte du client, le fournisseur est considéré comme le sous-traitant, c'est-à-dire, selon la directive 95/46/CE, comme «*la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement*» [9],[10].

Comme l'indique l'avis 1/2010, certains critères[11] peuvent être utilisés pour identifier le responsable du traitement. En fait, il peut arriver qu'un fournisseur de services d'informatique en nuage soit considéré comme un coresponsable du traitement conjointement, ou bien comme un responsable du traitement de plein droit, en fonction des circonstances concrètes. Cela pourrait par exemple être le cas du fournisseur qui traite des données pour ses propres besoins.

Il y a lieu de souligner que, même dans un environnement complexe de traitement des données, dès lors que différents responsables du traitement jouent un rôle dans le traitement de données à caractère personnel, il est impératif d'assurer le respect des règles de protection des données et d'attribuer clairement les responsabilités en cas d'infraction à ces dispositions, afin d'éviter tout affaiblissement de la protection des données à caractère personnel, ainsi que toute apparition de «conflits négatifs de compétence» ou de hiatus, qui reviendraient à ce que certains droits ou obligations découlant de la directive ne soient plus assumés par aucune des parties.

Dans le scénario actuel d'informatique en nuage, les clients de services d'informatique en nuage n'ont pas toujours la marge de manœuvre nécessaire pour négocier les conditions contractuelles d'utilisation des services en nuage, bon nombre d'entre eux faisant l'objet d'offres standardisées. Néanmoins, c'est en définitive le client qui prend la décision d'affecter tout ou partie des opérations de transformation aux services en nuage, à des fins particulières; le fournisseur d'informatique en nuage jouera un rôle de contractant à l'égard du client, ce qui est primordial dans ce cas de figure. Comme l'indique le groupe de travail de l'article 29 dans l'avis 1/2010[12] sur les notions de «responsable du traitement» et de «sous-traitant», «*le faible poids contractuel d'un petit responsable du traitement face à d'importants prestataires de services ne doit pas lui servir de justification pour accepter des clauses et conditions contractuelles contraires à la législation sur la protection des données*». Pour cette raison, le responsable du traitement doit choisir un fournisseur d'informatique en nuage qui garantisse le respect de la législation sur la protection des données. Une attention particulière doit être portée, d'une part, aux caractéristiques des contrats applicables, qui doivent notamment inclure un ensemble de garanties homogènes en matière de protection des données, y compris celles décrites par le groupe de travail aux paragraphes 3.4.3 (mesures techniques et organisationnelles) et 3.5 (flux de données transfrontaliers) et, d'autre part, à d'éventuels mécanismes supplémentaires qui peuvent s'avérer appropriés pour agir avec toute la diligence

---

9 L'environnement d'informatique en nuage peut également être utilisé par des personnes physiques (utilisateurs) pour le seul exercice d'activités personnelles ou domestiques. Dans ce cas, il convient d'analyser dans le détail si ce que l'on appelle «l'exemption domestique», en vertu de laquelle les utilisateurs ne sont pas qualifiés de responsables du traitement, s'applique. Cette question dépasse toutefois le cadre du présent avis.

10 Le présent avis porte uniquement sur la relation entre responsable du traitement et sous-traitant.

11 Notamment le niveau des instructions, le suivi de l'action par le client, l'expérience des parties.

12 Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», consultable à l'adresse: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf

requise et favoriser la responsabilisation (comme la vérification et la certification des services d'un fournisseur effectuées par des tiers indépendants – voir le paragraphe 4.2).

Les fournisseurs d'informatique en nuage (comme les sous-traitants) ont le devoir de garantir la confidentialité. La directive 95/46/CE précise que: «*Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales*». L'accès aux données par le fournisseur d'informatique en nuage pendant sa prestation de services doit par ailleurs fondamentalement répondre à la nécessité de respecter les dispositions de l'article 17 de la directive – voir le paragraphe 3.4.2.

Les sous-traitants doivent tenir compte du type de nuage en question (public, privé, communautaire ou hybride/IaaS, SaaS ou PaaS [voir annexe a) modèles de déploiement - b) modèles de services]) et du type de services souscrits par le client. Les sous-traitants sont chargés d'adopter des mesures de sûreté conformes à celles prévues par la législation européenne telle qu'appliquée dans le pays du responsable du traitement et du sous-traitant. Les sous-traitants doivent en outre soutenir et aider le responsable du traitement à respecter les droits (exercés) des personnes concernées.

3.3.2 Les sous-traitants

Les services d'informatique en nuage peuvent nécessiter la participation d'un certain nombre de parties contractantes qui agissent comme sous-traitants. Il est également fréquent pour les sous-traitants de souscrire à des services offerts par des sous-traitants ultérieurs, qui accèdent alors aux données à caractère personnel. Dans ce cas, les sous-traitants sont tenus d'en informer le client, en précisant le type de service sous-traité, les caractéristiques des sous-traitants existants ou potentiels, et les garanties prises pour que ces entités au fournisseur de services d'informatique en nuage respectent la directive 95/46/CE.

Toutes les obligations en la matière doivent par conséquent s'appliquer également aux sous-traitants ultérieurs, moyennant des contrats entre le fournisseur d'informatique en nuage et le sous-traitant reprenant les dispositions du contrat entre le fournisseur d'informatique en nuage et son client. Dans son avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», le groupe de travail «article 29» a évoqué la question de la multiplicité des sous-traitants dans les cas où les sous-traitants sont susceptibles d'entretenir une relation directe avec le responsable du traitement ou qu'ils agissent en tant que sous-traitants lorsque les sous-traitants ont délégué une partie des activités de traitement qui leur ont été confiées. «*Aucune disposition de la directive n'empêche de désigner, pour des raisons d'organisation, plusieurs entités comme sous-traitants ou (sous-)sous-traitants, notamment en subdivisant les tâches en question. Ces structures sont cependant toutes tenues de se conformer aux instructions données par le responsable du traitement pour procéder au traitement*»[13].

Dans ce type de scénario, il convient d'établir clairement les obligations et responsabilités découlant de la législation en matière de protection des données et d'éviter qu'elles ne soient dispersées tout au long de la chaîne de sous-traitance, afin de garantir le contrôle effectif des activités de traitement et de répartir précisément les responsabilités en la matière.

[13] Voir WP169, p. 29, Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf).

Un modèle possible de garantie, permettant de préciser les devoirs et les obligations des sous-traitants qui sous-traitent le traitement des données, a été établi pour la première fois dans la décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers[14]. Dans ce modèle, le sous-traitement ultérieur n'est autorisé qu'avec l'accord écrit préalable du responsable du traitement, et moyennant un accord écrit imposant au sous-traitant ultérieur les mêmes obligations que celles du sous-traitant. Lorsque le sous-traitant ultérieur n'exécute pas les obligations en matière de protection des données qui lui incombent en vertu de cet accord écrit, le sous-traitant en reste pleinement responsable envers le responsable du traitement. Une disposition de ce type pourrait être utilisée dans les clauses contractuelles liant un responsable du traitement et un fournisseur de services en nuage, lorsque ce dernier se propose de faire appel à la sous-traitance pour fournir ses services, de manière à assurer les garanties requises pour le sous-traitement ultérieur.

S'agissant des garanties au cours du sous-traitement ultérieur, la Commission a récemment suggéré une solution analogue dans sa proposition de règlement général sur la protection des données[15]. Les actes d'un sous-traitant doivent être régis par un contrat ou un autre acte juridique engageant le sous-traitant envers le responsable du traitement et stipulant notamment, entre autres exigences, que le sous-traitant ne doit pas faire appel à un autre sous-traitant sans l'autorisation préalable du responsable du traitement (article 26, paragraphe 2, de la proposition).

De l'avis du groupe de travail «article 29», le sous-traitant ne peut sous-traiter ses activités que sur la base de l'autorisation du responsable du traitement, qui peut généralement être donnée au début du service[16] et qui s'accompagne de l'obligation expresse pour le sous-traitant d'informer le responsable du traitement de toute proposition de modification relative à l'ajout ou au remplacement de sous-traitants ultérieurs, le responsable du traitement conservant à tout moment la possibilité de contester ces modifications ou de résilier le contrat. En outre, un contrat reflétant les dispositions du contrat entre le fournisseur d'informatique en nuage et son client devrait être signé entre le fournisseur de services en nuage et le sous-traitant. Le responsable du traitement devrait pouvoir disposer d'un recours contractuel en cas de violation du contrat par les sous-traitants ultérieurs. Cela pourrait consister à s'assurer que le sous-traitant est directement responsable envers le responsable du traitement de toute violation par un sous-traitant ultérieur auquel il a fait appel, ou à créer des droits bénéficiaires pour les tiers au profit du responsable du traitement dans les contrats liant le sous-traitant et les sous-traitants ultérieurs, ou à faire en sorte que ces contrats soient signés pour le compte du responsable du traitement des données, faisant ainsi de ce dernier une partie au contrat.

---

14 Voir la liste des questions les plus fréquentes II.5 de l'avis WP176.

15 Proposition de règlement du Parlement européen et du Conseil du 25 janvier 2012 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.

16 Voir la liste des questions les plus fréquentes II.1 de l'avis WP176, adoptée le 12 juillet 2010.

3.4 Les exigences en matière de protection des données dans la relation client-fournisseur

3.4.1 Respect des principes de base

La légalité du traitement des données à caractère personnel dans le nuage dépend de l'observation des principes de base de la législation de l'Union européenne en matière de protection des données. En l'occurrence, la transparence à l'égard de la personne concernée doit être garantie, le principe de spécification et de limitation des finalités doit être respecté et les données à caractère personnel doivent être effacées dès qu'il n'est plus nécessaire de les conserver. De plus, des mesures techniques et organisationnelles appropriées doivent être mises en œuvre pour garantir un niveau approprié de protection et de sécurité des données.

3.4.1.1 Transparence

La transparence revêt une importance fondamentale pour le traitement loyal et légitime des données à caractère personnel. La directive 95/46/CE fait obligation au client de fournir à la personne auprès de laquelle il collecte des données la concernant des informations sur son identité et sur les finalités du traitement. Le client devrait également fournir toutes informations supplémentaires concernant par exemple les destinataires ou les catégories de destinataires des données, qui peuvent également comprendre les sous-traitants et les sous-traitants ultérieurs, dans la mesure où ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données (voir l'article 10 de la directive)[17].

La transparence doit également être garantie dans la ou les relation(s) entre le fournisseur d'informatique en nuage, son client et les sous-traitants (le cas échéant). Le client ne peut apprécier la légalité du traitement de données à caractère personnel dans le nuage que si le fournisseur l'informe de toutes les questions pertinentes. Le responsable du traitement qui envisage de faire appel à un fournisseur d'informatique en nuage devrait soigneusement vérifier les conditions générales dudit fournisseur et les analyser sur le plan de la protection des données.

Pour garantir la transparence dans le nuage, il est nécessaire que le client ait connaissance de tous les sous-traitants prenant part à la fourniture du service en nuage concerné ainsi que de la localisation de tous les centres de données dans lesquels les données à caractère personnel peuvent être traitées[18].

Si la fourniture du service nécessite l'installation de logiciels dans le système du client (par exemple, des navigateurs périphériques), il serait de bonne pratique que le fournisseur d'informatique en nuage en informe son client, s'agissant notamment des implications de cette installation sur la protection et la sécurité des données. Inversement, le client devrait soulever cette question au préalable, si elle n'est pas suffisamment prise en compte par le fournisseur d'informatique en nuage.

---

[17] L'obligation correspondante d'informer la personne concernée existe lorsque des données qui n'ont pas été collectées auprès de la personne concernée elle-même mais auprès de sources différentes sont enregistrées ou communiquées à un tiers (voir l'article 11).

[18] Ce n'est qu'alors qu'il sera en mesure d'apprécier si les données à caractère personnel peuvent être transférées vers les pays tiers en dehors de l'espace économique européen (EEE) qui ne garantissent pas un niveau de protection adéquat au sens de la directive 95/46/CE. Voir également la section 3.4.6 ci-dessous.

3.4.1.2 Spécification et limitation des finalités

Selon le principe de spécification et de limitation des finalités, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités (voir l'article 6, paragraphe 1, point b), de la directive 95/46/CE). Le client doit définir la ou les finalité(s) du traitement avant la collecte des données à caractère personnel auprès de la personne concernée et en informer la personne concernée. Il ne doit pas traiter les données à caractère personnel de manière incompatible avec les finalités initialement prévues.

En outre, il faut s'assurer que les données à caractère personnel ne sont pas (illégalement) traitées pour d'autres finalités par le fournisseur d'informatique en nuage ou l'un de ses sous-traitants. Dans la mesure où un scenario type d'informatique en nuage peut facilement impliquer un grand nombre de sous-traitants, le risque de traiter des données à caractère personnel pour d'autres finalités qui seraient incompatibles doit donc être considéré comme assez élevé. Pour réduire ce risque au minimum, le contrat entre le fournisseur d'informatique en nuage et son client devrait prévoir des mesures techniques et organisationnelles, de manière à garantir la journalisation et l'audit des opérations de traitement des données à caractère personnel effectuées par les employés du fournisseur d'informatique en nuage ou par les sous-traitants[19]. Le contrat devrait prévoir des sanctions à l'égard du fournisseur ou du sous-traitant en cas de violation de la législation en matière de protection des données.

3.4.1.3 Effacement des données

Conformément à l'article 6, paragraphe 1, sous e), de la directive 95/46/CE, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les données à caractère personnel qui ne sont plus nécessaires doivent être effacées ou rendues strictement anonymes. Si ces données ne peuvent pas être effacées en vertu de règles juridiques relatives à la rétention (comme des réglementations fiscales), l'accès à ces données à caractère personnel devrait être bloqué. Il appartient au client de s'assurer que les données à caractère personnel sont effacées dès qu'elles ne sont plus nécessaires au sens précité[20].

Le principe de l'effacement des données s'applique aux données à caractère personnel, qu'elles soient ou non stockées sur un disque dur ou sur un autre support de stockage (une bande de sauvegarde, par exemple). Étant donné que les données à caractère personnel peuvent être conservées de façon redondante sur plusieurs serveurs et sur différents sites, il faut s'assurer qu'elles sont dans chaque cas effacées de manière irréversible (c'est-à-dire que les versions précédentes, les fichiers temporaires et même les fragments de fichiers doivent également être supprimés).

Les clients doivent être conscients du fait que les données d'enregistrement[21] facilitant la vérifiabilité par exemple du stockage, des modifications ou de l'effacement des données, peuvent aussi être qualifiées de données à caractère personnel concernant la personne qui a

---

19 Voir la section 3.4.3 ci-dessous.

20 L'effacement des données constitue un problème pendant toute la durée du contrat d'informatique en nuage et à sa résiliation. Il s'applique également en cas de substitution ou de retrait d'un sous-traitant.

21 Les remarques concernant les exigences en matière d'enregistrement figurent dans la section 4.3.4.2 ci-dessous.

lancé les opérations de traitement respectives[22]. L'effacement sécurisé des données à caractère personnel exige la destruction ou la démagnétisation du support de stockage, ou bien la suppression effective par écrasement des données à caractère personnel stockées. Pour l'écrasement de données à caractère personnel, il convient d'utiliser des logiciels spéciaux qui écrasent les données en écrivant de multiples fois par-dessus conformément à une spécification reconnue.

Le client devrait s'assurer que son fournisseur garantit l'effacement sécurisé dans le sens précité et que le contrat le liant au fournisseur contient des dispositions claires concernant l'effacement des données à caractère personnel[23]. Il en va de même pour les contrats entre fournisseurs d'informatique en nuage et sous-traitants.

3.4.2 Garanties contractuelles de la ou des relation(s) responsable du traitement/sous-traitant

Lorsqu'un responsable du traitement décide de sous-traiter des services d'informatique en nuage, il doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer, et doit veiller au respect de ces mesures (article 17, paragraphe 2, de la directive 95/46/CE). En outre, il est juridiquement tenu de s'engager formellement par contrat avec le fournisseur de services en nuage, comme l'indique l'article 17, paragraphe 3, de la directive 95/46/CE. Conformément à cet article, la relation entre le responsable du traitement et le sous-traitant doit être régie par un contrat ou un autre acte juridique contraignant. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures techniques et organisationnelles doivent être consignés par écrit ou sous une forme équivalente.

En particulier, le contrat doit au minimum imposer au sous-traitant l'obligation de se conformer aux instructions du responsable du traitement et de mettre en œuvre des mesures techniques et organisationnelles pour garantir la protection adéquate des données à caractère personnel.

Pour garantir la sécurité juridique, le contrat devrait par ailleurs mentionner les éléments suivants:

1. Des précisions sur les instructions (portée et modalités) du client adressées au fournisseur, notamment en ce qui concerne les accords sur les niveaux de service applicables (qui devraient être objectifs et mesurables) et sur les sanctions prévues (financières ou autres, y compris la possibilité d'engager des poursuites à l'encontre du fournisseur en cas de non-conformité).
2. Des indications sur les mesures de sûreté que le fournisseur d'informatique en nuage doit respecter, en fonction des risques que représente le traitement et de la nature des données à protéger. Il est très important que des mesures techniques et organisationnelles concrètes soient définies, à l'exemple de celles décrites au point 3.4.3 ci-dessous. Ce qui n'empêche pas, le cas échéant, l'application de mesures plus strictes, envisagées par le droit national du client.

[22] Cela signifie qu'il faut définir des durées de rétention raisonnables pour les fichiers journaux et mettre en place des processus visant à garantir l'effacement ou l'anonymisation de ces données en temps utile.

[23] Voir la section 3.4.3 ci-dessous.

3. L’objet et le calendrier du service en nuage à fournir, l’étendue, les modalités et la finalité du traitement des données à caractère personnel par le fournisseur d’informatique en nuage, ainsi que les types de données à caractère personnel traités.
4. La spécification des conditions de retour des données (à caractère personnel) ou de destruction des données une fois le service terminé. Il faut en outre s’assurer que les données à caractère personnel sont effacées en toute sécurité à la demande du client.
5. L’inclusion d’une clause de confidentialité liant le fournisseur d’informatique en nuage à l’un quelconque de ses employés qui peut avoir accès aux données. Seules les personnes autorisées peuvent avoir accès aux données.
6. L’obligation de la part du fournisseur d’apporter son soutien au client pour faciliter l’exercice par les personnes concernées de leurs droits d’accéder à leurs données, et de les corriger ou les supprimer.
7. Le contrat devrait expressément établir que le fournisseur d’informatique en nuage ne peut pas communiquer les données à des tiers, même à des fins de conservation, sauf si le contrat prévoit le recours à des sous-traitants. Le contrat devrait préciser que les sous-traitants ultérieurs ne peuvent être mandatés que sur la base d’une autorisation généralement donnée par le responsable du traitement, qui s’accompagne de l'obligation claire pour le sous-traitant d’informer le responsable du traitement de toute proposition de modification à cet égard, celui-ci conservant à tout moment la possibilité de contester ces modifications ou de résilier le contrat. Le fournisseur d’informatique en nuage doit être clairement tenu de donner le nom de tous les sous-traitants mandatés (par exemple, sur un registre public numérique). Il faut s’assurer que le contrat signé entre le fournisseur d’informatique en nuage et le sous-traitant reflète les dispositions du contrat signé entre le fournisseur d’informatique en nuage et son client (à savoir que les sous-traitants ultérieurs sont soumis aux mêmes obligations contractuelles que les fournisseurs d'informatique en nuage). En particulier, il doit être garanti que le fournisseur d’informatique en nuage et tous les sous-traitants n’agissent que sur instruction du client. Comme il est expliqué dans le chapitre sur le sous-traitement, la chaîne de responsabilité devrait être clairement établie dans le contrat, tout comme l’obligation du sous-traitant d’encadrer les transferts internationaux, par exemple en signant des contrats avec les sous-traitants ultérieurs, sur la base des clauses contractuelles types issues de la décision de la Commission européenne du 5 février 2010 (2010/87/UE).
8. Des précisions sur l’obligation du fournisseur d’informatique en nuage d’informer son client en cas de violation des données susceptible de l’affecter.
9. L’obligation du fournisseur d’informatique en nuage de fournir une liste des sites où les données peuvent être traitées.
10. Le pouvoir de contrôle du responsable du traitement et l’obligation correspondante du fournisseur d’informatique en nuage de coopérer.
11. Il convient d’établir contractuellement que le fournisseur d’informatique en nuage est tenu d’informer son client des changements pertinents relatifs aux différents services en nuage, comme la mise en œuvre de fonctions supplémentaires, par exemple.
12. Le contrat devrait prévoir la journalisation et l’audit des opérations de traitement des données à caractère personnel effectuées par les employés du fournisseur d’informatique en nuage ou par les sous-traitants.
13. La notification par le client de toute demande contraignante de divulgation des données à caractère personnel émanant d’un organe répressif, sauf disposition

contraire, telle qu'une interdiction à caractère pénal visant à préserver le secret d'une enquête policière.

14. Une obligation générale de la part du fournisseur de garantir que son organisation interne et ses modalités de traitement des données (ainsi que celles de ses éventuels sous-traitants ultérieurs) sont conformes aux prescriptions et normes légales, nationales et internationales, applicables.

En cas d'infraction de la part du responsable du traitement, toute personne ayant subi un préjudice du fait d'un traitement illicite a le droit d'obtenir, auprès du responsable du traitement, réparation du préjudice causé. Dans l'hypothèse où les sous-traitants utiliseraient les données à d'autres fins, ou s'ils les communiquaient ou les utilisaient d'une manière qui viole le contrat, ils seraient également considérés comme des responsables du traitement, et seraient tenus responsables des infractions auxquelles ils auront personnellement pris part.

Il convient de noter que, dans la plupart des cas, les fournisseurs de services en nuage offrent des services et des contrats types que les responsables du traitement doivent signer, définissant ainsi un format normalisé de traitement des données à caractère personnel. Le faible poids contractuel d'un petit responsable du traitement face à d'importants prestataires de services ne doit pas lui servir de justification pour accepter des clauses et conditions contractuelles contraires à la législation sur la protection des données.

3.4.3 Mesures techniques et organisationnelles en matière de protection et de sécurité des données

L'article 17, paragraphe 2, de la directive 95/46/CE fait porter au client (agissant en qualité de responsable du traitement des données) la pleine responsabilité d'une part, de choisir un fournisseur d'informatique en nuage qui prenne des mesures de sécurité sur le plan technique et au niveau de l'organisation à même de protéger les données à caractère personnel, et d'autre part, de rendre compte de ses actes.

Outre les principaux objectifs de sécurité que sont la disponibilité, la confidentialité et l'intégrité, une attention particulière doit aussi être portée aux objectifs complémentaires de transparence (voir le point 3.4.1.1 ci-dessus), de séparation[24], de possibilité d'intervention, de responsabilité et de portabilité, spécifiques à la protection des données. Cette section met en lumière ces objectifs principaux de protection des données, sans préjudice de toute autre analyse de risques complémentaire axée sur la sécurité[25].

3.4.3.1 Disponibilité

Assurer la disponibilité, c'est garantir un accès fiable et en temps opportun aux données à caractère personnel.

La perte accidentelle de la connectivité au réseau entre le client et le fournisseur ou les problèmes de performance du serveur dus à des actes malveillants, tels que des attaques par déni de service[26] (distribué), menacent gravement la disponibilité dans le nuage. Parmi les

---

[24] La Conférence des commissaires à la protection des données défend le concept plus général d'«indissociabilité», introduit dans la législation allemande.

[25] Voir notamment le rapport de l'ENISA à l'adresse http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[26] Une attaque par déni de service est une tentative concertée de rendre un ordinateur ou un élément de réseau indisponibles à leurs utilisateurs autorisés, que ce soit temporairement ou indéfiniment (par exemple, en utilisant de nombreux systèmes d'intrusion, qui paralysent leur cible en lançant de multiples demandes de communication externe).

autres risques de disponibilité figurent: les défaillances matérielles accidentelles sur le réseau et dans les systèmes de traitement et de stockage des données en nuage; les pannes de courant; et d'autres problèmes d'infrastructure.

Le responsable du traitement des données devrait vérifier si le fournisseur d'informatique en nuage a adopté des mesures raisonnables pour faire face aux risques de perturbations, comme la sauvegarde des liens internet, le stockage redondant et des mécanismes efficaces de sauvegarde des données.

3.4.3.2 Intégrité

L'intégrité peut se définir comme la qualité en vertu de laquelle les données sont authentiques et n'ont pas été modifiées par mégarde ou malveillance pendant le traitement, le stockage ou la transmission. La notion d'intégrité peut s'étendre aux systèmes informatiques et exige que le traitement des données à caractère personnel sur ces systèmes reste inaltéré.

Pour détecter les modifications apportées aux données à caractère personnel, il est possible de recourir à des mécanismes d'authentification cryptographiques tels que les codes ou signatures d'authentification des messages.

Toute ingérence portant atteinte à l'intégrité des systèmes informatiques dans le nuage peut être évitée ou détectée grâce aux systèmes de détection et de prévention d'intrusions (IPS/IDS). Ce point revêt une importance particulière pour les types d'environnements réseau ouverts dans lesquels les nuages fonctionnent généralement.

3.4.3.3 Confidentialité

Dans un environnement en nuage, le cryptage peut contribuer de manière significative à la confidentialité des données à caractère personnel s'il est utilisé correctement, bien qu'il ne rende pas les données à caractère personnel irréversiblement anonymes[27]. Le cryptage des données à caractère personnel devrait être systématique pour les données «en transit» et être utilisé lorsque c'est possible pour les données «au repos»[28]. Dans certains cas (par exemple, dans un service de stockage IaaS), un client peut ne pas utiliser la solution de cryptage proposée par le fournisseur d'informatique en nuage, et décider de chiffrer lui-même ses données à caractère personnel avant de les envoyer dans le nuage. Le cryptage des données au repos requiert de porter une attention particulière à la gestion des clés cryptographiques, car la sécurité des données dépend alors, en définitive, de la confidentialité des clés de cryptage.

Les communications entre le fournisseur d'informatique en nuage et son client, de même qu'entre les centres de données, devraient être cryptées. La gestion à distance de la plateforme en nuage ne devrait être assurée que par le biais d'un canal de communication sécurisé. Le client qui prévoit non seulement de stocker, mais également de traiter ultérieurement des données à caractère personnel dans le nuage (par exemple, en recherchant des enregistrements dans des bases de données), doit garder à l'esprit que le cryptage ne peut pas être maintenu pendant le traitement des données (à l'exception de calculs très spécifiques).

---

[27] Directive 95/46/CE – considérant 26: «[…] considérant que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable; […]». De même, les processus techniques de fragmentation des données qui peuvent être utilisés dans le cadre de la fourniture de services d'informatique en nuage n'entraînent pas une anonymisation irréversible et n'impliquent donc pas que les obligations en matière de protection des données ne s'appliquent pas.

[28] Cela est particulièrement vrai pour les responsables du traitement des données qui envisagent de transférer dans le nuage des données confidentielles au sens de l'article 8 de la directive 95/46/CE (par exemple, des données sur la santé) ou des données soumises à une obligation juridique spécifique de secret professionnel.

Les mécanismes d'autorisation et l'authentification forte (par exemple, l'authentification à deux facteurs) comptent parmi les autres mesures techniques visant à garantir la confidentialité. Les clauses contractuelles devraient également imposer des obligations de confidentialité aux employés des clients, des fournisseurs de services en nuage et des sous-traitants.

3.4.3.4 Transparence

Les mesures techniques et organisationnelles doivent favoriser la transparence afin de permettre un contrôle (voir le point 3.4.1.1).

3.4.3.5 Séparation (limitation de la finalité)

Dans les infrastructures en nuage, les ressources telles que le stockage, la mémoire et les réseaux sont partagés entre de nombreux «locataires» (*tenants*), ce qui crée de nouveaux risques de voir les données divulguées et traitées à des fins illégitimes. L'objectif de protection «séparation» est censé régler cette question et contribuer à garantir que les données ne seront pas utilisées au-delà de leur finalité initiale [article 6, paragraphe 1, point b), de la directive 95/46/CE] et que la confidentialité et l'intégrité seront maintenues[29].

Pour instaurer la séparation, il faut tout d'abord une structure de gouvernance adéquate des droits et des responsabilités en matière d'accès aux données à caractère personnel, qui fasse l'objet d'un réexamen régulier. Il convient de ne pas confier de missions assorties de privilèges excessifs (notamment, aucun utilisateur ou administrateur ne devrait être autorisé à accéder à l'intégralité du nuage). De manière plus générale, les administrateurs et les utilisateurs ne doivent pouvoir accéder qu'aux informations nécessaires pour servir leurs objectifs légitimes (principe du moindre privilège).

Ensuite, la séparation dépend également de l'adoption de mesures techniques, telles que le durcissement de l'environnement des hyperviseurs et la gestion appropriée des ressources partagées, si des machines virtuelles sont utilisées pour partager des ressources physiques entre plusieurs clients.

3.4.3.5 Possibilité d'intervention

La directive 95/46/CE donne à toute personne concernée un droit d'accès aux données, permettant d'obtenir la rectification, l'effacement et le verrouillage des données, ainsi qu'un droit d'opposition (voir les articles 12 et 14). Le client doit vérifier que le fournisseur d'informatique en nuage ne dresse pas d'obstacles techniques ou organisationnels à la mise en œuvre de ces exigences, y compris lorsque les données sont traitées ultérieurement par des sous-traitants.

Le contrat entre le client et le fournisseur devrait stipuler que le fournisseur d'informatique en nuage est tenu d'aider le client pour faciliter l'exercice des droits reconnus aux personnes concernées et de veiller à ce qu'il en soit de même dans sa relation avec un quelconque sous-traitant[30].

---

[29] Voir le point 3.4.1.2.

[30] Voir supra le point 6 de la section 3.4.2. Le fournisseur peut même être chargé de répondre à des demandes pour le compte du client.

3.4.3.6 Portabilité

Actuellement, la plupart des fournisseurs d'informatique en nuage n'utilisent pas de formats de données ni d'interfaces de service standardisés facilitant l'interopérabilité et la portabilité entre différents fournisseurs d'informatique en nuage. Si un client décide de migrer d'un fournisseur d'informatique en nuage à un autre, ce manque d'interopérabilité peut rendre impossible, ou pour le moins difficile, le transfert des données (à caractère personnel) du client au nouveau fournisseur d'informatique en nuage (ce que l'on a coutume d'appeler la dépendance vis-à-vis du fournisseur). Il en va de même des services que le client a développés sur une plateforme offerte par le premier fournisseur d'informatique en nuage (PaaS). Le client devrait vérifier si, et de quelle manière, le fournisseur garantit la portabilité des données et des services avant de souscrire à un service en nuage[31].

3.4.3.7 Responsabilité

En informatique, la responsabilité peut se définir comme la capacité de déterminer ce qu'une entité a fait à un certain moment du passé et de quelle façon. Dans le domaine de la protection des données, elle a généralement une signification plus large et désigne la capacité des parties de démontrer qu'elles ont pris toutes les mesures appropriées pour garantir le respect des principes de protection des données.

La responsabilité informatique est particulièrement importante pour enquêter sur les violations de données à caractère personnel, lorsque les clients, les fournisseurs et les sous-traitants ultérieurs peuvent tous assumer une part de responsabilité opérationnelle. La capacité d'une plateforme en nuage d'offrir des mécanismes fiables de contrôle et de journalisation complète revêt à cet égard une importance capitale.

En outre, les fournisseurs d'informatique en nuage devraient fournir la preuve documentaire qu'ils ont pris des mesures appropriées et efficaces pour que les principes de protection des données décrits dans les sections précédentes produisent leurs effets. Les procédures visant à garantir l'identification de l'ensemble des opérations de traitement des données et à répondre aux demandes d'accès, ainsi que l'affectation des ressources, comprenant la désignation de délégués à la protection des données chargés d'organiser le contrôle du respect des règles en matière de protection des données, ou encore les procédures de certification indépendante, sont des exemples de ces mesures. Les responsables du traitement des données devraient, en outre, veiller à être prêts à démontrer à l'autorité de contrôle compétente, à sa demande, qu'ils ont bien mis en place les mesures nécessaires[32].

3.5 Les transferts internationaux

Les articles 25 et 26 de la directive 95/46/CE subordonnent strictement la libre circulation des données à caractère personnel vers des pays situés en dehors de l'EEE, à la condition que ces pays, ou bien le destinataire, assurent un niveau de protection adéquat des données. À défaut, des garanties particulières doivent être mises en place par le responsable du traitement et ses coresponsables et/ou sous-traitants. Or l'informatique en nuage est le plus souvent fondée sur une absence de localisation stable des données dans le réseau du fournisseur d'informatique

---

[31] Le fournisseur devrait utiliser, de préférence, des formats de données et des interfaces standardisés ou ouverts. Dans tous les cas, les clauses contractuelles spécifiant les formats déterminés, le maintien des relations logiques et tous les frais découlant de la migration vers un autre fournisseur d'informatique en nuage devraient être décidés d'un commun accord.

[32] Le groupe de travail a formulé des remarques détaillées sur le thème de la responsabilité dans son avis 3/2010 sur le principe de la responsabilité http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf.

en nuage. Les données peuvent se trouver dans un centre de données à midi et à l'autre bout du monde à 14 heures. Le client est donc rarement en mesure de savoir en temps réel où se trouvent ses données et où elles sont transférées et stockées. Dans ce contexte, les instruments juridiques traditionnels permettant de réglementer les transferts de données vers des pays tiers qui n'assurent pas un niveau de protection adéquat démontrent leurs limites.

3.5.1 Sphère de sécurité et pays ayant un niveau de protection adéquat

Les constatations concernant le niveau de protection adéquat des données, y compris la sphère de sécurité, sont limitées géographiquement et ne couvrent donc pas l'intégralité des transferts dans le nuage.
Les transferts vers les organisations américaines qui adhèrent aux principes peuvent intervenir en toute légalité en vertu du droit de l'UE, dans la mesure où les organisations destinataires sont réputées apporter un niveau de protection adéquat aux données transférées.

Toutefois, du point de vue du Groupe de travail, l'auto-certification de la sphère de sécurité à elle seule peut ne pas toujours être jugée adéquate en l'absence d'une application stricte des principes de protection des données dans l'environnement en nuage. En outre, l'article 17 de la directive exige qu'un contrat soit signé entre le responsable du traitement et le sous-traitant à des fins de traitement, ce qui est confirmé par la réponse à la «FAQ 10» (question fréquemment posée) incluse dans les documents du cadre de référence de la sphère de sécurité («U.S.-EU Safe Harbor Framework»). Ce contrat n'est pas soumis à l'autorisation préalable des autorités européennes chargées de la protection des données. Il mentionne les traitements à réaliser ainsi que toutes les mesures nécessaires pour garantir que les données sont conservées en toute sécurité. Les différentes législations nationales et les autorités chargées de la protection des données peuvent poser des exigences supplémentaires.

Le Groupe de travail considère que les entreprises qui exportent des données ne devraient pas uniquement se fonder sur les déclarations de l'importateur des données affirmant qu'il dispose d'une certification «sphère de sécurité». Au contraire, l'entreprise exportatrice de données devrait obtenir la preuve de l'existence des auto-certifications de la sphère de sécurité et demander la preuve que ces principes sont bien respectés. Cela est tout particulièrement important en ce qui concerne les informations fournies aux personnes concernées par le traitement des données[33],[34].

Le Groupe de travail considère en outre que le client doit vérifier si les contrats types établis par les fournisseurs d'informatique en nuage sont conformes aux prescriptions nationales en matière de contrats de traitement des données. Les législations nationales peuvent exiger que le sous-traitement ultérieur soit défini dans le contrat, ce qui inclut les lieux d'établissement et autres renseignements concernant les sous-traitants ultérieurs, ainsi que la traçabilité des données. En principe, les fournisseurs d'informatique en nuage ne donnent pas ces indications à leurs clients – leur engagement à la sphère de sécurité ne peut pas compenser l'absence des garanties ci-dessus, lorsqu'elles sont requises par les législations nationales. Dans de tels cas, l'exportateur est incité à utiliser d'autres instruments juridiques disponibles, comme les clauses contractuelles types ou les règles d'entreprises contraignantes.

Enfin, le Groupe de travail considère également que les principes de la «sphère de sécurité» en eux-mêmes peuvent ne pas garantir à l'exportateur de données qu'il disposera de tous les

---

[33] Voir l'autorité allemande chargée de la protection des données: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

[34] Pour les exigences relatives à l'engagement par contrat de sous-traitants ultérieurs, voir le point 3.3.2.

moyens nécessaires pour assurer l'application par le fournisseur d'informatique en nuage aux États-Unis de mesures de sûreté appropriées, telles qu'elles peuvent être imposées par les législations nationales sur la base de la directive 95/46/CE[35]. En termes de sécurité des données, l'informatique en nuage augmente certains risques de sécurité propres au nuage, comme la perte de gouvernance, la suppression peu sûre ou incomplète des données, les pistes d'audit insuffisantes ou les défaillances du système de séparation[36], qui ne sont pas suffisamment pris en compte par les principes de la «sphère de sécurité» en vigueur relatifs à la sécurité des données[37]. Des garanties supplémentaires en faveur de la sécurité des données peuvent donc être déployées, par exemple en incluant l'expérience et les ressources de tiers qui peuvent évaluer l'adéquation des fournisseurs d'informatique en nuage à travers différentes actions d'audit, de normalisation et de certification[38]. Pour ces raisons, il serait peut-être opportun de compléter l'engagement de l'importateur de données à la «sphère de sécurité» avec des garanties supplémentaires tenant compte de la nature spécifique du nuage.

3.5.2 Dérogations

Les dérogations prévues à l'article 26 de la directive 95/46/CE permettent aux exportateurs de données de transférer les données en dehors de l'UE sans apporter de garanties supplémentaires. Cela étant, le Groupe 29 a adopté un avis dans lequel il a considéré que les dérogations ne devaient concerner que les cas où les transferts n'étaient ni récurrents, ni massifs, ni structurels[39].

Sur la base de cette interprétation, il est pratiquement impossible de se prévaloir de ces dérogations dans le cadre de l'informatique en nuage.

3.5.3 Clauses contractuelles types

Les clauses contractuelles types, telles qu'adoptées par la Commission européenne pour encadrer les transferts de données internationaux entre deux responsables du traitement ou entre un responsable du traitement et un sous-traitant, sont basées sur une approche bilatérale. Lorsque le fournisseur d'informatique en nuage est considéré comme le sous-traitant, les clauses types prévues par la décision 2010/87/CE de la Commission peuvent être utilisées entre le sous-traitant et le responsable du traitement comme base de l'environnement d'informatique en nuage pour offrir des garanties suffisantes en cas de transferts internationaux.

En plus des clauses contractuelles types, le Groupe de travail estime que les fournisseurs d'informatique en nuage pourraient proposer aux consommateurs des dispositions fondées sur leur expérience pragmatique, pour autant qu'elles n'aillent pas à l'encontre, directement ou indirectement, des clauses contractuelles types approuvées par la Commission ou qu'elles ne

---

35 Voir un avis de l'autorité danoise chargée de la protection des données: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Ces risques sont décrits en détail dans le rapport de l'ENISA "Cloud Computing: Benefits, Risks and Recommendations for Information Security" consultable à l'adresse: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 «Les organisations doivent prendre les mesures nécessaires pour éviter la perte, l'utilisation abusive, la consultation illicite, la divulgation, la modification et la destruction des données à caractère personnel».

38 Voir la section 4.2 ci-dessus.

39 Voir le document de travail 12/1998: Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données, adopté par le groupe de travail le 24 juillet 1998 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_fr.pdf).

portent pas atteinte aux droits ou libertés fondamentaux des personnes concernées[40]. Néanmoins, les entreprises ne peuvent pas modifier ni remplacer les clauses contractuelles types, sans quoi elles ne seraient plus des clauses «types»[41].

Lorsque le fournisseur d'informatique en nuage agissant comme sous-traitant est établi dans l'UE, la situation peut devenir plus complexe dans la mesure où les clauses types ne s'appliquent, en général, qu'aux transferts de données de responsables du traitement établis dans l'Union européenne vers des sous-traitants établis dans des pays tiers (voir le considérant 23 de la décision 2010/87/UE de la Commission sur les clauses types et l'avis WP 176).

En ce qui concerne la relation contractuelle entre le sous-traitant établi dans un pays tiers et les sous-traitants ultérieurs, un accord écrit imposant au sous-traitant ultérieur les mêmes obligations que celles du sous-traitant dans les clauses types devrait être mis en place.

3.5.4 Règles d'entreprises contraignantes: vers une approche globale

Les règles d'entreprises contraignantes constituent un code de conduite pour les entreprises qui transfèrent des données au sein de leur groupe. Cette solution s'appliquera également aux services d'informatique en nuage lorsque le fournisseur est un sous-traitant. En effet, le GT «article 29» travaille actuellement sur des règles d'entreprise contraignantes appliquées aux sous-traitants, qui permettront le transfert au sein du groupe vers les responsables du traitement, sans que les sous-traitants et les sous-traitants ultérieurs soient tenus de signer un contrat par client[42].

Ces règles d'entreprises contraignantes appliquées aux sous-traitants permettraient au client du fournisseur de confier ses données à caractère personnel au sous-traitant tout en étant assuré que les données transférées dans le champ d'activité du fournisseur bénéficieront d'un niveau de protection adéquat.

4. Conclusions et recommandations

Les entreprises et les administrations qui souhaitent utiliser l'informatique en nuage devraient, dans un premier temps, procéder à une analyse de risques rigoureuse et exhaustive. Cette analyse doit couvrir les risques liés au traitement des données dans le nuage (absence de contrôle et insuffisance des informations – voir la section 2 supra) en tenant compte du type de données traitées dans le nuage[43]. L'évaluation des risques juridiques concernant la protection des données, qui concernent principalement les obligations en matière de sécurité et les transferts internationaux, devrait également faire l'objet d'une attention particulière. Le

---

40 Voir la FAQ IV B1.9 9, Les entreprises peuvent-elles appliquer les clauses contractuelles types dans un contrat plus large et ajouter des clauses spécifiques? http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 Voir la FAQ IV B1.10, Les entreprises peuvent-elles modifier et remplacer les clauses contractuelles types approuvées par la Commission?

42 Voir le document de travail 02/2012 établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes appliquées au sous-traitant, adopté le 6 juin 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

L'ENISA fournit une liste des risques à prendre en considération.

traitement des données confidentielles à travers l'informatique en nuage soulève d'autres préoccupations. Il nécessite donc des garanties supplémentaires, sans préjudice des dispositions législatives nationales[44]. Les conclusions ci-dessous visent à établir une liste de questions à examiner concernant le respect des règles en matière de protection des données par les fournisseurs et les clients d'informatique en nuage, sur la base du cadre juridique actuel. Quelques recommandations y sont également formulées, dans la perspective des évolutions futures du cadre réglementaire au niveau de l'UE et au-delà.

4.1 Lignes directrices à l'intention des clients et des fournisseurs de services d'informatique en nuage

- Relation responsable du traitement/sous-traitant: le présent avis envisage principalement la relation client/fournisseur comme une relation responsable du traitement/sous-traitant (voir le point 3.3.1). Néanmoins, il existe des situations concrètes dans lesquelles le fournisseur d'informatique en nuage agit aussi en tant que responsable du traitement, par exemple, lorsqu'il retraite certaines données à caractère personnel pour des finalités qui lui sont propres. Dans ce cas, le fournisseur d'informatique en nuage est pleinement (conjointement) responsable du traitement et doit remplir toutes les obligations juridiques prévues par les directives 95/46/CE et 2002/58/CE (le cas échéant);
- Responsabilité du client de services en nuage en tant que responsable du traitement: le client, en tant que responsable du traitement, doit observer la législation sur la protection des données et répondre de toutes les obligations légales mentionnées dans les directives 95/46/CE et 2002/58/CE, le cas échéant, à l'égard notamment des personnes concernées (point 3.3.1). Le client devrait choisir un fournisseur d'informatique en nuage qui garantisse le respect de la législation européenne sur la protection des données, telle qu'elle ressort des garanties contractuelles appropriées récapitulées ci-après;
- Garanties en matière de sous-traitance: tout contrat liant un fournisseur d'informatique en nuage et un client devrait contenir des dispositions relatives à la sous-traitance. Le contrat devrait préciser que les sous-traitants ultérieurs ne peuvent être mandatés que sur la base d'une autorisation généralement donnée par le responsable du traitement, qui s'accompagne de l'obligation claire pour le sous-traitant d'informer le responsable du traitement de toute proposition de modification à cet égard, celui-ci conservant à tout moment la possibilité de contester ces modifications ou de résilier le contrat. Le fournisseur d'informatique en nuage doit être clairement tenu de donner le nom de tous les sous-traitants mandatés. Le fournisseur d'informatique en nuage devrait signer avec chaque sous-traitant un contrat reflétant les dispositions du contrat signé avec son client; le client devrait s'assurer qu'il dispose d'un recours contractuel en cas de violation du contrat par les sous-traitants ultérieurs du fournisseur (point 3.3.2);
- Respect des principes fondamentaux de protection des données:
    - Transparence (point 3.4.1.1): les fournisseurs d'informatique en nuage devraient informer leurs clients de tous les aspects pertinents (concernant la protection des données) de leurs services lors des négociations contractuelles; en particulier, les clients devraient être informés de tous les sous-traitants prenant part à la fourniture du service en nuage concerné ainsi que des lieux où les données à caractère personnel sont susceptibles d'être stockées ou traitées par le fournisseur d'informatique en nuage et/ou ses sous-traitants [en

[44] Voir le mémorandum de Sopot, et la note de bas de page 2 supra.

particulier, si ces lieux sont en tout ou partie situés en dehors de l'espace économique européen (EEE)]; le client devrait recevoir des informations utiles sur les mesures techniques et organisationnelles mises en œuvre par le fournisseur; il serait de bonne pratique que le client fournisse aux personnes concernées des renseignements sur le fournisseur d'informatique en nuage et sur tous les sous-traitants (s'il en existe), ainsi que sur les lieux où les données sont susceptibles d'être stockées ou traitées par le fournisseur d'informatique en nuage et/ou ses sous-traitants;

- Spécification et limitation des finalités (point 3.4.1.2): le client devrait veiller au respect des principes de spécification et de limitation des finalités et faire en sorte qu'aucune donnée ne soit traitée à d'autres fins par le fournisseur ou par un quelconque sous-traitant. Des mesures contractuelles appropriées (y compris des mesures techniques et organisationnelles) devraient refléter les engagements pris à cet égard;
- Conservation des données (point 3.4.1.3): il incombe au client de s'assurer que les données à caractère personnel sont effacées (par le fournisseur et par tout sous-traitant) du lieu où elles sont stockées dès lors qu'elles ne sont plus nécessaires à la réalisation des finalités spécifiques pour lesquelles elles ont été collectées; des mécanismes d'effacement sécurisé (destruction, démagnétisation, écrasement) devraient être expressément prévus dans le contrat;

- <u>Garanties contractuelles (points 3.4.2, 3.4.3 et 3.5):</u>
  - En règle générale: le contrat avec le fournisseur (et ceux à établir entre le fournisseur et les sous-traitants) devrait offrir suffisamment de garanties en termes de mesures de sécurité techniques et organisationnelles (conformément à l'article 17, paragraphe 2, de la directive) et devrait être consigné par écrit ou sous une forme équivalente. Le contrat devrait préciser les instructions du client au fournisseur, y compris l'objet et le calendrier du service, les niveaux de service objectifs et mesurables et les sanctions prévues (financières ou autres); il devrait indiquer les mesures de sûreté à respecter en fonction des risques que représente le traitement et de la nature des données, conformément aux exigences ci-après et sous réserve de mesures plus strictes envisagées par le droit national du client; si le fournisseur d'informatique envisage de recourir à des clauses contractuelles types, il devrait s'assurer que ces clauses sont conformes aux exigences en matière de protection des données (point 3.4.2); en particulier, ces clauses devraient mentionner les mesures techniques et organisationnelles mises en œuvre par le fournisseur;
  - Accès aux données: seules les personnes autorisées devraient avoir accès aux données; le contrat devrait prévoir une clause de confidentialité à l'égard du fournisseur et de ses employés;
  - Communication des données à des tiers: elle devrait être exclusivement réglementée par contrat, lequel devrait inclure l'obligation pour le fournisseur de donner le nom de tous ses sous-traitants – par exemple sur un registre public numérique – et de garantir au client l'accès aux informations en cas de modification, de manière à lui donner la possibilité de contester ces modifications ou de résilier le contrat; le contrat devrait par ailleurs imposer au fournisseur de notifier toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité répressive, sauf

disposition contraire; le client devrait garantir que le fournisseur rejettera toute demande non contraignante de divulgation des données;

- Obligation de coopérer: le client devrait faire en sorte que le fournisseur soit tenu de coopérer avec lui dans l'exercice de son droit de contrôler les opérations de traitement, de faciliter l'exercice par les personnes concernées de leurs droits d'accès/de correction/d'effacement des données, et (le cas échéant) de l'informer de toute violation de données affectant ses données;
- Transferts internationaux de données: le client de services en nuage est tenu de vérifier si le fournisseur peut garantir la légalité des transferts de données internationaux et limiter les transferts aux pays choisis par le client, dans la mesure du possible. les transferts de données vers des pays tiers qui n'assurent pas un niveau adéquat de protection exigent des garanties particulières, que sont le recours à l'accord sur la «sphère de sécurité», aux clauses contractuelles types ou aux règles d'entreprise contraignantes, selon le cas; le recours aux clauses contractuelles types pour les sous-traitants (conformément à la décision 2010/87/CE de la Commission) nécessite d'apporter certaines adaptations à l'environnement en nuage (pour éviter les contrats distincts par client entre un fournisseur et ses sous-traitants ultérieurs), qui pourraient impliquer la nécessité d'obtenir l'autorisation préalable de l'autorité chargée de la protection des données compétente; une liste des lieux dans lesquels le service peut être fourni devrait figurer au contrat;
- Journalisation et audit du traitement: le client devrait demander la journalisation des opérations de traitement exécutées par le fournisseur et ses sous-traitants; le client devrait être habilité à réaliser l'audit de ces opérations de traitement, bien que les audits et la certification réalisés par des tiers choisis par le responsable du traitement puissent également être acceptés, sous réserve de la garantie d'une transparence totale (par exemple en prévoyant la possibilité d'obtenir un exemplaire du certificat d'audit du tiers ou du rapport d'audit attestant du contrôle);
- Mesures techniques et organisationnelles: elles devraient être destinées à remédier aux risques induits par l'absence de contrôle et le manque d'informations qui sont très caractéristiques de l'environnement d'informatique en nuage. Les mesures techniques comprennent les mesures visant à garantir la disponibilité, l'intégrité, la confidentialité, la séparation, la possibilité d'intervention et la portabilité telles que définies dans le présent document alors que les mesures organisationnelles portent surtout sur la transparence (voir le point 3.4.3 pour plus de détails).

4.2 Certifications en matière de protection des données délivrée par des tiers

- Le contrôle ou la certification indépendants réalisés par un tiers de bonne réputation peut constituer un moyen réaliste pour les fournisseurs d'informatique en nuage de prouver qu'ils respectent leurs obligations telles qu'elles sont précisées dans le présent avis. Cette certification indiquerait au moins que les contrôles relatifs à la protection des données réalisés par un organisme tiers de bonne réputation ont été soumis à des audits ou à des examens menés en référence à des normes reconnues, et qui répondent aux exigences fixées dans le présent avis[45]. Dans le cadre de l'informatique en nuage,

[45] Parmi ces normes figurent celles émises par l'Organisation internationale de normalisation, le Conseil international des normes d'audit et d'assurance, et le Conseil des normes de l'Institut américain des

les clients potentiels devraient vérifier si les fournisseurs de services en nuage peuvent leur fournir un exemplaire du certificat d'audit du tiers ou encore du rapport d'audit attestant du contrôle, au regard notamment des exigences fixées dans le présent avis.

- La vérification individuelle des données, hébergées dans un environnement multipartite et virtuel de serveurs, peut s'avérer irréalisable du point de vue technique et peut dans certains cas augmenter les risques pour les contrôles physiques et logiques de sécurité des réseaux mis en place. Dans de tels cas, une vérification menée par un tiers choisi par le responsable du traitement peut être considérée comme pouvant se substituer au droit d'un responsable du traitement donné de procéder à un audit.
- L'adoption de normes et de certifications spécifiques à la protection de la vie privée est essentielle à l'établissement d'une relation de confiance entre les fournisseurs d'informatique en nuage, les responsables du traitement et les personnes concernées.
- Ces normes et certifications devraient couvrir les mesures techniques (telles que la localisation des données ou le cryptage) de même que les processus suivis par les fournisseurs d'informatique en nuage pour garantir la protection des données (tels que les politiques de contrôle d'accès, le contrôle d'accès ou les sauvegardes).

4.3 Recommandations: évolutions futures

Le Groupe de travail est parfaitement conscient du fait que les complexités de l'informatique en nuage ne peuvent pas être entièrement résolues par les garanties et les solutions décrites dans le présent avis, lequel constitue cependant une base solide pour sécuriser le traitement de données à caractère personnel que les clients établis dans l'EEE soumettent aux fournisseurs d'informatique en nuage. La présente section a pour but de mettre l'accent sur certaines questions qui doivent être abordées à court et à moyen terme pour renforcer les garanties en place et pour aider le secteur de l'informatique en nuage à résoudre les problèmes soulevés, tout en garantissant le respect des droits fondamentaux à la protection de la vie privée et à la protection des données.

- Un meilleur équilibre des responsabilités entre le responsable du traitement et le sous-traitant: le groupe de travail se félicite des dispositions figurant à l'article 26 de la proposition de la Commission européenne (proposition de règlement général sur la protection des données) qui tendent à rendre les sous-traitants plus responsables envers les responsables du traitement en les aidant à assurer le respect notamment de leurs obligations en matière de sécurité et de leurs obligations connexes. L'article 30 de la proposition prévoit l'obligation juridique pour le sous-traitant de mettre en œuvre les mesures techniques et organisationnelles qui s'imposent. Le projet de proposition précise qu'un sous-traitant qui ne se conforme pas aux instructions du responsable du traitement devient responsable du traitement et se trouve alors soumis aux règles spécifiques en matière de contrôle conjoint. Le groupe de travail «article 29» estime que cette proposition va dans la bonne direction pour remédier au déséquilibre qui caractérise généralement l'environnement d'informatique en nuage, dans lequel le client (particulièrement s'il est une PME) peut avoir du mal à exercer le plein contrôle, exigé par la législation sur la protection des données, sur la façon dont le fournisseur fournit les services demandés. De plus, les personnes concernées et les petites entreprises utilisatrices ne se trouvant pas dans la même situation juridique face aux grands fournisseurs

---

experts-comptables agréés (Auditing Standards Board of the American Institute of Certified Public Accountants), pour autant que ces organisations proposent des normes qui répondent aux exigences fixées dans le présent avis.

d'informatique en nuage, il est recommandé aux clients et aux entreprises commerciales de jouer un rôle plus dynamique pour négocier des conditions générales plus équilibrées après de ces fournisseurs.

- **Accès aux données à caractère personnel à des fins répressives et de sécurité nationale: il est primordial que le futur règlement prévoie d'interdire aux responsables du traitement qui exercent leurs activités dans l'UE de communiquer les données à caractère personnel à un pays tiers sur la demande de l'autorité judiciaire ou administrative de ce pays, sauf autorisation expresse découlant d'un accord international ou de traités d'entraide judiciaire ou sauf approbation de l'autorité de contrôle. Le règlement (CE) n° 2271/96 du Conseil constitue un bon exemple de fondement juridique approprié[46]. Ce déséquilibre dans la proposition de la Commission préoccupe le Groupe de travail, en ce qu'il implique une perte considérable de sécurité juridique pour les personnes concernées dont les données à caractère personnel sont stockées dans des centres de données à travers le monde. Pour cette raison, le Groupe de travail souhaiterait souligner[47] la nécessité d'inclure dans le règlement le recours obligatoire aux traités d'entraide judiciaire en cas de communication des données interdites par le droit de l'Union ou des États membres.**

- **Précautions particulières du secteur public: il convient d'ajouter une mise en garde particulière concernant la nécessité qu'un organisme public évalue en premier lieu si la communication, le traitement et le stockage des données en dehors du territoire national peuvent présenter des risques inacceptables de sécurité et de protection de la vie privée pour les citoyens et pour la sécurité nationale et l'économie – en particulier lorsque des bases de données sensibles (comme les données de recensement) ou des services stratégiques (comme les soins médicaux) sont en jeu[48]. Ce point mérite en tout cas d'être pris en considération chaque fois que des données confidentielles sont traitées dans le nuage. De ce point de vue, les gouvernements nationaux et les institutions de l'Union européenne pourraient envisager de poursuivre l'étude d'un nuage gouvernemental européen qui constituerait un espace virtuel supranational où pourraient s'appliquer des règles uniformes et harmonisées.**

---

46 Règlement (CE) n° 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant Journal officiel L 309, 29/11/1996, p. 1 - 6, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:FR:HTML

47 Voir WP 191 - Avis 01/2012 sur les propositions de réforme de la protection des données, page 23.

48 À cet égard, l'ENISA formule les recommandations suivantes dans son rapport intitulé "Security & Resilience in Governmental Clouds" (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): «Du point de vue de l'architecture, et pour ce qui est des applications sensibles, les nuages privés et communautaires semblent offrir la solution actuellement la mieux adaptée aux besoins des administrations publiques, en ce qu'ils offrent le niveau de gouvernance, de contrôle et de visibilité le plus élevé, même s'il convient de tenir dûment compte de l'ampleur de l'infrastructure au moment de mettre sur pied un nuage privé ou communautaire».

- **Partenariat européen dans le domaine du nuage informatique: le Groupe de travail soutient la stratégie de partenariat européen dans le domaine du nuage informatique présentée à Davos en janvier 2012 par M[me] Kroes, vice-présidente de la Commission européenne[49]. Cette stratégie suppose la passation de marchés publics informatiques pour stimuler le marché européen des services en nuage. Le transfert de données à caractère personnel à un fournisseur européen d'informatique en nuage, tenu en dernier ressort de respecter la législation européenne sur la protection des données, pourrait apporter des avantages considérables aux consommateurs en matière de protection des données, notamment en favorisant l'adoption de normes communes (particulièrement dans le domaine de l'interopérabilité et de la portabilité des données) et la sécurité juridique.**

[49] Discours de M[me] Neelie Kroes, vice-présidente de la Commission européenne chargée de la stratégie numérique, consacré à la mise en place d'un partenariat européen dans le domaine du nuage informatique et prononcé le 26 janvier 2012 à Davos, Suisse, lors du Forum économique mondial, consultable à l'adresse URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38&format=HTML&aged=1&language=EN&guiLanguage=fr

ANNEXE

a) Modèles de déploiement

Le nuage privé[50] est une infrastructure informatique attachée à une organisation particulière. Il peut être géré dans les locaux de l'organisation, ou être sous-traité à un tiers (généralement par le biais de l'hébergement de serveurs), placé sous le contrôle strict du responsable du traitement. Un nuage privé est comparable à un centre de données conventionnel – à la différence que des mécanismes technologiques sont mis en œuvre pour optimiser l'utilisation des ressources disponibles et valoriser ces ressources au moyen d'investissements limités et progressifs.

Le nuage public, à l'inverse, est une infrastructure qui appartient à un fournisseur spécialisé dans la prestation de services qui met ses systèmes à la disposition des utilisateurs, des entreprises et/ou des administrations publiques – et les partage donc avec eux. Les services sont accessibles par l'internet, ce qui nécessite le transfert des opérations de traitement des données et/ou des données elles-mêmes vers les systèmes du fournisseur de service. Ce dernier joue donc un rôle essentiel dans la protection effective des données stockées dans ses systèmes. En plus des données, l'utilisateur est tenu de transférer une grande part du contrôle qu'il exerce sur ces données.

Aux nuages «publics» et «privés» s'ajoutent les nuages dits «intermédiaires» ou «hybrides» dans lesquels des services fournis par des infrastructures privées coexistent avec des services achetés sur un nuage public. Les «nuages communautaires», dans lesquels l'infrastructure informatique est commune à plusieurs organisations au profit d'une communauté particulière d'utilisateurs, sont également à mentionner.

Leur flexibilité et la simplicité de leur configuration confèrent aux systèmes en nuage une capacité de dimensionnement «élastique», en ce sens qu'ils peuvent être adaptés aux exigences spécifiques, selon une approche basée sur l'utilisation. Les utilisateurs n'ont pas à gérer les systèmes informatiques, qui reposent sur des accords de sous-traitance et sont, pour cette raison, intégralement gérés par le tiers dans le nuage duquel les données sont stockées. Il est fréquent que de grands fournisseurs de services informatiques disposant d'infrastructures complexes interviennent, ce qui explique que le nuage puisse couvrir plusieurs sites et l'utilisateur, ignorer où exactement ses données sont stockées.

---

[50] Aux États-Unis, le NIST (National Institute of Standards and Technology) travaille depuis quelques années sur la normalisation des technologies en nuage et les définitions qu'il en donne sont également citées dans le rapport de l'ENISA:
Nuage privé.
L'infrastructure en nuage est utilisée par une seule organisation. Elle peut être gérée par l'organisation ou par un tiers, sur site ou hors site. Il convient de souligner qu'un «nuage privé» utilise certaines technologies qui sont également caractéristiques des «nuages publics» comme, notamment, les technologies de virtualisation qui favorisent la réorganisation ou la réforme de l'architecture informatique telle qu'elle est expliquée ci-dessus.
Nuage public.
L'infrastructure en nuage est mise à la disposition du grand public ou d'un grand groupe industriel et appartient à une organisation qui vend des services en nuage.

b) Modèles de services

Selon les besoins de l'utilisateur, plusieurs solutions d'informatique en nuage sont proposées sur le marché. Elles peuvent être regroupées en trois principales catégories ou «modèles de services», qui s'appliquent généralement aux solutions de nuage privé et de nuage public:

- **IaaS (de l'anglais «Cloud Infrastructure as a Service», infrastructure en tant que service):** un fournisseur loue une infrastructure technologique, c'est-à-dire des serveurs virtuels distants, auxquels l'utilisateur final peut faire appel en vertu d'accords et de mécanismes afin de remplacer les systèmes informatiques de l'entreprise dans les locaux de l'entreprise et/ou d'utiliser l'infrastructure louée conjointement aux systèmes de l'entreprise de manière simple, efficace et utile. Ces fournisseurs sont habituellement des acteurs spécialisés du marché qui peuvent effectivement s'appuyer sur une infrastructure physique, complexe, qui recouvre généralement plusieurs zones géographiques.
- **SaaS (de l'anglais «Cloud Software as a Service», logiciel en tant que service):** un fournisseur offre en ligne différents services d'application et les met à la disposition des utilisateurs finals. Ces services visent généralement à remplacer les applications conventionnelles que les utilisateurs doivent installer sur leurs systèmes locaux; en conséquence, les utilisateurs sont, à terme, censés externaliser leurs données vers le fournisseur particulier. C'est le cas, par exemple, des applications bureautiques web habituelles comme les tableurs, les outils de traitement de texte, les registres et agendas informatisés, les calendriers partagés, etc.; toutefois, les services en question comprennent également des applications de messagerie en nuage.
- **PaaS (de l'anglais «Cloud Platform as a Service», plateforme en tant que service):** un fournisseur propose des solutions de développement avancé et l'hébergement d'applications. Ces services s'adressent en général aux acteurs du marché qui les utilisent pour développer et héberger des solutions basées sur des applications propriétaires pour répondre aux besoins internes ou fournir des services à des tiers. Cette fois encore, les services fournis par un fournisseur PaaS rendent inutiles le recours par l'utilisateur à du matériel ou à des logiciels supplémentaires et/ou spécifiques au niveau interne.

Une parfaite transition vers un système en nuage entièrement public ne paraîtrait pas matériellement possible à court terme pour plusieurs raisons, s'agissant notamment des grandes entités comme les grandes entreprises ou organisations qui doivent remplir des obligations particulières – par exemple, les grandes banques, les organismes gouvernementaux, les grandes municipalités, etc. Il y a à cela deux raisons principales: premièrement, des facteurs dynamiques sont liés aux investissements nécessaires pour réaliser une telle transition; et deuxièmement, les informations particulièrement utiles et/ou confidentielles qui seront traitées dans les cas spécifiques doivent être prises en compte.

Un autre facteur qui milite en faveur des nuages privés (au moins dans les cas mentionnés ci-dessus) est lié au fait que le fournisseur du nuage public ne peut pas toujours garantir une qualité des services (sur la base d'accords sur les niveaux de service) propre à répondre à la nature cruciale du service fourni par le responsable du traitement – du fait peut-être que la largeur de bande et la fiabilité de l'internet ne sont pas suffisantes ou appropriées dans un secteur donné, ou bien au regard des connexions particulières entre utilisateur et fournisseur. D'un autre côté, on peut raisonnablement s'attendre à ce que les nuages privés puissent être loués, à bail ou non, dans certains des cas précédents (cela peut en effet s'avérer plus économique) ou à ce que des modèles de nuages hybrides (aux composantes à la fois publiques et privées) puissent être déployés. Il y a lieu d'examiner, dans tous les cas, les incidences significatives.

En l'absence de normes approuvées au niveau international, on court le risque de voir se développer des solutions de nuage «personnalisées», ou autrement fédérées, qui comportent des risques plus élevés de verrouillage (ainsi que des risques qui ont été désignés sous le

terme de «monocultures de la protection de la vie privée»)[51] et qui empêchent le plein contrôle sur les données sans garantir l'interopérabilité. L'interopérabilité et la portabilité des données sont en effet des facteurs clés du développement de la technologie en nuage de même qu'elles permettent le plein exercice des droits en matière de protection des données dévolus aux personnes concernées (tels que le droit d'accès ou de rectification).

[51] Voir l'étude du Parlement européen «Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy», publiée en décembre 2011.

De ce point de vue, le débat actuel sur les technologies en nuage constitue un exemple marquant des tensions qui existent entre les approches axées sur les coûts et les approches axées sur les droits, comme cela a été brièvement évoqué dans la section 2 ci-dessus. Bien qu'il soit matériellement possible – et même recommandé du point de vue de la protection des données – de recourir aux nuages privés, compte tenu des circonstances spécifiques du traitement, cela n'est pas toujours réalisable à long terme pour les organisations, surtout dans le cadre d'une approche axée sur les coûts. Une évaluation minutieuse des intérêts en jeu s'impose, dans la mesure où il n'existe actuellement aucune solution universelle dans ce domaine.