Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing

D'un point de vue juridique, la CNIL constate que le Cloud computing soulève un certain nombre de difficultés au regard du respect de la législation relative à la protection des données personnelles, en particulier dans le cas du Cloud public. Ces difficultés sont amplifiées dans le cas des offres standardisées avec des contrats d'adhésion ne laissant pas aux clients la possibilité de les négocier. De manière générale, il est constaté que les clients souffrent d'une insuffisance de transparence de la part des prestataires de Cloud quant aux conditions de réalisation des prestations, notamment sur la sécurité et sur la question de savoir si leurs données sont transférées à l'étranger, et plus précisément à destination de quels pays.

Par conséquent, il est indispensable qu'une entreprise française qui envisage de recourir à un service de Cloud computing réalise une analyse de risques et soit très rigoureuse dans le choix de son prestataire. En particulier, l'entreprise devra prendre en considération les garanties offertes par un prestataire en matière de protection des données personnelles et s'assurer que ce dernier lui fournira toutes les garanties nécessaires au respect de ses obligations au regard de la loi Informatique et Libertés, notamment en termes d'information des personnes concernées, d'encadrement des transferts et de sécurité des données. Il est à noter qu'en cas d'impossibilité de négocier un contrat, une comparaison des conditions contractuelles proposées par les différents prestataires est indispensable. Ceci permet d'effectuer un choix prenant en compte les considérations tant économiques que juridiques et techniques.

Concernant la sécurité, la CNIL constate que les offres de Cloud reconnues peuvent présenter des niveaux de sécurité supérieurs à ceux que peuvent garantir les PME. Cependant, le Cloud génère de nouveaux risques, tant du côté du prestataire que du côté du client, notamment au niveau de la pérennité des données. Il est donc nécessaire de s'assurer que ces nouveaux risques sont maitrisés avant de choisir une solution de Cloud.

La CNIL a établi les recommandations suivantes afin d'aider les entreprises françaises, notamment les PME, à effectuer une prise de décision éclairée lorsqu'elles envisagent d'avoir recours à des prestations de services de Cloud computing. Ces recommandations indicatives sont principalement basées sur une analyse de risques réalisée au préalable par les clients et des engagements de transparence des prestataires vis-à-vis de leurs clients qui doivent être formalisés dans les contrats de prestation de services.

Recommandation n°1 : Identifier clairement les données et les traitements qui passeront dans le Cloud

Avant d'envisager le recours au Cloud computing, le client responsable de traitement doit clairement identifier les données, traitements ou services qui pourraient être hébergés dans le Cloud.

Pour chaque traitement, il doit établir quels types de données pourraient être concernés en distinguant :

- les données à caractère personnel,
- les données sensibles[1],
- les données stratégiques pour l'entreprise,
- les données utilisées dans les applications métiers.

Dans le cas où une partie seulement des données et traitements est transférée dans le Cloud, comme par exemple le logiciel de messagerie, le client doit veiller à s'assurer que les traitements passés dans le Cloud ne risquent pas d'inclure des données d'autres traitements qui n'ont pas migré. Un tel exemple est l'utilisation d'une messagerie « Cloud » dans laquelle les collaborateurs échangent des contenus stratégiques pour l'entreprise.

Par ailleurs, certains types de données sont soumis à une réglementation spécifique, il est donc nécessaire de vérifier si les données qui pourraient être transférées dans le Cloud sont soumises à de telles obligations et, lorsque cela est le cas, d'identifier les conditions minimales à leur transfert. Par exemple, les données de santé ne peuvent être stockées que par un hébergeur de données de santé agréé par le Ministère de la santé.

Recommandation n°2 : Définir ses propres exigences de sécurité technique et juridique

Le passage au Cloud demande une approche rigoureuse en termes de sécurité technique et juridique.

Contrairement aux offres classiques d'externalisation, dans lesquelles les prestataires fournissent une réponse personnalisée à un cahier des charges défini par le client, de nombreuses offres de Cloud sont « standard » pour tous les clients et ne répondent pas à un cahier des charges particulier.

Pour autant, le client doit définir ses propres exigences et évaluer si les offres envisagées répondent à l'ensemble des exigences formulées. En effet, si le but du Cloud est de décharger le client de certaines tâches opérationnelles, il doit s'assurer *a priori* que le prestataire suit un niveau d'exigence au moins égal au sien.

[1] Données sensibles au sens de l'article 8 de la Loi Informatique et Libertés ou données relevant de l'article 9.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Les exigences doivent comprendre l'ensemble des points importants pour le client et considérer notamment :

- les contraintes légales (localisation des données, garantie de sécurité et de confidentialité, réglementations spécifiques à certains types de données, etc.) ;
- les contraintes pratiques (disponibilité, réversibilité/portabilité[2], etc.) ;
- et les contraintes techniques (interopérabilité avec le système existant, etc.).

Pour les données et les traitements « métier », le client doit particulièrement veiller à garantir la réversibilité et s'assurer qu'un niveau de disponibilité suffisant est garanti par le prestataire et par son fournisseur d'accès à Internet.

Recommandation n°3 : Conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise

Conduire une analyse de risques complète est essentiel pour être en mesure de définir les mesures de sécurité appropriée à exiger du prestataire ou à mettre en œuvre au sein de l'entreprise. La méthode EBIOS[3] constitue une méthode pertinente pour l'analyse de risques à condition que les données à caractère personnel soient considérées dans les biens à protéger et que les impacts sur la vie privée des personnes concernées soient pris en compte.

Pour les organismes qui n'ont pas les moyens de mener une analyse complète, la Commission souhaite mettre en avant les risques suivants, qui sont plus importants dans le cas du Cloud que dans le cas de traitements informatiques traditionnels, et qui sont particulièrement pertinents pour la protection des données personnelles. Une liste plus complète de 35 risques fournie par l'ENISA[4] peut aussi être utilisée.

Les principaux risques identifiés par notre Commission sont les suivants :

- perte de gouvernance sur le traitement ;
- dépendance technologique vis-à-vis du fournisseur de Cloud Computing, c'est-à-dire l'impossibilité de changer de solution (pour un autre fournisseur ou une solution interne) sans perte de données ;
- faille dans l'isolation des données, c'est-à-dire le risque que les données hébergées sur un système virtualisé soient modifiées ou rendues accessibles à des tiers non autorisés, suite à une défaillance du prestataire ou à une mauvaise gestion du rôle d'hyperviseur ;

[2] La réversibilité (ou portabilité) est la possibilité de pouvoir obtenir une copie de l'intégralité de ses données dans un format structuré et couramment utilisé. Ceci permet au responsable de traitement de s'assurer qu'il puisse changer de solution si besoin sans perte d'information (données, structure, etc.).

[3] La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI.

[4] Agence Européenne chargée de la sécurité des réseaux et de l'information, rapport disponible en anglais et en espagnol à l'adresse suivante : http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

- réquisitions judiciaires, notamment par des autorités étrangères ;
- faille dans la chaîne de sous-traitance, dans le cas où le prestataire a lui-même fait appel à des tiers pour fournir le service ;
- destruction ineffective ou non sécurisée des données, ou durée de conservation trop longue ;
- problème de gestion des droits d'accès par les personnes causé par une insuffisance de moyens fournis par le prestataire ;
- indisponibilité du service du prestataire, ce qui comprend l'indisponibilité du service en lui-même mais aussi l'indisponibilité des moyens d'accès au service (notamment les problèmes réseaux) ;
- fermeture du service du prestataire ou acquisition du prestataire par un tiers ;
- non-conformité réglementaire, notamment sur les transferts internationaux.

Dans le cas où une partie seulement des données et traitements sont transférés dans le Cloud, comme par exemple le logiciel de messagerie, le client doit également considérer l'impact de la migration partielle sur les traitements et données non transférés, par exemple si les données sensibles ou stratégiques sont explicitement exclues du transfert dans le Cloud, les traitements nécessitant l'envoi de telles données par courriel devront être adaptés.

La plupart des ces risques ont vocation à être réduits par des dispositions contractuelles, pouvant inclure des pénalités pour le prestataire, et par des mesures techniques et organisationnelles au niveau du client et du prestataire. La Commission recommande que le client évalue la pertinence de ces risques pour sa propre situation et étudie les mesures mises en place par lui-même et par le prestataire pour réduire ces risques.

Recommandation n°4 : Identifier le type de Cloud pertinent pour le traitement envisagé

Il existe différentes offres de services de Cloud computing sur le marché, qui peuvent être distinguées selon trois modèles de services et trois modèles de déploiement.

Les modèles de services sont les suivants :

- SaaS : « Software as a Service », c'est-à-dire la fourniture de logiciel en ligne ;
- PaaS : « Platform as a Service », c'est-à-dire la fourniture d'une plateforme de développement d'applications en ligne ;
- IaaS : « Infrastructure as a Service », c'est-à-dire la fourniture d'infrastructures de calcul et de stockage en ligne.

Les modèles de déploiement sont les suivants :

- « Public » quand un service est partagé et mutualisé entre de nombreux clients ;
- « Privé » quand le Cloud est dédié à un client ;

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

- « Hybride » quand un service est partiellement dans un Cloud public et partiellement dans un Cloud privé. Dans ce cas, nous considérons que le service peut être étudié comme deux traitements interconnectés. Nous ne ferons donc pas référence à ce modèle de déploiement.

Chaque offre de service de Cloud computing étant spécifique, il convient de les comparer en identifiant les forces et les faiblesses de chacune au regard du traitement considéré. Une telle analyse permettra de sélectionner l'offre de Cloud computing la mieux adaptée.

Il est à noter qu'il peut tout à fait être envisagé de choisir des solutions de Cloud computing différentes en fonction des traitements. Ainsi, il est par exemple possible de choisir un service IaaS public français pour le site Internet de l'entreprise, un hébergeur de santé homologué pour les données de santé et un SaaS européen privé pour les courriels.

Non seulement une telle conception permet de choisir l'offre la plus adaptée à chaque traitement particulier, mais elle permet également de garantir une meilleure protection des données collectées par une entreprise puisqu'elles ne sont pas toutes confiées au même prestataire de services de Cloud computing.

Enfin, une approche par étape peut permettre une transition vers le Cloud computing progressive et ainsi de mieux appréhender les risques particuliers du Cloud computing. Il sera alors possible de tirer profit des premières expériences afin de faire évoluer les pratiques internes et de mieux négocier ou mieux choisir les contrats suivants.

Le transfert du traitement ou des données dans le Cloud peut ainsi s'effectuer progressivement par catégorie de données et exigence de sécurité croissante, par exemple en commençant par le transfert des logiciels support (messagerie, agenda, contacts, etc.), puis par les applications contenant des données sensibles ou stratégiques (par exemple les traitements RH) et en finissant par les applications métiers.

Recommandation n°5 : Choisir un prestataire présentant des garanties suffisantes

En tant que responsables du traitement, les clients de services de Cloud computing doivent s'assurer qu'ils sont en mesure de remplir leurs obligations. Pour ce faire, ils doivent choisir des prestataires garantissant la mise en place de mesures de sécurité et de confidentialité appropriées, et qui soient transparents vis-à-vis de leurs clients sur les moyens employés pour exécuter leurs prestations (transfert de données à l'étranger, recours à des sous-traitants, politique et mesures de sécurité, etc.).

Le choix d'un prestataire doit être effectué en considération de la grille d'analyse suivante :

Etape n°1 : Déterminer la qualification juridique du prestataire

Lorsqu'un client fait appel à un prestataire de services, il est généralement admis que le premier est responsable de traitement et le second sous-traitant.

Toutefois, la CNIL constate que dans certains cas de PaaS et de SaaS publics, les clients, bien que responsables du choix de leurs prestataires, ne peuvent pas réellement leur donner d'instructions et ne sont pas en mesure de contrôler l'effectivité des garanties de sécurité et de

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

confidentialité apportées par les prestataires. Cette absence d'instruction et de moyens de contrôle est due notamment à des offres standardisées, non modifiables par les clients, et à des contrats d'adhésion qui ne leur laissent aucune possibilité de négociation.

Dans de telles situations, le prestataire pourrait *a priori* être considéré comme conjointement responsable en vertu de la définition de « responsable du traitement » fournie à l'article 2 de la directive 95/46/CE, puisqu'il participe à la détermination des finalités et des moyens des traitements de données à caractère personnel.

Dans le cas d'une responsabilité conjointe, il est pertinent que les responsabilités incombant à chaque partie soient clairement définies.

La CNIL suggère alors le partage des responsabilités suivant :

Hypothèse	Formalités déclaratives	Information des personnes	Obligation de confidentialité et sécurité	Exercice des droits des personnes concernées auprès du …
Le prestataire est conjointement responsable du traitement	**Client**[5]	**Client**[6]	**Client + Prestataire**	**Client (avec le concours du prestataire)**[7]

Identifier si le prestataire est responsable conjoint du traitement ou non permet de déterminer qui est responsable vis-à-vis des autorités compétentes de protection des données personnelles.

En effet, en vertu des pouvoirs qui lui sont conférés par la loi Informatique et Libertés, la CNIL peut contrôler et sanctionner tout responsable du traitement qui ne respecterait pas ses obligations conformément à la loi Informatique et Libertés. Par conséquent, si le client et le prestataire sont conjointement responsables du traitement, ils seront tous deux susceptibles d'être contrôlés et potentiellement sanctionnés.

[5] Le client et le prestataire auront des obligations déclaratives auprès de la CNIL concernant le traitement dont ils sont conjointement responsables. Ils devront alors déterminer qui d'entre eux effectuera ces formalités. La CNIL recommande que ce soit le client qui s'en charge, puisque le recours à un prestataire de Cloud peut s'inscrire dans un traitement plus général, mais il est tout à fait envisageable que ce soit le prestataire qui s'acquitte des formalités pour son compte et pour celui du client. Dans tous les cas, la partie en charge de ces formalités déclaratives devra être en mesure de fournir la preuve, sur demande de l'autre partie, qu'elles ont été dûment effectuées auprès de la CNIL.

[6] Bien que l'obligation d'information incombe à la fois au client et au prestataire tous deux responsables de traitement, il est souhaitable qu'en pratique ce soit l'entité à laquelle la personne concernée a communiqué ses données qui l'informe des moyens de traitement auxquels le prestataire a recours. Par conséquent, le prestataire doit fournir au client toutes les informations nécessaires au respect de cette obligation d'information. Toutefois, le prestataire doit rester la personne de contact à laquelle la personne concernée devra s'adresser pour obtenir davantage d'information sur le traitement pour lequel le prestataire agit comme responsable conjoint du traitement.

[7] La dissémination possible des données sur différents serveurs localisés dans divers pays peut rendre plus compliqué l'exercice de leurs droits par les personnes concernées. Il convient alors de s'assurer que le prestataire et le client mettent en œuvre les garanties nécessaires pour permettre aux personnes concernées d'exercer leurs droits d'accès, de rectification, de modification, de mise à jour ou d'effacement.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Etape n°2 : Evaluer le niveau de protection assuré par le prestataire aux données traitées

Quelle que soit la qualification du prestataire, il est de la responsabilité du client de choisir un prestataire qui assure un niveau de protection suffisant aux données qu'il lui confie.

La CNIL a listé ci-après les éléments essentiels, au regard de la protection des données personnelles, devant figurer dans un contrat de prestation de services de Cloud computing.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Eléments essentiels devant figurer dans un contrat de prestation de services de Cloud computing

Informations relatives aux traitements

- Respect des principes européens en matière de protection des données personnelles et de la loi Informatique et Libertés (notamment des principes de proportionnalité et de respect des finalités) ;
- Existence d'un système de remontée des plaintes et des failles de sécurité ;
- Moyens de traitement ;
- Destinataires des données ;
- Sous-traitance :
  - Information et obtention du consentement du client en cas d'utilisation de tiers ou de sous-contractants situés ou non à l'étranger pour participer à la réalisation du traitement (Note : *si le prestataire est responsable conjoint du traitement, il devra seulement informer le client et non pas obtenir son consentement*) ;
  - Report dans les contrats de sous-traitance ultérieurs contractés par le prestataire des obligations contractuelles prévues dans le contrat de prestation signé entre le client et le prestataire et organisation de la responsabilité contractuelle des sous-contractants vis-à-vis du prestataire et du client.
- Existence de procédures simples permettant de respecter les droits des personnes concernées vis-à-vis de leurs données (droits d'accès, modification ou suppression, etc.).

Garanties mises en œuvre par le prestataire

- Durée de conservation des données limitée et raisonnable au regard des finalités pour lesquelles les données ont été collectées ;
- Destruction et/ou restitution des données en fin de prestation ou en cas de rupture anticipée du contrat dans un format structuré et couramment utilisé ;
- Devoir de coopération avec les autorités de protection des données compétentes ;
- Lorsque le prestataire est sous-traitant, indication que le client peut procéder à des audits du prestataire afin de s'assurer que ces garanties sont effectivement mises en œuvre.

Localisation et transferts

- Indication claire et exhaustive des pays hébergeant les centres de données du prestataire où les données seront traitées ;

- Assurance d'une protection adéquate à l'étranger (notamment grâce à des Clauses contractuelles types ou à des règles contraignantes d'entreprise « BCR ») ;

- Possibilité de limiter les transferts de données uniquement vers des pays membres de l'Espace Economique Européen ou vers des pays tiers reconnus comme assurant un niveau de protection adéquat par décision de la Commission européenne (*Note : Au contraire des autres éléments, celui-ci est laissé à la négociation des parties. En tout état de cause, un prestataire qui laisse la possibilité à ses clients de limiter les transferts de données vers des pays membres de l'EEE ou vers des pays tiers assurant un niveau de protection adéquat reconnu par la Commission européenne offrira à ses clients des garanties de protection des données renforcées. Toutefois, les clients doivent être conscients que lorsqu'ils choisissent des prestataires localisés dans des pays tiers, les autorités administratives ou judiciaires locales peuvent adresser des requêtes aux prestataires pour accéder aux données) ;*

- Information immédiate du client en cas de requête provenant d'une autorité administrative ou judiciaire étrangère.

Formalités auprès de la CNIL

- Lorsque le prestataire est sous-traitant, obligation de fournir au client toute information utile permettant de procéder à la déclaration du traitement auprès de la CNIL ;

- Lorsque le prestataire est responsable conjoint du traitement, le client et le prestataire doivent déterminer quelle partie sera en charge des formalités pour son compte et pour celui de l'autre partie. Quelle que soit la solution choisie, la partie qui ne déclare pas devra fournir à celle qui effectuera les formalités déclaratives toute information utile permettant de procéder à la déclaration du traitement auprès de la CNIL.

Sécurité et confidentialité

- Indication des obligations incombant au prestataire en matière de sécurité des données et, lorsque celui-ci est sous-traitant, précision qu'il ne peut agir que sur instruction du client ;

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

- Politique de sécurité et mesures minimales de sécurité :

[Note : le prestataire sous-traitant devra tenir à la disposition du client le détail des mesures mises en place, tandis que le prestataire responsable conjoint du traitement devra seulement garantir que des mesures suffisantes ont été mises en œuvre.]

  - Existence d'une politique de sécurité accessible ;

  - Mesures de sécurité et sûreté physique sur le site d'hébergement (protection du site et sécurité des accès, sécurité électrique et système de climatisation, etc.) ;

  - Mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données : par exemple, chiffrement des données et procédés garantissant ainsi que le prestataire n'a pas accès aux données qui lui sont confiées (chiffrement côté client, avec un algorithme reconnu et une gestion des clés adéquate, avant tout transfert) et liaison chiffrée avec le serveur de Cloud (connexion de type https ou VPN par exemple), etc. ;

  - Autres mesures de sécurité logique (protection du réseau (pare-feu, antivirus, détection d'intrusion, etc.), gestion des mises à jour, protection du terminal, gestion des habilitations, authentification des personnels, sécurité des développements applicatifs, etc.) ;

- Certifications : preuve de certifications pertinentes par des auditeurs indépendants et qualifiés, par exemple une certification ISO 27001 sur un périmètre incluant intégralement les services fournis, définition rigoureuse d'une politique d'audit du prestataire par le client comprise dans les garanties générales *[Note : au contraire des autres éléments, la certification est laissé à la négociation des parties. En tout état de cause, un prestataire qui dispose d'une certification offrira à ses clients des garanties de protection des données renforcées]* ;

- Réversibilité/portabilité : garantir la réversibilité ou la portabilité aisée des données dans un format structuré et couramment utilisé, sur demande du client et à tout moment ;

- Traçabilité : accès aux journaux de traçabilité des actions effectuées sur les données par les personnels du client et par ceux du prestataire et information de toute anomalie détectée par le prestataire ;

- Continuité de service, sauvegardes et intégrité : système de sauvegarde, redondance des serveurs, etc. ;

- Engagement de niveaux de services (« *Service Level Agreements* » ou « *SLAs* ») : engagements contraignants pour le prestataire sur le niveau de service, devant notamment prévoir des pénalités pour le prestataire en cas de non-respect des engagements contractuels. Ceci doit être mis en place en particulier pour les clauses relatives à la protection des données (durée de conservation, exercice des droits des personnes concernées, disponibilité du traitement, etc.).

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Au vu de ces éléments essentiels identifiés par la CNIL, des modèles de clauses contractuelles pouvant être insérées dans les contrats de prestations de service sont proposés en annexe.

Ces modèles de clauses ont vocation à aider les sociétés clientes de services de Cloud, notamment les PME, à choisir un prestataire qui offre toutes les garanties nécessaires en termes de protection des données personnelles et de sécurité au regard de la loi Informatique et Libertés.

La CNIL rappelle que si ces éléments essentiels ne figurent pas directement ou indirectement dans un contrat de prestation, les clients ne seront pas en mesure de satisfaire aux obligations légales qui leur incombent en leur qualité de responsables de traitement.

Par conséquent, les prestataires qui n'offrent pas ces garanties essentielles dans leurs contrats et qui refusent toute négociation avec leurs clients potentiels ne devraient pas être sélectionnés. En effet, en acceptant de telles conditions contractuelles insuffisantes, les clients s'exposent à un risque élevé de non-conformité à la législation en vigueur.

En outre, lorsqu'il n'est pas possible de négocier un contrat de prestation de Cloud computing avec un prestataire, ces éléments essentiels doivent également servir de base aux clients pour comparer les différentes offres disponibles sur le marché et faire un choix pertinent qui tiendra compte de leurs obligations légales.

Recommandation n°6 : Revoir la politique de sécurité interne

Le Cloud computing suppose une révision complète des procédures internes conformément aux conclusions de l'analyse de risques. En effet, le recours au Cloud introduit de nouveaux risques liés en particulier aux transmissions par internet ou à l'utilisation de terminaux mobiles et nomades. Une attention particulière doit être apportée aux mécanismes d'authentification des employés et le prestataire de Cloud doit proposer un service compatible avec ces exigences de sécurité.

Recommandation n°7 : Surveiller les évolutions dans le temps

Dans un esprit d'amélioration continue, la Commission recommande de réaliser périodiquement une évaluation du service de Cloud computing en fonction de l'évolution dans le temps du contexte, des risques, des solutions disponibles sur le marché, de la législation, etc.

En particulier, la mise à jour de l'analyse de risques préconisée est nécessaire dès qu'une évolution significative du service a lieu afin d'adapter les mesures ou les solutions dès que nécessaire. Ces évolutions peuvent concerner les fonctionnalités du produit ou la fourniture technique du service (nouveau centre de données, changement de politique de sécurité, évolution du traitement initiée par le client, etc.).

Annexe : Modèles de clauses contractuelles

La CNIL propose des modèles de clauses contractuelles reprenant les éléments essentiels énumérés à la recommandation n°5. Ces modèles peuvent être insérés dans les contrats de prestations de services de Cloud computing.

Notons qu'à elles seules, ces clauses ne constituent pas un contrat de prestation de services. De plus, il peut être nécessaire de les adapter en fonction du contexte, des cocontractants, etc.

Note : Les mots commençant par une majuscule devront être définis dans la partie « Définitions » du contrat (« Client », « Prestataire », « Parties », « Données », « Prestation », « Traitement », etc.).

1) Informations relatives aux traitements

a) Respect des principes français en matière de protection des données personnelles

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Les Parties s'engagent à collecter et à traiter toute donnée personnelle en conformité avec toute réglementation en vigueur applicable au traitement de ces données, et notamment à la loi n°78-17 du 6 janvier 1978 modifiée. Au regard de cette loi, le Client est responsable du Traitement réalisé au titre du Contrat. »

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Les Parties s'engagent à collecter et à traiter toute donnée personnelle en conformité avec toute réglementation en vigueur applicable au traitement de ces données, et notamment à la loi n°78-17 du 6 janvier 1978 modifiée. Au regard de cette loi, les Parties sont conjointement responsables du Traitement réalisé au titre du Contrat. »

b) Existence d'un système de remontée des plaintes et des failles de sécurité

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Le Prestataire s'engage à communiquer au Client la survenance de toute faille de sécurité ayant des conséquences directes ou indirectes sur le Traitement, ainsi que toute plainte qui lui serait adressée par tout individu concerné par le Traitement réalisé au titre du Contrat. Cette communication devra être effectuée dans les plus brefs délais et au maximum quarante-huit heures après la découverte de la faille de sécurité ou suivant réception d'une plainte. »

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

c) Moyens de traitement

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« *Afin d'exécuter la Prestation, le Prestataire traitera les Données par le biais des moyens de traitement suivants : [fournir une description des moyens logiciels et techniques de traitement utilisés par le Prestataire]*. »

d) Sous-traitance

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Prestataire informe le Client, qui l'accepte, qu'il fera sous-traiter l'exécution du Contrat par les sous-contractants suivants : [indiquer leurs noms et leur pays d'établissement s'ils sont établis dans un pays tiers].

Le cas échéant, le Prestataire s'engage à reporter dans les engagements qu'il contractera avec des sous-contractants les obligations qui lui incombent au titre du Contrat.

Le Prestataire restera seul responsable vis-à-vis du Client de l'exécution de ses obligations contractuelles résultant du présent contrat. »

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Lorsque le Prestataire a recours à des sous-contractants, il devra en informer le Client et lui fournir la liste des destinataires des données.

Le cas échéant, le Prestataire s'engage à reporter dans les engagements qu'il contractera avec des sous-contractants les obligations qui lui incombent au titre du Contrat.

Le Prestataire restera seul responsable vis-à-vis du Client de l'exécution de ses obligations contractuelles résultant du présent contrat. »

e) Existence de procédures simples permettant de respecter les droits des personnes concernées vis-à-vis de leurs données

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Prestataire s'engage à coopérer avec le Client et à l'aider à satisfaire aux exigences légales relatives à la protection des données à caractère personnel qui incombent à ce dernier, afin notamment de respecter les droits des personnes concernées en vertu des articles 38 à 43 de la loi n°78-17 du 6 janvier 1978 modifiée. »

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Les Parties s'engagent à mettre en œuvre des procédures simples permettant aux personnes concernées d'exercer leurs droits en vertu des articles 38 à 43 de la loi n°78-17 du 6 janvier 1978 modifiée. »

2) Garanties mises en œuvre par le prestataire

a) Durée de conservation des données limitée et raisonnable au regard des finalités pour lesquelles les données ont été collectées

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Prestataire s'engage à ne pas conserver les Données au-delà de la durée de conservation fixée par le Client au regard des finalités pour lesquelles elles ont été collectées, et en tout état de cause à ne pas les conserver après la fin du Contrat. »

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Le Prestataire s'engage à ne pas conserver les Données au-delà de la durée de conservation fixée en concertation avec le Client au regard des finalités pour lesquelles elles ont été collectées, et en tout état de cause à ne pas les conserver après la fin du Contrat. »

b) Destruction et/ou restitution des données

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Au terme du Contrat ou en cas de rupture anticipée de ce dernier pour quelque cause que ce soit, le Prestataire et ses éventuels sous-contractants restitueront sans délai au Client une copie de l'intégralité des Données dans le même format que celui utilisé par le Client pour communiquer les Données au Prestataire ou à défaut, dans un format structuré et couramment utilisé.

Cette restitution sera constatée par procès-verbal daté et signé par les Parties.

Une fois la restitution effectuée, le Prestataire détruira les copies des Données détenues dans ses systèmes informatiques dans un délai raisonnable et devra en apporter la preuve au Client dans un délai raisonnable suivant la signature du procès-verbal de restitution. »

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

c) Devoir de coopération avec les autorités de protection des données compétentes

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Les Parties s'engagent à coopérer avec les autorités de protection des données compétentes, notamment en cas de demande d'information qui pourrait leur être adressée ou en cas de contrôle. »

d) Audits

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Client se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le Prestataire de ses obligations au titre du Contrat, notamment par le biais d'un audit.

Le Prestataire s'engage à répondre aux demandes d'audit du Client et effectuées par le Client lui-même ou par un tiers de confiance qu'il aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Prestataire, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit au Client.

Les audits doivent permettre une analyse du respect du présent Contrat et de la loi Informatique et Libertés, notamment :

- *par la vérification de l'ensemble des mesures de sécurité mises en œuvre par le Prestataire,*
- *par la vérification des journaux de localisation des Données, de copie et de suppression des Données,*
- *par l'analyse des mesures mises en place pour supprimer les Données, pour prévenir toutes transmissions illégales de Données à des juridictions non adéquates ou pour empêcher le transfert de Données vers un pays non autorisé par le Client.*

L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié. »

Note : Lorsque le prestataire est responsable conjoint du traitement, il n'est pas requis que le client ait la possibilité d'effectuer des audits auprès du prestataire, ceci est cependant une garantie supplémentaire pour le client.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

3) Localisation et transferts

a) Destinataires

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Le Prestataire devra fournir au Client toute information utile concernant les destinataires des Données, afin que ce dernier soit en mesure d'informer les personnes concernées par le Traitement et de répondre à leurs demandes d'accès en vertu des articles 32 et 39 de la loi n°78-17 du 6 janvier 1978 modifiée. »

b) Indication claire et exhaustive des pays hébergeant les serveurs du prestataire

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Prestataire informe le Client que les Données seront hébergées dans des serveurs localisés dans les pays suivants : [fournir une liste exhaustive des pays hébergeant les serveurs du prestataire].

En cas de modification des pays destinataires par le Prestataire, ce dernier devra en informer préalablement le Client sans délai et obtenir son consentement écrit. Le cas échéant, le Prestataire devra fournir au Client une liste des pays destinataires mise à jour. »

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Le Prestataire informe le Client que les Données seront hébergées dans des serveurs localisés dans les pays suivants : [fournir une liste exhaustive des pays hébergeant les serveurs du prestataire].

En cas de modification des pays destinataires par le Prestataire, ce dernier devra en informer le Client sans délai. Le cas échéant, le Prestataire devra fournir au Client une liste des pays destinataires mise à jour. »

c) Assurance d'une protection adéquate à l'étranger (notamment grâce à des Clauses contractuelles types ou à des règles contraignantes d'entreprise « BCR »)

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Client doit s'assurer que des garanties suffisantes sont apportées pour encadrer les transferts des Données, notamment par la mise en œuvre de règles contraignantes d'entreprise (« BCR ») sous-traitants ou par la signature des clauses contractuelles types 2010/84/UE adoptées par la Commission européenne avec les parties intéressées, comprenant le Prestataire et les éventuels sous-contractants. »

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Note : A l'heure où nous publions ce document, les BCR sous-traitants ont été adoptés par le Groupe de travail de l'article 29 (G29) mais l'avis n'a pas encore été publié. Ils ne constitueront donc un moyen de protection adéquat qu'à compter de la publication de l'avis du G29.

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Les Parties doivent s'assurer que des garanties suffisantes sont apportées pour encadrer les transferts des Données, notamment par la mise en œuvre de règles contraignantes d'entreprise (« BCR ») ou par la signature des clauses contractuelles types adoptées par la Commission européenne avec les parties intéressées, comprenant les éventuels sous-contractants. »

d) Possibilité de limiter les transferts de données uniquement vers des pays tiers assurant un niveau de protection adéquat

Note : Au contraire des autres éléments celui-ci est laissé à la négociation des parties. En tout état de cause, un prestataire qui laisse la possibilité à ses clients de limiter les transferts de données vers des pays membres de l'Espace Economique Européen ou vers des pays tiers assurant un niveau de protection adéquat reconnu par la Commission européenne offrira à ses clients des garanties de protection des données renforcées. Toutefois, les clients doivent être conscients que lorsqu'ils choisissent des prestataires localisés dans des pays tiers, les autorités administratives ou judiciaires locales peuvent adresser des requêtes aux prestataires pour accéder aux données (cf. clause 3.e) ci-après).

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Lorsque le Client a consenti à ce que le Prestataire ait recours à un ou plusieurs sous-contractant(s), les Parties conviennent que les Données ne pourront être transférées par le Prestataire qu'à destination de sous-contractants établis dans des pays membres de l'Espace Economique Européen et/ou de pays tiers reconnus par la Commission européenne comme assurant un niveau de protection adéquat. »

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Lorsque le Prestataire a recours à un ou plusieurs sous-contractant(s), les Parties conviennent que les Données ne pourront être transférées par le Prestataire qu'à destination de sous-contractants établis dans des pays membres de l'Espace Economique Européen et/ou de pays tiers reconnus par la Commission européenne comme assurant un niveau de protection adéquat. »

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

e) Information du client en cas de requête provenant d'une autorité administrative ou judiciaire étrangère

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« En cas de requête provenant d'une autorité administrative ou judiciaire reçue par le Prestataire, ce dernier s'engage à en informer immédiatement le Client.

4) Formalités auprès de la CNIL

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Client s'acquittera des formalités déclaratives relatives au Traitement auprès des autorités de protection des données à caractère personnel compétentes. Le Prestataire s'engage à lui fournir toute information utile afin de procéder à ces formalités. »

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Les Parties conviennent que [choisir entre le Client ou le Prestataire] s'acquittera des formalités déclaratives relatives au Traitement auprès des autorités de protection des données à caractère personnel compétentes. [Le Client ou le Prestataire, selon ce qui aura été décidé] fournira à la partie déclarante toute information utile afin de procéder à ces formalités.

[Le Client ou le Prestataire, selon ce qui aura été décidé] fournira à l'autre partie, sur simple demande, la preuve que les formalités requises ont été effectuées. »

5) Sécurité et confidentialité

a) Indication des obligations incombant au prestataire en matière de sécurité des données et, lorsque celui-ci est sous-traitant, précision qu'il ne peut agir que sur instruction du client

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Dans le cadre de l'exécution du Contrat, le Prestataire agira uniquement sur les instructions du Client. A ce titre, le Prestataire s'engage à ne pas utiliser les Données pour son propre compte ou pour celui d'un tiers.

Conformément à l'article 34 de la loi Informatique et Libertés modifiée, le Prestataire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment de les protéger contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés, notamment lorsque le Traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées. »

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Conformément à l'article 34 de la loi Informatique et Libertés modifiée, le Prestataire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment de les protéger contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés, notamment lorsque le Traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées. »

b) Politique de sécurité et mesures de sécurité

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est sous-traitant]

« Le Prestataire fournit au Client la politique de sécurité des systèmes d'information qu'il a mise en place et l'informe des évolutions de cette politique. Il tient à la disposition du client les documents relatifs à la sécurité de ses données comprenant notamment la documentation technique nécessaire, les analyses de risques produites et la liste détaillée des mesures de sécurité mises en œuvres.

Les supports informatiques et documents fournis par le Client au Prestataire restent la propriété du Client.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont le Prestataire prend connaissance à l'occasion de l'exécution du Contrat.

Le Prestataire s'engage à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au Contrat avec l'accord préalable du Client ;

- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;

- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;

- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat. »

[Le modèle de clause suivant peut être utilisé lorsque le prestataire est responsable conjoint du traitement]

« Le Prestataire fournit au Client la politique de sécurité des systèmes d'information qu'il a mise en place et l'informe des évolutions de cette politique. Il informe le Client des risques potentiels liés au Traitement.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Les supports informatiques et documents fournis par le Client au Prestataire restent la propriété du Client.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont le Prestataire prend connaissance à l'occasion de l'exécution du présent Contrat. »

c) Certification

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

Note : Au contraire des autres éléments, la clause ci-dessous est laissée à la négociation des parties. En tout état de cause, un prestataire qui dispose d'une certification pourra offrir à ses clients des garanties de protection des données renforcées.

« Le Prestataire informe le Client qu'il dispose de la certification [inscrire le nom de la certification obtenue par le prestataire] sur le périmètre concerné par le Traitement mis en œuvre par le Client. Le Prestataire communiquera au Client le périmètre concerné par la certification. Par ailleurs, il s'engage à maintenir pendant toute la durée du Contrat les critères permettant de répondre aux exigences de la certification obtenue. »

d) Réversibilité/portabilité des données

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Sur demande du Client, à tout moment et pour quelque cause que ce soit, le Prestataire et ses éventuels sous-contractants fourniront sans délai au Client une copie de l'intégralité de ses Données dans le même format que celui utilisé par le Client pour communiquer les Données au Prestataire ou à défaut, dans un format structuré et couramment utilisé. »

e) Traçabilité

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Le Prestataire tient à la disposition du Client les traces de connexion aux Données traitées par les personnels autorisés des Parties et, le cas échéant, des personnes concernées, et ce pendant une durée de [inscrire la durée de conservation des traces de connexion par le prestataire] mois. »

Note 1 : Il est recommandé que cette durée soit de trois ou six mois, en fonction de la confidentialité des données traitées.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Note 2 : Si le prestataire participe à l'analyse des traces de connexion aux données ou s'il propose au client un service d'analyse des traces de connexion aux données, il conviendra d'ajouter la clause ci-après :

« *Le Prestataire informe le Client de toute anomalie qu'il détectera dans ces traces de connexion.* »

f) Continuité de service, sauvegardes et intégrité

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Le Prestataire s'engage à prendre les mesures nécessaires pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du Contrat.

Il s'engage à utiliser un système de sauvegarde des Données et de continuité de service dont le détail est fourni dans l'accord de niveau de service annexé au Contrat. »

g) Engagements de niveau de service

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Le Prestataire s'engage sur les niveaux de service définis dans l'accord de niveau de service annexé au Contrat. »

Note : annexer au contrat de prestation de services un accord de niveau de service.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00