



## **FEEDBACK TO THE CNIL CONSULTATION**

The European Privacy Association (EPA) brings together experts on privacy and data protection from across Europe and represents a unique European platform enhancing dialogue among all stakeholders, such as decision-makers, researchers, privacy commissions, NGOs, industry and the media.

EPA informs and educates the general public about industry efforts to improve privacy, e- security and data protection, providing a unified response to public concerns. Extremely aware of the global aspect of privacy and data protection, EPA develops policies and produces legal and scientific positions engaging with policymakers at every level across Europe: the European Parliament, the Commission, Member State regulatory authorities and international organizations.

EPA activity is primarily focused on cyber security, online ads and profiling, cloud computing, mobility, e-government and citizens data, RFID, privacy, terrorism, spamming, search engines, social networks, and the economy of human information.

# **Consultation relative au Cloud computing**

Consultation ouverte du 17 octobre au 17 novembre 2011

**Fiche de présentation de la partie prenante à la consultation  
(toutes les informations sont facultatives)**

**Nom de la société**

European Privacy Association

**Secteur d'activité :**

Think-tank

**Pays dans lequel se trouve l'établissement principal :**

Belgium

**Pour le Cloud computing, vous êtes :**

**Un prestataire**

**Un Client**

Merci de renvoyer ce document

- **par voie électronique** à [consultationcloud@cnil.fr](mailto:consultationcloud@cnil.fr)
- **ou par courrier papier** à

**Commission Nationale Informatique et Libertés CNIL**  
**Service des affaires européennes et internationales**  
**8 Rue Vivienne**  
**75002 PARIS.**

**Terminologie / abréviations :**

Dans le cadre de cette consultation, la société offrant des services de Cloud computing sera dénommée « prestataire », les entreprises et administrations clientes de prestataires de Cloud seront appelées « client ».

## I. Définition du Cloud computing

### A. Le Constat de la CNIL

Le terme Cloud computing étant à la fois récent et recouvrant de nombreuses notions, il n'y a pas encore de consensus pour en donner une définition précise.

### B. Solution proposée

Une approche fondée sur les éléments caractéristiques du Cloud computing nous semble ici plus appropriée.

La CNIL propose donc de retenir le faisceau d'indices suivant afin de caractériser l'existence d'une prestation de Cloud computing :

- **simplicité d'un service à la demande** : un utilisateur peut de manière unilatérale, immédiatement et généralement sans intervention humaine, avoir à disposition les ressources informatiques dont il a besoin (temps de calcul de serveurs, capacité de stockage, etc.).
- **extrême flexibilité** : les ressources mises à disposition ont une capacité d'adaptation forte et rapide à une demande d'évolution, généralement de manière transparente pour l'utilisateur.
- **accès « léger »** : l'accès aux ressources ne nécessite pas d'équipement ou de logiciel propriétaire. Il se fait au travers d'applications facilement disponibles (parfois libres<sup>1</sup>), généralement depuis un simple navigateur Internet.
- **virtualisation des ressources** : les ressources informatiques du prestataire sont configurées pour être utilisées par une multitude de machines et sont souvent réparties dans différents centres d'hébergements (éventuellement dans différents endroits de la planète).
- **paiement « à l'usage »** : le paiement de la prestation de Cloud computing peut s'effectuer proportionnellement à l'usage.

---

<sup>1</sup> Une application / logiciel libre est une application/logiciel dont la licence donne à chacun (et sans contrepartie) le droit d'utiliser, d'étudier, de modifier, de dupliquer, et de diffuser le dit logiciel. Il existe également des systèmes d'exploitation libres comme LINUX.

C. Question posée

**Ce faisceau d'indices permet-il selon vous de caractériser une prestation de Cloud computing ? Selon vous, faut-il compléter ce faisceau d'indices ?**

**Réponse**

Yes, these elements certainly characterize Cloud computing services and shall be taken into account. However, they only take into consideration the position of the final client. It shall be stressed at the same time that:

(i) Cloud computing implies relatively new paradigms also for the providers – such as the utilization of several different servers or bundles of servers that work in close cooperation each other and that can be located in different geographical locations (in this sense Cloud computing is the direct consequence of Grid computing). This point has been mentioned under the entry ‘virtualization of resources’ but must be stressed because it is one of the core elements of Cloud computing;

(ii) Cloud users cannot only access remotely-stored software (according to the paradigm of Software as a Service – SaaS) but also middleware, infrastructure (a sort of virtualized hardware) as a service etc. (respectively MaaS, IaaS, etc.).

## II. La qualification des parties : vers une présomption de sous-traitance ?

### A. Le principe

Aux termes de l'article 3 de la loi de 1978, le responsable de traitement est défini comme la personne physique ou morale qui détermine les finalités et les moyens du traitement de données à caractère personnel. Le sous-traitant quant à lui, traite les données à caractère personnel pour le compte du responsable de traitement et selon ses instructions.

### B. Solution proposée

#### 2. Le client

Le client sera toujours responsable de traitement. En effet, en collectant des données et en décidant d'en externaliser le traitement auprès d'un prestataire, il est responsable de traitement en ce qu'il détermine les finalités et les moyens de traitement des données.

#### 3. Le prestataire

En principe, le prestataire agit pour le compte et sur les instructions du client responsable de traitement.

Dès lors, il semble possible d'établir **une présomption de sous-traitance** dans la relation qu'entretiennent le client et le prestataire.

Une telle présomption sera particulièrement effective lorsque le client aura recours à un Cloud privé<sup>2</sup> qui implique une grande maîtrise de la réalisation de la prestation du Cloud.

En revanche, lorsqu'un client a recours à un Cloud public<sup>3</sup>, les rôles respectifs du client et du prestataire peuvent s'avérer difficiles à déterminer, et dépendront également du type de services souscrit par le client. La Commission propose que la présomption de sous-traitance puisse tomber en application d'un faisceau d'indices qui doit permettre de déterminer la marge de manœuvre dont dispose le prestataire pour réaliser la prestation de services.

---

<sup>2</sup> Dans le Cloud privé, les ressources informatiques (infrastructure, applications, etc.) sont mises à disposition d'une seule et même organisation. Ces ressources peuvent être détenues, gérées et administrées par l'organisation elle-même ou par un tiers. Dans tous les cas, l'organisation a généralement une maîtrise sur l'infrastructure associée et la localisation des données. Lorsque l'infrastructure est partagée entre plusieurs organisations supportant une communauté précise et ayant des préoccupations communes, on parle alors de « Clouds communautaires ».

<sup>3</sup> Dans le Cloud public, les ressources informatiques sont exploitées par des tiers et font coexister les tâches soumises par un grand nombre de clients sur les mêmes serveurs, systèmes de stockage et autres composants de l'infrastructure. L'utilisateur final n'a généralement aucun moyen de savoir quels autres usagers sont présents sur le serveur, le réseau ou le disque sur lequel ses tâches sont exécutées.

**Critère**

**Niveau d'instruction**

**Signification**

Evaluer dans quelle mesure le prestataire est tenu par les instructions du client.

**Degré de contrôle de l'exécution de la prestation.**

Evaluer le niveau de contraintes que le client peut imposer au prestataire.

**Expertise du prestataire**

Evaluer le niveau d'expertise du prestataire afin de savoir dans quelle mesure il maîtrise le traitement des données.

**Degré de transparence du responsable de traitement au niveau de la prestation de services.**

Savoir dans quelle mesure l'identité du prestataire est connue des personnes concernées. En effet, si l'identité du prestataire est connue par les personnes concernées qui utilisent les services du client, le prestataire pourra être présumé comme agissant également comme responsable de traitement.

L'application de ce faisceau d'indices permettra notamment de prendre en compte la nature particulièrement standardisée des offres de Cloud computing dont il résulte généralement une très grande maîtrise de la prestation par le prestataire.

**La CNIL soumet donc à consultation l'analyse suivante :**

- le client est nécessairement responsable de traitement
- le prestataire est présumé sous-traitant à moins que le faisceau d'indices ne fasse tomber cette présomption démontrant alors que le prestataire agit comme responsable de traitement.

Dans le cadre de la réflexion menée sur la révision de la directive, il serait intéressant de réfléchir à la création d'un statut légal pour le sous-traitant afin de faire peser sur ce dernier un certain nombre d'obligations spécifiques.

## C. Question posée

**L'analyse présentée ci-dessus reflète-t-elle selon vous la spécificité du Cloud computing ? Pourquoi ?**

### Réponse

The above analysis reflects to a big extent the specificities of Cloud computing, but the complexity of the Cloud requires some further comments. First of all, it is certainly true that the Cloud provider (*'prestataire'*) is not necessarily a data processor (*'sous-traitant'*) but can also act as data controller (*'responsable du traitement'*). Basically three options shall be taken into account:

- The Cloud provider as data processor and the client as data controller: under this model we assume that the Cloud provider is deemed to be data processor without taking into account the abovementioned bundle of elements proposed by the Commission. In other terms, the Cloud provider is deemed to always be, and as a general rule, the data processor. Theoretically, this model is viable in the sense that it is in line with the spirit of the EC Data Protection Directive, in particular with the concept of 'unitariness of data processing' (i.e. one data flow is a unique data processing controlled and managed by a unique data processor) that underline the rationale of data protection in Europe. However, practically this model is not fully applicable, given the present data protection rules, and it does not encompass the complexity of Cloud scenarios, since in practice the client/data controller has few, if any, possibilities to monitor the activities of the Cloud provider/processor (mainly if the provider is a big ICT multinational company, as it often is). Following the opinion expressed by the Article 29 Working Party (Opinion 1/2010 on the concepts of "controller" and "processor") it is necessary to verify who is in charge of choosing the security measures to protect the data that are processed, and that if the party qualified as processor decides the security measures to adopt, then the processor may be deemed to be data controller. The crucial issue to assess therefore is: who establishes the security measures in a Cloud data processing (most likely the Cloud provider) and who is responsible for the data security in the Cloud;
- Both client and Cloud provider as data controllers: under this model, both client and Cloud provider are deemed to be data controllers in their respective fields, i.e. as regards respectively the collection of users' data and the processing of these data in the Cloud. In particular, the provider is data controller since it is responsible for the implementation of security measures in the Cloud infrastructure and he must assure that no security incidents happen. This model has the advantage to strengthen the position of the Cloud provider also in terms of responsibilities. An evident shortcoming of this model rests in the fact that the client of the Cloud service provider should collect the data subjects' consent to transfer their data to another data controller, such as a Cloud provider. From the practical perspective this requirement makes the implementation of this model practically undesirable. The position of European Privacy Association is that the Cloud provider can be qualified either as a

controller or as a processor, depending on some factual indexes (neutrality). However, given the present data protection rules and contrary perhaps to the common opinion, we make a strong argument that the cloud provider-as-a-controller scheme is in most cases the real appropriate one. Note that when we qualify the cloud provider as a controller we adopt a functional notion of control, which means that we limit the matter of such control only to the purposes and means of the cloud provider, that is to the technical organization of the cloud structure and to the security of data processed within that structure;

- The Cloud provider as data processor unless some elements let presume that he is data controller (model proposed by the Commission): this model is a combination of the previous ones, and it surely reflects the complexity of Cloud business models. However, since the elements to take into account in order to establish whether or not the Cloud provider is data controller are not always clear and available (given lack of visibility concerning the processing on the Cloud provider side) the implementation of this model is likely to generate litigation. Furthermore it is not clear whether or not all elements must be present or whether the absence of one element is sufficient to assume that the Cloud provider is data processor and not data controller – in this case Cloud providers may be data processors simply by contractually obliging the clients not to disclose to final users' that the Cloud infrastructure of the concerned provider is used to deliver the services, even if all other elements may indicate that the Cloud provider is data controller.

**To conclude, and summarize our opinion, it should be pursued a clear determination of duties, obligations and liabilities in the Cloud value chain regardless of formal definitions and roles.**

**Que pensez-vous d'un régime juridique spécifique pour les prestataires ?**

### **Réponse**

It is necessary to clarify the position of Cloud providers, since it is clear that the actual definition of data processor does not fully reflect their role. However, definitions are not of pivotal importance in the sense that the clear indication of roles, obligations and responsibilities is definitely more important than theoretical definitions. Actual static roles shall be overtaken in light of the 'principle of accountability', in other words on the basis of the principle that it is crucial to assess who does what. See under the answer above regarding our doubts about the presumption elements proposed.

In general terms an *ad hoc* legislation for Cloud providers is not advisable provided that legislation shall be as general as possible and shall be adaptable to different technical scenarios. The legislation may well state for instance that data processors are deemed to be joint controllers (eventually under a regime of joint liability with the main controller) if some conditions are met or if some clear and objective presumption elements are present. We reinforce the necessity of clear definition of duties, obligations and liabilities regardless of definition of roles.

### **III. Le droit applicable**

Le Cloud computing étant basé sur l'utilisation de multiples serveurs situés en divers points de la planète, les difficultés quant à la détermination du droit applicable sont évidentes. En effet, la flexibilité et la fluidité des transferts de données rendent potentiellement applicables autant de lois que de pays dans lesquels se trouvent des serveurs traitant les données.

Il est pourtant particulièrement important d'identifier la loi applicable, afin notamment de déterminer quelles obligations pèsent sur le responsable de traitement.

## D. Le principe

Aux termes de l'article 5 de la loi du 6 janvier 1978 modifiée, la loi s'applique si le responsable de traitement :

- ✓ a son établissement sur le territoire français
- ✓ a recours à des moyens de traitement situés sur le territoire français (sans être établi sur le territoire d'un autre Etat membre)

## E. Pistes de réflexion

Alors que la CNIL est favorable à une extension de la notion de moyens de traitement, elle souhaite tout de même tempérer les conséquences excessives d'une interprétation particulièrement large des moyens de traitement et une éventuelle application systématique de la loi française.

### Question posée :

**Selon vous quels critères pourraient permettre de déterminer la loi applicable aux acteurs du Cloud ?**

### Réponse

The presence of technical infrastructures shall not be taken as criterion to determine the applicable law since it creates confusion and it multiplies the number of applicable legislations. For EU-based companies the applicable law shall be that of the place of main establishment (e.g. a French company is subject to French law), and for extra-EU companies that do not have a subsidiary or branch in Europe an accreditation scheme can be envisaged (e.g. an American company that wants to process personal data in Europe can select a country of accreditation and will be subject to that national legislation). This scheme already exists in the field of Binding Corporate Rules (with the concepts of mutual recognition and leading authority) and, outside privacy law, in the field of Value Added Tax. The logical condition for a smooth functioning of this scheme is harmonization among legislations in the EU in order to avoid the phenomenon of forum shopping.

## II. Encadrement des transferts

### A. Le principe

Aux termes de l'article 68 de la loi de 1978, les données à caractère personnel ne peuvent faire l'objet d'un transfert que si l'Etat dans lequel se situe le destinataire de données assure un niveau de protection adéquat. L'article 69 de ladite loi prévoit expressément les outils permettant d'encadrer ce type de transferts : clauses contractuelles types, règles internes

d'entreprises (ou BCR), Safe Harbor ou exceptions.

Le recours à ces outils **implique de connaître le ou les pays dans lesquels les données vont être communiquées, élément essentiel pour procéder aux déclarations/autorisations auprès de la CNIL et pour informer les personnes concernées des transferts vers ces pays.**

Or, le Cloud computing est le plus souvent fondé sur une absence de localisation stable des données. Le Client est donc rarement en mesure de savoir en temps réel où se trouve les données et où elles sont transférées et stockées.

Dans ce contexte, les instruments juridiques permettent d'encadrer les transferts de données vers des pays tiers n'assurant pas un niveau de protection adéquat démontrent leurs limites.

Il existe par ailleurs des exceptions au principe d'interdiction de transferts

## B. Solutions proposées

### (i) Sur un plan juridique

La multiplication des lieux potentiels de stockage des données rend difficile la mise en œuvre des instruments juridiques garantissant un niveau de protection adéquat.

La CNIL propose d'une part, d'appeler les prestataires de services à intégrer les clauses contractuelles types dans leurs contrats de prestations de services, d'autre part, de réfléchir à la faisabilité de BCR sous-traitants.

Ces « BCR sous-traitants » permettraient à un client du prestataire de confier ses données personnelles à ce sous-traitant en étant assuré que les données transférées au sein du groupe du prestataire bénéficie d'un niveau de protection adéquat.

### (ii) Sur un plan technique

L'encadrement des transferts pourrait également dépendre des solutions techniques utilisées. Certains prestataires évoquent par exemple le recours à des « métadonnées »<sup>4</sup> pour définir ou décrire une autre donnée quel que soit son support (papier ou électronique), ou encore les solutions de chiffrement homomorphe<sup>5</sup>.

Le recours au chiffrement pourrait également apparaître comme une solution satisfaisante pour garantir l'envoi de données vers certains pays uniquement.

Dans un tel cas, le client pourrait alors endosser véritablement son rôle de responsable de

---

<sup>4</sup> Méthode permettant de lier des informations précises aux données et notamment permettrait de déterminer le périmètre géographique sur lequel les données pourront être transférées.

<sup>5</sup> Moyen de chiffrement permettant au prestataire d'agrèger des messages bien qu'ils soient chiffrés et sans qu'il en est connaissance.

traitement en déterminant précisément avant même la réalisation de la prestation, les pays destinataires de données.

**En pratique :**

- **Le prestataire de Cloud**, qu'il soit responsable de traitement ou sous traitant, devra obtenir une approbation de ses BCR par les autorités européennes de protection des données, selon la procédure actuelle.
- **Le client** effectuera sa demande d'autorisation de transferts auprès des autorités de protection sur la base des BCR du prestataire approuvés.

C. Questions posées

**1. Lequel des instruments existants vous semble le mieux adapté au Cloud computing ?**

**Réponse**

In general terms Binding Corporate Rules for data processors shall be positively assessed. However, at present, the process to obtain approval of BCR (for controllers) is too complex and it thus needs to be simplified.

Anyway, BCR for processor (alone) are not THE solution to the issues related to data transfer in the cloud. Often cloud services are composed of different cloud layers that are respectively provided by different Cloud service providers (es. the service offered by Cloud provider A is a SaaS that is provided to the client leveraging in fact the PaaS of a Cloud provider B). So if we look at the present means of transferring data outside the EEA, not only BCR should be extended to processors but also the Model Contractual Clauses provided by the European Commission. So to support lawful circulation of data in the cloud environment, BCR for processors may be coordinated with the use of Model Contractual Clauses by processors (i.e., from processor within the EEA to a processor extra-EEA).

**2. Comment avez-vous encadré les transferts réalisés dans le cadre de la prestation des Cloud que vous proposez ou auquel vous avez souscrit ?**

**Réponse**

Not applicable.

**Les BCR sous-traitants vous semblent-ils être une solution intéressante ? Quel mécanisme envisageriez-vous pour ces BCR ?**

**Réponse**

Yes, they are useful instruments and their adoption must be promoted. In particular, it would be useful to have a certification system granted by trusted third parties that would make the approval process of Binding Corporate Rules by national authorities faster and less cumbersome. These trusted certificatory bodies would verify if the conditions to obtain Binding Corporate Rules approved exist (please refer to the [Opinion 3/2010 on the principle of accountability](#) of the Article 29 Working Party).

On a long-term perspective, and taking into account the many resources required for national data protection authorities to deal with Binding Corporate Rules, the creation of a relevant “European privacy quality certificate” can be envisaged.

**3. Avez-vous déjà réfléchi à des solutions techniques qui permettraient de mieux identifier et contrôler les flux de données dans le cadre des prestations de Cloud ?**

**Réponse**

The solutions envisaged by CNIL are viable and can be effectively implemented.

## **VI. Sécurité des données**

Les problèmes de sécurité et de confidentialité des données externalisées vers le Cloud, couverts par l'article 34 de la loi « informatique et libertés », sont en général un des premiers sujets de préoccupation des utilisateurs<sup>6</sup>.

Dans le cas d'un organisme ayant recours à une offre de Cloud computing, **la gestion de la sécurité de ces données se trouve largement déléguée au prestataire**, pour lequel il est souvent difficile d'obtenir des garanties sur le niveau de sécurité réel. En application de l'article 35 de la loi, le sous-traitant doit « *présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées dans l'article 34* »<sup>7</sup>, le responsable de traitement ayant quant à lui « *une obligation de veiller au respect de ces mesures [de sécurité et de confidentialité]* » **Error! Bookmark not defined.**

<sup>6</sup> Dans une étude effectuée par *IDC Enterprise Panel* (Etats-Unis), à la question « *Rate challenges/issues ascribed to the 'Cloud'/on-demand model* » la sécurité apparaît en tête avec 74,6% (source : présentation du NIST sur le Cloud Computing et la sécurité, disponible à l'URL : <http://csrc.nist.gov/groups/SNS/Cloud-computing/Cloud-computing-v26.ppt>).

<sup>7</sup> Article 35 de la loi « informatique et libertés ».

De plus, le même article prévoit que « *Le contrat liant le sous-traitant au responsable de traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable de traitement.* »

**Il est donc nécessaire que ces exigences en termes de sécurité se trouvent matérialisées dans un contrat. Il est notamment essentiel que les responsabilités et rôles des parties soient clairement définis au préalable, afin de traiter efficacement les cas d'incident pouvant aboutir à une perte ou une divulgation de données.**

### Question posée

**Quel commentaire pouvez-vous formuler sur les relations contractuelles entre client et prestataire concernant les mesures de sécurité et le respect des articles 34 et 35 de loi informatique et libertés ?**

### Réponse

It is pivotal that the Cloud provider is contractually liable for the security incidents that may happen. Actually usually this is not the case in point if we take into account the Cloud providers' standard terms and conditions/agreements. Furthermore, as already pointed out above, for the clients it is usually impossible, or at least very difficult, to verify the adoption of security measures by the Cloud provider (in fact, security issues in the framework of the paradigm controller-processor are not likely to be manageable). From a practical perspective, liabilities of the parties involved shall be clarified in the standard terms and conditions/agreements.

Security incidents should be reported by reposted by Cloud service providers to the competent authorities and, eventually, to clients – extension of Data breach notification duty. Joint liability for data controller and data processor in case of security incidents could be proposed. However, we believe that purely legal means are scarcely effective. They need to be combined with the implementation of technology standards and of privacy-by-design models, since effective data security is the central issue in the Cloud and prevails over legal definitions and formal rules.

## **4. Des risques spécifiques au Cloud**

**Il est recommandé d'effectuer une analyse de risques<sup>8</sup> préalablement à la rédaction de toute politique de sécurité, en particulier pour les systèmes d'information de taille importante.** Cette recommandation a déjà été formulée par l'ENISA<sup>9</sup> dans son rapport paru

<sup>8</sup> La méthode d'analyse de risque la plus utilisée en France est celle développée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI, anciennement DCSSI), dénommée EBIOS (voir à l'url : [http://www.ssi.gouv.fr/site\\_article45.html](http://www.ssi.gouv.fr/site_article45.html)).

<sup>9</sup> *European Network and Information Security Agency*

en novembre 2009 et intitulé « Cloud computing: benefits, risks and recommendations for information security »<sup>10</sup> et par l'ANSSI dans son rapport plus général sur « L'externalisation des systèmes d'information – Maîtriser les risques » publié le 19 mars 2010<sup>11</sup>.

Cette analyse de risques doit notamment prendre en compte la nature de l'organisme qui utilise le Cloud et le type de données traitées dans le Cloud.

**La CNIL considère donc qu'adopter une démarche d'analyse de risques pour évaluer l'impact du passage au Cloud devrait être adopté par les responsables de traitement qui souhaitent utiliser le Cloud computing pour certains de leurs traitements de données personnelles.**

**Question posée :**

**Quels commentaires pouvez-vous formuler sur la recommandation de mener une analyse de risques avant le passage au Cloud ?**

**Réponse**

It is impossible to be performed an informed risk analysis if privacy roles and relevant duties, obligations and liabilities cannot be clearly allocated. Therefore, before considering risk analysis a clear determination of duties, obligations and liabilities in the Cloud value chain regardless of formal definitions and roles is needed. Moreover, to perform an accurate risk analysis, clients need to know security and privacy policies of the different Cloud service providers, so to compare them and eventually choose the most appropriate one. In this respect, the European Privacy Association is working together with Cloud Security Alliance on the definition of a template for Privacy Level Agreement (PLA) in order to: a) provide cloud customers with a tool to assess a Cloud service providers commitment to address personal data protection; and b) offer contractual protection against possible economical damages due to lack of compliance or commitment of the Cloud service providers vis a vis privacy and data protection regulation.

**5. Constats et propositions en matière de sécurité**

- a) Les points de sécurité à renforcer

Lors de l'utilisation du Cloud computing, la CNIL recommande d'examiner particulièrement certains aspects de la sécurité :

<sup>10</sup> Ce rapport identifie notamment 35 risques spécifiques au Cloud computing. L'ENISA a précisé l'analyse à réaliser dans le cas de l'utilisation du Cloud par les services publics dans un second rapport, publié en janvier 2011 et intitulé « Security & Resilience in the Governmental Clouds ». Dans ce rapport, l'ENISA fournit un guide d'analyse à destination des services publics et recommande, globalement, l'utilisation de Clouds privés, dont le rapport bénéfice/risques en matière de sécurité semble positif

<sup>11</sup> Notamment les risques liés à la localisation et à l'hébergement mutualisé.

- **la protection externe du réseau** (pare-feu, serveur proxy avec analyse de contenu, détection d'intrusion, etc.)
- **la protection du terminal** (PC portable, assistant personnel, téléphone portable) : antivirus, système d'exploitation et des logiciels mis à jour régulièrement, firewall<sup>12</sup>.
- **le chiffrement des liaisons**<sup>13</sup> de manière à garantir la confidentialité des échanges
- **la traçabilité** : conserver un historique des connexions et des opérations effectuées<sup>14</sup> sur les données (en effet, dans de nombreuses offres, y compris de grandes sociétés, les événements de type « administration » qui permettent par exemple la création/suppression de compte ou les accès aux données ne sont pas enregistrés).

Pour les prestataires proposant des offres à destination d'organismes publics ou de sociétés, on peut rajouter :

- **la gestion des habilitations** par exemple le compte d'une personne ayant quitté l'organisme doit être immédiatement désactivé car le fait qu'elle n'a plus accès aux locaux ne l'empêche pas d'accéder aux systèmes d'information.
- **l'authentification** : de même, l'authentification doit être renforcée. Le recours à une authentification forte s'avèrera nécessaire dès lors que les données accédées sont sensibles et/ou volumineuses.

### Questions posées:

**Quels commentaires pouvez-vous formuler sur cette analyse ? Selon vous, sur quelles mesures de sécurité la CNIL devrait-elle attirer l'attention des responsables de traitement ?**

### Réponse

ID management: Cloud service providers must assure rigorous ID management system enabling only selected subjects and to the extent their profile allow them

Access control: Traceability of who does what in the cloud environment (comprehensive logging), preventing unauthorized access or alteration of the data

Data integrity: deploying present state of art technology to preserve the data.

<sup>12</sup> Ou « pare-feu » servant à filtrer les connexions entrantes et sortantes. Ici, il se présentera sous forme d'un logiciel, ou à défaut de la fonctionnalité fournie par le système d'exploitation du terminal.

<sup>13</sup> Par exemple en ayant recours à https (HyperText Transfer Protocol Secure) pour sécuriser la navigation.

<sup>14</sup> Sil s'agit d'une offre de type *IaaS*, il sera important d'activer les journaux au niveau du système d'exploitation (sécurité, système, application), et au niveau des équipements contribuant à la sécurité du réseau (firewall, IDS). S'il y a en plus des prestations de type *SaaS*, il faudra journaliser les événements (création de compte, exports, accès en écriture/lecture) au niveau de la base de données et/ou de l'applicatif associé. De plus, l'accès aux journaux devrait être protégé en écriture et limité au minimum de personnes. Bien que généralement gérés par la société offrant le service de Cloud computing, ils devraient être accessibles (éventuellement sur demande) au client.

b) L'accès des administrateurs et le chiffrement

Lorsqu'aucun chiffrement n'est mis en œuvre au niveau du stockage des données, ce qui est très souvent le cas, les administrateurs informatiques<sup>15</sup> du prestataire ont un accès total aux données de leurs clients<sup>16</sup>.

Une manière de se protéger partiellement de ces risques est de s'assurer que les administrateurs du prestataire ont une clause de confidentialité dans leur contrat de travail ou ont signé un engagement en ce sens. Une traçabilité des actions d'administration dans des journaux qui ne leur sont pas accessibles est par ailleurs recommandée.

**Cependant, pour le client responsable de traitement, le chiffrement des données stockées dans le Cloud constitue le seul moyen d'empêcher que les administrateurs informatiques du prestataire<sup>17</sup> aient accès aux données qui lui sont confiées.**

Question posée

**Quels commentaires pouvez-vous formuler sur le chiffrement dans le Cloud ?**

Réponse

It is undoubtedly a good solution in order to avoid that unauthorized people access sensible information. Please refer to the answer immediately above for further information.

c) La destruction des données et la réversibilité

Lorsque la prestation offerte par le prestataire s'achève (fermeture d'un compte, rupture de contrat, etc.) il est important pour le client de s'assurer que les données qu'il a confiées au prestataire ne sont plus accessibles à ce dernier. En fonction de la sensibilité de ces données, les mesures suivantes peuvent être exigées :

- effacement classique des données
- effacement « sécurisé »<sup>18</sup> des données
- restitution des supports de stockage (disques durs, bandes de sauvegarde) ou destruction physique dans le cas de matériels dédiés au client (cas des Clouds privés par exemple) ; dans ce cas, il est important que ceci soit prévu dans des clauses contractuelles dès le

---

<sup>15</sup> Réseau/ système d'exploitation, base de données et application ;

<sup>16</sup> Ce qui peut représenter une quantité très importante de données quand on pense aux dizaines de milliers de clients d'ADP ou aux millions de clients de Google pour reprendre les exemples précédents.

<sup>17</sup> Et donc la société de « Cloud computing » elle-même.

<sup>18</sup> Les données effacées à l'aide de la fonction de suppression du système d'exploitation peuvent être facilement récupérables, même une fois la corbeille vidée ou après formatage du support. Il existe en effet de nombreux logiciels, dont certains sont gratuits (Recuva par exemple), permettant de récupérer des données après effacement ou formatage. C'est la raison pour laquelle il existe des logiciels d'effacement sécurisé qui fonctionnent par réécriture de bits aléatoires sur les données.

départ<sup>19</sup>.

Par ailleurs, la question de la réversibilité des données doit être prise en compte par le client avant la souscription à un service de Cloud computing. Le client peut souhaiter conserver les données qu'il a confiées au prestataire et dans ce cas, le prestataire devrait prévoir une restitution dans un format standardisé qui permette au client de réutiliser ces données avec un autre prestataire ou un logiciel classique.

**Question posée :**

**Quels commentaires pouvez-vous formuler sur la restitution des données et la réversibilité ?**

**Réponse**

In private Clouds it is usually possible to negotiate clauses about restitution and reversibility of data. In public Clouds things are different, especially in case of standardized Cloud services offered by big ICT companies. Of course, the contractual clauses about restitution and reversibility of data are likely to be effective if there is an effective interoperability among the different Clouds. Interoperability, transfer back and data portability should be always assured by Cloud providers.

L'ensemble des problématiques citées ci-dessus pourrait être partiellement traité par un renforcement de la transparence des prestataires de Cloud sur leurs politiques de sécurité. Des mesures de certification des centres de données, tenant compte de la question de la protection des données personnelles pourraient renforcer la confiance des clients et des Autorités de protection des données, sans induire de risques supplémentaires<sup>20</sup>. Toutefois, il n'existe pas de normes de sécurité adaptées au Cloud, qui prennent pleinement en compte la problématique de la protection des données personnelles.

La CNIL recommande que des normes de sécurité incluant la question de la protection des données personnelles dans le Cloud soient définies par le secteur et promues pour renforcer la transparence vis-à-vis des clients.

**Questions posées :**

- **Approuvez-vous l'analyse de la CNIL sur l'absence de normes ou de certifications sur la protection des données personnelles dans le Cloud ?**
- **Quelles propositions de normalisation ou de certification pouvez-vous formuler à ce sujet ?**

**Réponses**

The European Privacy Association supports certification effort that aim at combining data

<sup>19</sup> Le rachat des supports a posteriori est parfois possible mais est en général facturé très cher.

<sup>20</sup> A l'inverse, si chaque client aurait la capacité de faire un audit sur le centre de données, ces audits permanents induisent de nouveaux risques sur la sécurité du centre.

protection regulatory compliance and data security. Actually Cloud Security Alliance has already announced effort in the development of cloud security and privacy standards under ISO/IEC. The European Privacy Association is also developing a European Privacy Trustmark that takes into consideration also security aspects.