Summary of responses to the public consultation on Cloud computing run by CNIL from October to December 2011 and analysis by CNIL

1. *Definition of Cloud Computing*

In the public consultation, CNIL defined Cloud computing on the basis of various definitions as well as the criteria defined by NIST[1] following a long consultation process. The following criteria were chosen:

- simplicity of an on-demand service;
- extreme flexibility;
- "light" access;
- resource virtualization;
- pay-per-use.

The consultation also distinguished between Cloud computing services using three different service models:

- SaaS: Software as a Service, i.e. the provision of software online;
- PaaS: Platform as a Service, i.e. the provision of a platform for application development online;
- IaaS: Infrastructure as a Service, i.e. the provision of computing and storage infrastructure online.

To keep things simple, the consultation did not look at the different models for deploying these services, namely the 'public Cloud', where a service is shared and pooled among numerous customers, the 'private Cloud', where a service is dedicated to one customer, and the 'hybrid Cloud', where these two models are combined. There were many contributions that mentioned the importance of these distinctions.

The consultation does not take issue with the definition of Cloud computing put forward by CNIL. However, a few vocabulary adjustments could be made that would take account of these contributions, such as replacing 'virtualization' with 'pooling', which many people suggested and which is indeed a better term.

[1] List of characteristics drawn up by the *National Institute of Standards and Technology*, USA, in the document "*The NIST Definition of Cloud Computing*", http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

While the consultation was meant to cover all Cloud computing models, many responses referred mainly to public Cloud offerings for companies, and particularly SaaS (online software) offerings. The analyses presented in this document therefore tend to focus on this particular Cloud computing model (characterized by standard offerings, a certain amount of pooling, no information about location, and standard contracts).

2. Cloud computing service provider qualification

According to Article 3 of the French Data Protection Act of 1978, as amended, the data controller is defined as the natural or legal person which determines the purposes and means of the processing of personal data. The data processor processes personal data on behalf of the data controller and in accordance with its instructions.

To help those involved in the Cloud to work out who is playing each role, CNIL has suggested the following solution:

- Customer: this will always be the data controller. By collecting the data and deciding to outsource the data processing to a service provider, it is the data controller because it determines the purposes and means of processing of the data.

- Service Provider: in principle, it acts on behalf of and on the instructions of the customer, who is the data controller. Consequently it seems possible to establish the presumption that the service provider is the data processor for the customer.

This presumption works particularly well when the customer is using a private Cloud, i.e. a Cloud used by one customer only, which implies that there is a large amount of control over provision of the Cloud service by the service provider. When a customer is using a public Cloud, where by nature the service provider defines the operation and purposes of the online application accessible by various customers, the respective roles of the customer and service provider can be difficult to determine and also depend on the type of services subscribed to by the customer. CNIL therefore proposed that the presumption regarding who is the processor should be based on a set of indicators determining the amount of room for maneuver the service provider has when performing the services.

These indicators consist of the following criteria:

1. The **level of instruction** given to the service provider by the customer: this criterion can be used to evaluate the extent to which the service provider is constrained by instructions from the customer (who is the data controller). If the customer allows the service provider a large amount of freedom in the performance of the service, the service provider will also be acting as data controller provided that the other criteria listed below are met.

For example: A home learning company uses a service provider to share the course material it provides for its students. To access the course material, the students have to register on the home learning company's platform.

This company, which is acting as data controller, has accepted the service provider company's terms of use. The service provision contract signed between the home learning company and the service provider does not expressly state the storage conditions, volume of data stored or the geographical area in which the data are stored. The service provider therefore has a large

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

amount of autonomy and consequently could also qualify as data controller rather than processor, provided that the criteria below are also met. On the other hand, if the service provision contract is very specific and the home learning company controls the performance of the service, having defined it in advance in the service contract, the service provider company will be considered to be a data processor.

2. The **degree of control** exercised by the customer (who is the data controller) over the performance of the service by the service provider: this criterion is an effective indicator of how the service provider implements the customer's instructions. The level of 'supervision' by the customer, as data controller, over the services of its service provider, should be examined.

For example: A customer company acting as data controller does not monitor the service provider it is using and the service provider is not under any obligation to report regularly on the progress of the tasks it has been asked to perform. In this case, the service provider should also be considered to be a data controller rather than a data processor, provided that the criteria below are met.

3. The **added value** supplied by the service provider over the processing of the customer's data: this criterion shows how much expertise the service provider has in data processing. The greater the service provider's expertise in a field, the more capable it will be of deciding the means of processing to be used for performance of the services and the more likely it is also to qualify as data controller.

For example: A hairdresser's salon uses an online application for consulting and printing documents to manage its customer base. It is thus the data controller because it decides the purposes of the processing (management of its customer base) and the means of processing (use of a service provider). However, when the data are transferred to the service provider providing the application, the service provider controls the conditions in which it performs the services for the customer. Under these circumstances, the service provider can therefore also be considered to be a data controller rather than a data processor, provided that the criteria below are met.

4. The **degree of transparency** in the use of a service provider: this criterion can give an indication as to qualification of the service provider. If the service provider's identity is known to the persons using the customer's services, the service provider can also be presumed to be acting as data controller.

For example: The company X uses the online storage services of a service provider for the payroll management of its employees, for which purpose the company is considered to be the data controller. When the employees have access to the interface on which their pay slips are placed, it is clearly stated that the service is managed by the service provider. This indicator would allow the presumption to be made that in this case the service provider is also acting as data controller and not as data processor.

The application of these indicators enables account to be taken of the highly standardized nature of Cloud computing offerings, where it is generally the case that the service provider has a large amount of control over the service.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

The opinion of the contributors was divided on the proposal for a presumption regarding qualification as processor: half of them agreed with it, the other half did not. The comments they made suggest that qualification as processor should not be based on presumption but should depend on what the service provider offers:

- examination of this should look at the type of Cloud (public or private) and the service model (IaaS, SaaS, PaaS);
- the criteria that make up this set of indicators should be clarified (concept of expertise, degree of transparency) or else they are not appropriate for Cloud computing (standard contracts);
- because the majority of Cloud offerings are based on standard contracts, data controllers are not actually able to negotiate with service providers, and so most service providers are highly likely to be data controllers;
- joint responsibility is a source of legal uncertainty.

The opinion of the contributors was divided in terms of legal certainty, as regards the relevance of introducing a presumption of qualification as processor, which made by applying the criteria, and was more favorable to the proposal to create a legal status specific to processors.

CNIL's position

When a customer uses a service provider, it is generally accepted that the former is the data controller and the latter the processor.

However, CNIL notes that in some cases of PaaS and public SaaS, although customers are responsible for their choice of service provider, they cannot actually give the service provider instructions and they are unable to check the effectiveness of the security and confidentiality safeguards put in place by the service provider. This lack of instructions and of means of control is due mainly to the existence of standard offerings that customers cannot modify, and to standard service contracts that do not allow them room to negotiate.

In these situations the service provider could therefore, on the face of it, be considered to be joint controller according to the definition of 'controller' given in Article 2 of Directive 95/46/EC, because it participates in determining the purposes and means of the processing of personal data.

To avoid the risk of responsibilities being diluted by the presence of joint data controllers, these joint data controllers must clearly state in the service contract between them how their responsibilities are shared, in particular to prevent the presence of joint data controllers from having any impact on the persons whose data is being processed.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

CNIL proposes the following table for the sharing of responsibilities between the customer and the service provider:

Hypothesis	Notifications to CNIL	Information to data subjects	Obligation of confidentiality and security	Exercise of data subjects' rights to the ...
The service provider is joint data controller for the processing	**Customer**[2]	**Customer**[3]	**Customer and service provider**	**Customer (with the service provider's support)**[4]

CNIL also points out that a service provider may only use personal data given to it by its customers on its customers' instructions. Consequently, a service provider that wanted to process data for purposes other than those determined by its customers (a common example is targeted advertising) would be acting outside its customers' instructions if it did not inform them of its intention to do so and obtain their prior permission. If the service provider obtained this permission, it would then be the data controller for the processing it performed for a purpose other than that of the customer's processing. In this situation, the customer and service provider would each be responsible for the processing they performed. They would also be responsible for informing the persons concerned of the means of processing, in accordance with Article 32 of the French Data Protection Act of 1978, as amended.

Since the launch of the public consultation by CNIL, on 25 January 2012 the European Commission published its draft regulation on personal data protection, which introduces a legal status of processor in Article 26, and gives a non-exhaustive list of the information that should appear in the service contract.

[2] The customer and the service provider will have notification obligations towards CNIL concerning the processing for which they are joint controllers. They must then determine which of them will undertake these formalities. CNIL recommends that the customer takes responsibility for this, since the use of a Cloud service provider may form part of more general processing, but it is quite possible for the service provider to undertake the formalities on his own behalf and on the behalf of the customer. In all cases, the party responsible for these notifications must be able to supply evidence at the other party's request that they have been duly accomplished to CNIL.

[3] Although the customer and the service provider, both data controllers, are responsible for the provision of information, in practice it is preferable that the entity to which the data subjects have communicated their data informs them of the processing means used by the service provider. Consequently, the service provider must give the customer all the information necessary to meet this obligation of provision of information. However, the service provider must remain the contact to whom the data subject must refer to obtain more information on the processing for which the service provider acts as joint data controller.

[4] The fact that the data may be spread across servers located in different countries can make it more complicated for data subjects to exercise their rights. It is therefore necessary to ensure that the service provider and the customer are providing the necessary safeguards to enable the data subjects to exercise their right of access, correction, alteration, updating or deletion.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

The draft text places a number of obligations on the processor jointly with the data controller. The processor is thus subject to the obligations of providing documentation (Article 28), cooperation with the supervisory authority (Article 29), security of processing (Article 30), notification of a personal data breach to the supervisory authority (Article 31), impact assessment (Article 33), prior authorization and prior consultation of the supervisory authority (Article 34), designation of a data protection officer (Article 35) and handling of transfers (Articles 40, 42 and 43).

Consequently, the creation of this legal status placing a number of obligations on the processor is an interesting solution that restores the balance of power and therefore of responsibilities.

5. Determination of applicable law

The consultation put an open question to the contributors to find out what criteria could be used to determine the law applicable to those involved in Cloud computing services.

A large proportion of the contributors suggested using only the data controller's law to determine the applicable law. However, this proposal fails to take account of the criterion concerning means of processing, as currently envisaged by Article 5-I-2 of the French Data Protection Act (which states that the French Data Protection Act is applicable when the processing is performed by a data controller not established in the European Union but which is using means of processing located on French territory), thereby restricting the geographical scope of application of the French act and risking accentuation of the phenomenon of "forum shopping"[5] that already plagues European legislation. Consequently, a solution of this kind is difficult to envisage.

On the other hand, taking account of the difficulty of determining the applicable law based on the data controller, targeting has been suggested as a criterion of interest, since it guarantees better protection of the personal data of individuals. However, companies have said that using this criterion could lead to the cumulative application of the law of several countries, which they would not want.

Targeting was the criterion chosen in the draft EC regulation, which provides for its application to data controllers not established in the European Union but which offer goods or services to people living on EU territory (Article 3 of the draft EC regulation).

6. Regulating framework for data transfers

In the consultation, CNIL suggested the following legal and technical solutions for regulating data transfers outside the European Union:

[5] In this case, "forum shopping" refers to the fact that a company chooses to locate in one country rather than another because of advantages in the legislation of that country. For example, if the prior permission of the UK data protection authority did not have to be sought for transfers to countries outside the European Union, this might encourage an American company wishing to open a subsidiary in Europe to choose to locate in the United Kingdom.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

❖ On a legal level

The fact that there are so many potential data storage sites makes it difficult to implement the legal instruments guaranteeing an adequate level of protection.

CNIL suggests, on the one hand, that service providers be asked to include the EC Standard contractual clauses in their service provision contracts and, on the other, that consideration be given to the feasibility of BCR for processor[6].

These BCR for processor' would enable a customer of the service provider to hand its personal data over to that processor with the certainty that the data transferred within the service provider's group has an adequate level of protection.

❖ On a technical level

Regulation of transfers could also rely on technical solutions. For example, some service providers mention the use of metadata to define or describe another item of data, regardless of its medium (paper or computer), or homomorphic encryption solutions.

The use of encryption might also appear to be a satisfactory solution to guarantee that data will be sent only to certain countries.

In this case, the customer could then truly perform its role of data controller by determining precisely, before the service is performed, to which countries the data will be sent.

CNIL asked the participants in the public consultation which instrument out of those currently in existence was best suited to Cloud computing.

Although on the whole the contributors said that current transfer mechanisms were generally not suited to Cloud computing, it emerged from the consultation that BCR are considered the best tool. Moreover, the proposal to recognize BCR for processor was enthusiastically welcomed by the market players.

In the draft regulation published by the European Commission, Articles 42 ("Transfers by way of appropriate safeguards") and 43 ("Transfers by way of binding corporate rules") stipulate that data transfers to third countries are possible if the data controller or processor has implemented instruments that offer appropriate safeguards, subject to prior authorization from the national supervisory authority when the instruments introduced are not legally binding. The draft regulation therefore expressly recognizes BCR for processor.

At the request of service providers, and following a feasibility study done by CNIL in 2011, the BCR subgroup of the Working Group on Article 29 is currently writing an opinion on BCR for processor, which should be published soon.

[6] Binding Corporate Rules

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

Until the publication of this opinion, regulating data transfers through the signature of the EC Standard contractual clauses is recommended. Solutions vary depending on the service provider's qualification and location:

- If the customer is transferring data to a Cloud service provider located outside the EU who is acting as processor: signature of the standard contractual clauses from 2010, which provide in particular subcontracting chains.

- If the customer is transferring data to a Cloud service provider located within the EU, who is acting as processor and who then transfers the data to a processor located outside the EU: there are several possible mechanisms (signature of the standard contractual clauses from 2010 between the data controller and the non-EU processor, mandate or tripartite contract).

- If the customer is transferring data to a Cloud service provider located outside the EU, who is acting as data controller: signature of the standard contractual clauses from 2001 or 2004. If the service provider then transfers its customer's data to a processor outside the EU, there are two solutions that can be considered:

    - either the **customer** signs the standard contractual clauses from 2010 directly with this processor,

    - or the **Cloud service provider** signs a contract with the subcontractor that contains the same obligations that are in the standard clauses from 2010, provided that the service contract between the customer and the Cloud service provider includes an obligation on the Cloud service provider to sign an equivalent contract to the standard contractual clauses with any processor.

7. *Cloud Computing security*

The issue of data security is of key importance for customers using Cloud computing and the consultation confirmed customer's central concern with this issue. By switching to Cloud computing, the company is outsourcing the personal data it processes but also other asset-related and strategic data and the processes themselves. Any failure in the Cloud service can make it impossible for the company to undertake any activity and a data breach or leak can have major consequences for its operation, as regards its customers and competitors.

a. Strengthening the Cloud contract and the service level agreements for data protection

While the inclusion of contract conditions on secure processing is seen as a necessity by most players, some underline its limitations due to the standard nature of Cloud computing service offerings and the finding that, in practice, the service provider unilaterally decides the measures it believes are appropriate. It therefore seems necessary to consider that additional means should be defined to govern the security of processing in the Cloud, such as service provider certification or customer audits.

For this reason CNIL has drawn up a list of the minimum provisions that a contract should include (e.g. liability in the event of data loss) and is encouraging the creation of SLAs/PLAs[7]

[7] SLA: Service Level Agreement. SLAs are common practice in service provision.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

associated with the contract that covers data protection issues. Ultimately it would be desirable for standard service provider contracts to include such SLAs/PLAs.

b. Risk assessment

As far as risk assessment is concerned, the sector recognizes how important this is for a customer wishing to switch to Cloud computing: the documents of ENISA and the Cloud Security Alliance are recognized as suitable tools for risks assessment but they should be complemented by proper consideration of personal data protection. For this reason CNIL has made recommendations, aimed particularly at small companies that do not necessary have the financial or technical means to conduct a full risk assessment. In particular, CNIL has identified the data protection risks that apply generally to Cloud computing.

c. Security measures

Concerning security measures, many contributions underlined the overlap between the measures put forward by CNIL and the measures imposed by certain existing security standards such as ISO 27001, SAS70 and ISAE3402. These standards provide a framework that can facilitate the assessment of the service provider's security, though without giving absolute guarantees: the exact conditions of application of the standard need to be examined each time, and in particular the relevant perimeter of the service provider's activity. The responses show that many professionals identify as many risk factors on the customer's side as on the service provider's.

d. Use of encryption

In the specific case of encryption put forward by CNIL in its consultation as the safest way for the customer to control the use of personal data, the contributions of the players most involved in providing Cloud services (particularly service providers but also some major customers) show that this solution is not yet technically operational for most Cloud computing services. Only the IaaS-type data storage services currently seem to be eligible for the implementation of encryption on the customer's side. For the most widely available application offerings (SaaS), progress is still to be made. On the other hand, other solutions such as "obfuscation"[8] and data fragmentation are suggested by some, but should be explored in more detail to determine their characteristics and any contribution they could make to data protection.

The risk of foreign authorities accessing data, e.g. under the Patriot Act in the United States, must be taken into account in any risk assessment. Even when data are transferred across encrypted links (e.g. https or VPN), they are usually processed unencrypted by the Cloud computing service provider. One solution for reducing this risk, when the customer has the resources to implement adequate key management and is using a recognized algorithm, is to encrypt the data on the customer's terminals before transferring it via a secure channel[9].

PLA: Privacy Level Agreement, a version of SLAs for data protection issues. This concept is currently under development, particularly within the Cloud Security Alliance (CSA). CNIL is participating in the CSA's work on PLAs.

[8] A word that refers to a procedure aimed at making data difficult to understand

[9] For information, a secure channel (e.g. https or VPN) safeguards the confidentiality of the data while it is being sent, to ensure only the destination server (here, the Cloud service provider's server) can read the data sent. If the data are sent unencrypted, they can be read by the service provider.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00

However, this solution is not suitable for many SaaS services, for example online document management services, because the service provider needs unencrypted access to the data in order to provide the service. Moreover, the impossibility of sufficiently reducing the risk of foreign authorities accessing to the data has already led some data protection authorities to limit or even ban the use of some SaaS services[10].

e. Reversibility (or portability)

All those providing Cloud services seem to have taken account of the issue of reversibility/portability, though there is still progress to be made (on formats and the software needed to use the restored data, etc.), particularly for the customer's business applications.

f. *Standards and certifications*

In conclusion, many players confirm CNIL's analysis on the need to define technical references for the protection of personal data, particularly in Cloud computing. The ISO 27001 standard is regularly held up as an example in matters related to information system security. However, it should be noted that this is a generic standard that does not take account of all of the issues specific to privacy. ISO 27001 certification over a perimeter that completely encompasses the Cloud solution is therefore a reference in terms of security best practice but it does not fully meet expectations. Work is currently being done at the ISO to take better account of the problem of data protection, now that the perimeter studied has been properly established. Any work on standardization should take account of the maturity of the services and consequently this approach seems most likely to concern IaaS services in the short term.

CNIL's role will be to advise data controllers on the best practices to adopt, and to participate in the standardization work being done by the sector. The work of the CSA (Cloud Security Alliance), in which CNIL is participating, seems to provide a context for the work that is recognized by everyone and could include the question of personal data protection.

[10] The Norwegian authority has banned the use of Google Docs in various cases, particularly where personal data are concerned. The Danish authority has banned its use where sensitive data are concerned.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - T.: +33 (0)1 53 73 22 22 – F.: +33 (0)1 53 73 22 00