CNIL
Commission Nationale de l'Informatique et des Libertés

Recommendations for companies planning to use Cloud computing services

From a legal standpoint, CNIL finds that Cloud computing raises a number of difficulties with regard to compliance with the legislation on the protection of personal data, in particular in the case of public Cloud. These difficulties are amplified in the case of standard offers with standard contracts that customers are not able to negotiate. In general, it is found that customers suffer from a lack of transparency on the part of Cloud service providers regarding the conditions for provision of the services, particularly in terms of security and knowing whether their data are transferred abroad, and more precisely, to which country.

Consequently, it is essential that any French company planning to use a Cloud computing service conducts a risk analysis and is very strict in the choice of its service provider. In particular, the company must take into consideration the guarantees offered by a service provider regarding the protection of personal data and must make sure that the service provider will give it all the necessary guarantees to fulfil its obligations under the Data Protection Act, particularly in terms of information to data subjects, regulation of transfers and data security. Note that if it is impossible to negotiate a contract, it is essential to compare the contractual conditions proposed by the different service providers. This allows a choice to be made based on both economic and legal and technical considerations.

As concerns security, CNIL finds that the recognised Cloud offers can have security levels higher than those that can be guaranteed by SMEs. However, Cloud generates new risks, both for the service provider and for the customer, in particular in terms of the permanence of the data. It is therefore necessary to ensure that these new risks are controlled before choosing a Cloud solution.

CNIL has prepared the following recommendations to help French companies, and especially SMEs, to make an enlightened decision when they plan to use Cloud computing services. These guidance recommendations are based mainly on a risk analysis carried out beforehand by customers and undertakings of transparency on the part of service providers towards their customers which must be formalised in the service contracts.

Recommendation 1: Clearly identify the data and processing operations which will be passed to Cloud

Before planning to use Cloud computing, a data controller customer must clearly identify the data, the processing operations or the services which may be hosted in Cloud.

For each type of processing, the customer must establish which types of data may be concerned, distinguishing between:

- personal data,
- sensitive data[1],
- strategic data for the company,
- data used in business applications.

If only some of the data and processing are transferred to Cloud, such as the messaging software, for instance, the customer must make sure that the processing operations transferred to Cloud are not likely to include data of other processing operations which have not migrated. An example of this is the use of a "Cloud" messaging service in which staff members exchange content that is strategic for the company.

In addition, certain types of data are subject to specific regulations, and it is therefore necessary to check whether the data which may be transferred to Cloud are subject to such obligations and, if so, to identify the minimum conditions for their transfer. For example, medical data can only be stored in a medical data host approved by the Ministry of Health.

Recommendation 2: Define your own requirements for technical and legal security

The transition to Cloud requires a rigorous approach in terms of technical and legal security.

Unlike conventional outsourcing offers, in which service providers provide a tailor-made response to a specification defined by the customer, many Cloud offers are "standard" for all customers and do not meet a particular specification.

However, the customer must define his own requirements and assess whether the offers envisaged meet all the requirements defined. While the purpose of Cloud is to relieve the customer of certain operational tasks, he must make sure in principle that the service provider observes a requirement level that is at least equal to his own.

[1] Sensitive data in the meaning of Article 8 of the French Data Protection Act or data covered by Article 9.

The requirements must include all the important points for the customer and must consider, in particular:

- the legal constraints (location of data, guarantee of security and confidentiality, regulations specific to certain types of data, etc);
- the practical constraints (availability, reversibility/portability[2], etc);
- the technical constraints (interoperability with existing system, etc).

For "business" data and processing, the customer must take special care to guarantee reversibility and must make sure that a sufficient level of availability is guaranteed by the service provider and by his Internet access provider.

Recommendation 3: Carry out a risk analysis to identify the security measures essential for the company

Carrying out a full risk analysis is essential for companies to be able to define the appropriate security measures to be demanded of the service provider or to be put in place within the company. The EBIOS[3] method is relevant as a risk analysis method provided that personal data are considered as property to be protected and that the impacts on the privacy of the data subjects are taken into account.

For organisations which do not have the means to conduct a full analysis, the Authority wishes to highlight the following risks, which are more significant in the case of Cloud than in conventional computer processing, and which are particularly relevant for the protection of personal data. A more complete list of 35 risks supplied by ENISA[4] can also be used.

The main risks identified by the Authority are as follows:

- loss of governance regarding processing;
- technological dependency on the Cloud Computing supplier, i.e. the impossibility of changing solution (for another supplier or an internal solution) without loss of data;
- flaw in the isolation of the data, that is, the risk that the data hosted on a virtualised system will be modified or made accessible to unauthorised third parties, following a failure by the service provider or poor management of the hypervisory role;

[2] Reversibility (or portability) means the possibility of obtaining a copy of all one's data in a structured and widely-used format. This enables the data controller to ensure that he can change solution if necessary without any loss of information (data, structure, etc).

[3] The EBIOS method (Expression of Needs and Identification of Security Objectives) makes it possible to assess and handle the risks related to the security of information systems (SIS). It can also be used to communicate about them within the organisation and to its partners in order to contribute to the SIS risk management process.

[4] European Network and Information Security Agency; report available in English and Spanish from the following address: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

  - judicial requisitions, in particular by foreign authorities;
  - a flaw in the subcontracting chain, if the service provider himself has used third parties to provide the service;
  - ineffective or non-secure destruction of data, or excessive retention period;
  - problem of management of access rights for data subjects caused by the inadequacy of means put in place by the service provider;
  - unavailability of service, which includes unavailability of the service itself but also unavailability of the means of access to the service (particularly network problems);
  - shutdown of service or takeover of service provider by a third party;
  - non-compliance with regulations, in particular on international transfers.

If only part of the data and processing are transferred to Cloud, such as messaging software, the customer must also consider the impact of partial migration on processing and data that are not transferred; for instance, if sensitive or strategic data are explicitly excluded from transfer to Cloud, the processing operations necessitating the sending of such data by email must be adapted.

Most of these risks should be reduced by contractual provisions, that can include penalties for the service provider, and by technical and organisational measures for the customer and the service provider. CNIL recommends that the customer assess the relevance of these risks for his own situation and study the measures put in place by himself and by the service provider to reduce these risks.

Recommendation 4: Identify the relevant type of Cloud for the planned processing

There are various Cloud computing service offers on the market, which can be distinguished according to three service models and three deployment models.

The service models are as follows:

- SaaS: "Software as a Service", that is, online software provisioning;
- PaaS: "Platform as a Service", that is, online application development platform provisioning;
- IaaS: "Infrastructure as a Service", that is, online computing and storage infrastructure provisioning.

The deployment models are as follows:

- "Public" when a service is shared and pooled between many customers;
- "Private" when the Cloud is dedicated to one customer;

- "Hybrid" when a service is partly in a public Cloud and partly in a private Cloud. In this case we consider that the service can be studied as two interconnected processing types. We shall therefore not refer to this deployment model.

As each Cloud computing service offer is specific, they should be compared by identifying the strengths and weaknesses of each one in terms of the processing type considered. An analysis of this kind will make it possible to select the most appropriate Cloud computing offer.

Note that it is quite possible to choose different Cloud computing solutions according to the processing type. For example, a French public IaaS service can be chosen for the company's website, an accredited medical server for the medical data and a private European SaaS for emails.

Not only does such an approach make it possible to choose the most appropriate offer for each particular type of processing, but it also guarantees better protection of the data collected by a company because they are not all entrusted to the same Cloud computing service provider.

Finally, a step-by-step approach can allow a gradual transition to Cloud computing and thus a better understanding of the particular risks of Cloud computing. It will then be possible to draw on the first experiences to develop internal practices and better negotiate or better choose the subsequent contracts.

The transfer of processing or data to Cloud can thus be done progressively by data category and increasing security requirements; for example, beginning with the transfer of support software (messaging system, diary, contacts, etc), followed by applications containing sensitive or strategic data (for instance, HR processing operations), and finishing with the business applications.

Recommendation 5: Choose a service provider offering sufficient guarantees

As data controllers, the customers of Cloud computing services must ensure that they are able to fulfil their obligations. To do so, they must choose service providers that guarantee the setup of appropriate measures of security and confidentiality, and who are transparent towards their customers regarding the means used to provide their services (transfer of data abroad, use of subcontractors, security policy and measures, etc).

The choice of a service provider must be made in consideration of the following analytical grid:

Step 1: Determine the service provider's legal qualification

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

However, CNIL finds that in some cases of public PaaS and SaaS, customers, although responsible for the choice of their service providers, cannot really give them instructions and are not in a position to monitor the effectiveness of the security and confidentiality guarantees given by the service providers. This absence of instructions and monitoring facilities is due particularly to standard offers that cannot be modified by the customers, and to standard contracts that give them no possibility of negotiation.

In such situations the service provider could in principle be considered as joint controller pursuant to the definition of "data controller" given in Article 2 of Directive 95/46/EC, since he contributes to the definition of the purposes and means for personal data processing.

In cases where there are joint controllers, the responsibilities of each party should be clearly defined.

CNIL then suggests the following division of responsibilities:

Assumption	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**[5]	**Customer**[6]	**Customer + Service Provider**	**Customer (with the service provider's support)**[7]

Identifying whether or not the service provider is a joint data controller serves to determine who is responsible towards the competent personal data protection authorities.

Indeed, by virtue of the powers conferred on it by the Data Protection Act, CNIL can monitor and sanction any data controller who does not fulfil his obligations pursuant to the Data Protection Act. Consequently, if the customer and the service provider are joint data controllers, they may both be monitored and potentially sanctioned.

[5] 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 carry out 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 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.

[6] 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 his 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 controller.

[7] The fact that 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 rights of access, correction, alteration, updating or deletion.

Step 2: Assess the level of protection given by the service provider for the data processed

Whatever the qualification of the service provider, the customer is responsible for choosing a service provider who provides a sufficient level of protection for the data he entrusts to him.

CNIL has listed below the essential elements, in terms of the protection of personal data, that should appear in a Cloud computing service contract.

Essential elements that should appear in a Cloud computing service contract

Information on processing

- Compliance with the European principles on the protection of personal data and the French Data Protection Act (particularly the principles of proportionality and compliance with purposes);

- Existence of a system for reporting complaints and security breaches;

- Processing means;

- Recipients of data;

- Subcontracting:

    - Informing and obtaining the consent of the customer if third parties or subcontractors, whether or not based abroad, are used to participate in the processing operation (Note: *if the service provider is a joint data controller, he only has to inform the customer and not obtain his consent*);

    - Passing on, in subsequent subcontracts entered into by the service provider, of the contractual obligations stipulated in the service contract signed between the customer and the service provider and definition of the subcontractors' contractual liability towards the service provider and the customer.

- Existence of simple procedures for observing the rights of the data subjects to their data (rights of access, alteration or deletion, etc).

Guarantees put in place by the service provider

- Limited and reasonable retention period for the data with regard to the purposes for which the data have been collected;

- Destruction and/or restitution of data at end of service or in case of early termination of the contract in a structured and widely-used format;

- Duty to cooperate with the competent data protection authorities;

- When the service provider is a data processor, indication that the customer can audit the service provider to make sure that these guarantees are effectively implemented.

Location and transfers

- Clear and complete indication of the countries hosting the service provider's data centres where the data will be processed;

- Assurance of adequate protection abroad (particularly by means of the EC Standard contractual clauses or binding corporate rules, "BCR");

- Possibility of limiting data transfers solely to member countries of the European Economic Area or to third countries recognised as providing an adequate level of protection by a decision of the European Commission (*Note: Unlike the other elements, this one is open to negotiation by the parties. At all events, a service provider who gives his customers the possibility of limiting data transfers to EEA member countries or to third countries providing an adequate level of protection as recognised by the European Commission, will offer his customers reinforced guarantees of data protection. However, customers must be aware that when they choose service providers located in third countries, the local administrative or judicial authorities may send requests to the service providers for access to the data);*

- Immediate information to the customer in case of a request from a foreign administrative or judicial authority.

Formalities with CNIL

- When the service provider is a data processor, the obligation to give the customer all useful information for making the processing notification to CNIL;

- When the service provider is a joint data controller, the customer and the service provider must decide which party will be responsible for the formalities on its own behalf and on behalf of the other party. Whichever solution is chosen, the party not declaring must give the one accomplishing the notification formalities all useful information for making the processing notification to CNIL.

Security and confidentiality

- Indication of the obligations incumbent on the service provider for security of the data and, when he is a data processor, the specification that he can only act on the customer's instruction;

- Security policy and minimum security measures:

[Note: the data processor service provider must make available to the customer the details of the measures put in place, while a service provider who is a joint data controller only has to guarantee that sufficient measures have been put in place.]

    - Existence of an accessible security policy;
    - Measures of physical safety and security on the host site (protection of site and security of access, electrical safety and air-conditioning systems, etc);
    - Measures needed to ensure the availability, integrity and confidentiality of the data: for example, encryption of data and procedures to guarantee that the service provider does not have access to the data entrusted to him (encryption on customer side, with a recognised algorithm and adequate management of keys, before any transfer) and encrypted link with the Cloud server (e.g. https or VPN connection), etc;
    - Other logical security measures (protection of network (firewall, antivirus, intruder detection, etc), management of updates, protection of terminal, management of authorisations, staff authentication, security of application developments, etc);

  - Certifications: proof of relevant certifications by independent and qualified auditors, such as an ISO 27001 certification on a perimeter that includes all the services provided, strict definition of a policy for audit of the service provider by the customer included in the general guarantees *[Note: unlike the other elements, certification is open to negotiation by the parties. At all events, a service provider who has a certification will offer his customers reinforced guarantees of data protection]*;

  - Reversibility/portability: guarantee the easy reversibility or portability of the data in a structured and widely-used format, at the customer's request and at any time;

  - Traceability: access to traceability logs of actions performed on the data by the customer's and service provider's staff and reporting of any anomaly detected by the service provider;

  - Continuity of service, backups and integrity: backup system, redundancy of servers, etc;

  - Service Level Agreements or SLAs: undertakings that are binding for the service provider on the service level, that should stipulate penalties for the service provider if the contractual undertakings are not fulfilled. This must be put in place in particular for the clauses on data protection (retention period, exercise of rights of data subjects, availability of processing, etc).

In light of the essential elements identified by CNIL, models of contractual clauses that can be inserted in the service contracts are proposed in the appendix.

These model clauses are designed to help companies who are Cloud service customers, and in particular SMEs, to choose a service provider offering all the necessary guarantees in terms of personal data protection and security in accordance with the French Data Protection Act.

CNIL recalls that if these essential elements do not appear directly or indirectly in a service contract, the customers will be unable to fulfil their legal obligations as data controllers.

As a consequence, service providers who do not offer these essential guarantees in their contracts and who refuse any negotiation with their potential customers should not be selected. Indeed, by accepting such insufficient contractual conditions, customers run a high risk of failing to comply with current legislation.

In addition, when it is not possible to negotiate a Cloud computing service contract with a service provider, these essential elements must also serve as a basis for customers to compare the different offers available on the market and make a relevant choice which takes account of their legal obligations.

Recommendation 6: Review the internal security policy

Cloud computing requires a complete review of the internal procedures in line with the conclusions of the risk analysis. In fact, the use of Cloud introduces new risks related, in particular, to transmissions via the Internet or the use of mobile terminals. Special attention must be paid to the mechanisms for authentication of employees and the Cloud service provider must offer a service compatible with these security requirements.

Recommendation 7: Monitor changes over time

In a spirit of continuous improvement, CNIL recommends that the Cloud computing service be assessed periodically in light of changes over time in the context, the risks, the solutions available on the market, legislation, etc.

In particular, the recommended risk analysis must be updated as soon as a significant change in the service takes place in order to adapt the measures or solutions as soon as necessary. These changes may concern the functionalities of the product or the technical provision of the service (new data centre, change in security policy, change in processing initiated by the customer, etc).

Appendix: Models of contractual clauses

CNIL proposes models of contractual clauses containing the essential elements listed in Recommendation 5. These models can be inserted into Cloud computing service contracts.

Note that in themselves, these clauses do not constitute a service contract. Furthermore, it may be necessary to adapt them according to the context, the co-contractors, etc.

Note: The words beginning with a capital letter must be defined in the "Definitions" part of the contract ("Customer", "Service Provider", "Parties", "Data", "Service", "Processing", etc).

1) Information on processing

a) Observance of French principles on the protection of personal data

[The following model clause may be used when the service provider is a data processor]

"The Parties undertake to collect and process all personal data in compliance with any current regulation applicable to the processing of these data, and in particular with Law 78-17 of 6 January 1978 amended. According to this law, the Customer is data controller for the Processing carried out under the Contract."

[The following model clause may be used when the service provider is a joint data controller]

"The Parties undertake to collect and process all personal data in compliance with any current regulation applicable to the processing of these data, and in particular with Law 78-17 of 6 January 1978 amended. According to this law, the Parties are joint data controllers for the Processing carried out under the Contract. "

b) Existence of a system for reporting complaints and security breaches

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"The Service Provider undertakes to inform the Customer of the occurrence of any security breach having direct or indirect consequences on the Processing, as well as of any complaint sent to him by any individual concerned by the Processing carried out under the Contract. This information must be communicated as soon as possible and no later than forty-eight hours after the discovery of the security breach or following the receipt of a complaint."

c) Processing means

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"To provide the Service, the Service Provider shall process the Data using the following processing means: [provide a description of the software resources and processing techniques used by the Service Provider]."

d) Subcontracting

[The following model clause may be used when the service provider is a data processor]

"The Service Provider informs the Customer, who accepts, that he will have the Contract performed by the following subcontractors: [indicate their names and their country of location if they are established in a third country].

If applicable, the Service Provider undertakes to pass on, in his agreements with subcontractors, the obligations incumbent on him under the Contract.

The Service Provider shall remain solely liable towards the Customer for the fulfilment of his contractual obligations arising from this contract."

[The following model clause may be used when the service provider is a joint data controller]

"When the Service Provider uses subcontractors, he must inform the Customer thereof and provide him with a list of the data recipients.

If applicable, the Service Provider undertakes to pass on, in his agreements with subcontractors, the obligations incumbent on him under the Contract.

The Service Provider shall remain solely liable towards the Customer for the fulfilment of his contractual obligations arising from this contract."

e) Existence of simple procedures for respecting the rights of the data subjects to their data

[The following model clause may be used when the service provider is a data processor]

"The Service Provider undertakes to cooperate with the Customer and help him to meet the legal requirements incumbent on him for the protection of personal data, in particular in order to respect the rights of the data subjects pursuant to Articles 38 to 43 of Law 78-17 of 6 January 1978 amended."

[The following model clause may be used when the service provider is a joint data controller]

"The Parties undertake to put in place simple procedures allowing the data subjects to exercise their rights pursuant to Articles 38 to 43 of Law 78-17 of 6 January 1978 amended."

2) Guarantees put in place by the service provider

a) Limited and reasonable retention period for the data with regard to the purposes for which the data were collected

[The following model clause may be used when the service provider is a data processor]

"The Service Provider undertakes not to retain the Data after the retention period set by the Customer with regard to the purposes for which they were collected, and at all events not to retain them after the end of the Contract."

[The following model clause may be used when the service provider is a joint data controller]

"The Service Provider undertakes not to retain the Data after the retention period set by agreement with the Customer with regard to the purposes for which they were collected, and at all events not to retain them after the end of the Contract."

b) Destruction and/or restitution of data

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"At the expiry of the Contract or in the event of its early termination for any reason whatsoever, the Service Provider and his subcontractors if any shall return without delay to the Customer a copy of all the Data in the same format as that used by the Customer to communicate the Data to the Service Provider or failing this, in a structured and widely-used format.

This restitution shall be ascertained by a report dated and signed by the Parties.

Once the restitution has been carried out, the Service Provider shall destroy the copies of the Data held in his computer systems within a reasonable period and shall provide proof thereof to the Customer within a reasonable period following the signature of the restitution report."

c) Duty to cooperate with the competent data protection authorities

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"The Parties undertake to cooperate with the competent data protection authorities, particularly when they receive a request for information or in the case of an inspection."

d) Audits

[The following model clause may be used when the service provider is a data processor]

"The Customer reserves the right to conduct any checks he considers useful to ascertain the Service Provider's fulfilment of his obligations under the Contract, particularly through an audit.

The Service Provider undertakes to reply to the Customer's requests for audit to be carried out by the Customer himself or by a trusted third party whom he has selected, who is recognised as an independent auditor, that is, independent of the Service Provider, having an appropriate qualification, and free to give the details of his comments and audit conclusions to the Customer.

Audits must allow an analysis of compliance with this Contract and with the French Data Protection Act, in particular:

- *by the verification of all the security measures used by the Service Provider,*
- *by the verification of the Data location, copying and deletion logs,*
- *by an analysis of the measures put in place to delete the Data, to prevent any illegal transmission of Data to inappropriate courts or to prevent the transfer of Data to a country not authorised by the Customer.*

Finally, the audit must make it possible to ensure that the security and confidentiality systems put in place cannot be circumvented without this being detected and reported."

Note: When the service provider is a joint data controller, the customer does not have to be entitled to conduct audits of the service provider, although this is an additional guarantee for the customer.

3) Location and transfers

a) Recipients

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"The Service Provider shall provide the Customer with all useful information concerning the recipients of the Data, so that the Customer is able to inform the data subjects and respond to their requests for access pursuant to Articles 32 and 39 of Law 78-17 of 6 January 1978 amended."

b) Clear and complete indication of countries hosting the service provider's servers

[The following model clause may be used when the service provider is a data processor]

"The Service Provider informs the Customer that the Data will be hosted in servers located in the following countries: [provide a complete list of the countries hosting the service provider's servers].

If the recipient countries are changed by the Service Provider, he shall inform the Customer thereof in advance without delay and obtain his written consent. If applicable, the Service Provider shall provide the Customer with an updated list of recipient countries."

[The following model clause may be used when the service provider is a joint data controller]

"The Service Provider informs the Customer that the Data will be hosted in servers located in the following countries: [provide a complete list of the countries hosting the service provider's servers].

If the recipient countries are changed by the Service Provider, he shall inform the Customer thereof without delay. If applicable, the Service Provider shall provide the Customer with an updated list of the recipient countries."

c) Assurance of adequate protection abroad (in particular by means of the EC Standard contractual clauses or binding corporate rules – BCR)

[The following model clause may be used when the service provider is a data processor]

"The Customer must ensure that sufficient guarantees are given to regulate Data transfers, in particular by the use of binding corporate rules (BCR) for subcontractors or by the signature of the Standard contractual clauses adopted by the European Commission with the parties concerned, including the Service Provider and any subcontractors."

[The following model clause may be used when the service provider is a joint data controller]

"The Parties must ensure that sufficient guarantees are given to regulate Data transfers, in particular by the use of binding corporate rules (BCR) or by the signature of the Standard contractual clauses adopted by the European Commission with the parties concerned, including any subcontractors."

d) Possibility of limiting data transfers solely to third countries providing an adequate level of protection

Note: Unlike the other elements this one is open to negotiation by the parties. At all events, a service provider who gives customers the possibility of limiting data transfers to member countries of the European Economic Area or to third countries providing an adequate level of protection as recognised by the European Commission will offer his customers reinforced guarantees of data protection. However, customers should be aware that when they choose service providers located in third countries, the local administrative or judicial authorities may send requests to the service providers for access to the data (cf. Clause 3.e) herebelow).

[The following model clause may be used when the service provider is a data processor]

"When the Customer has accepted that the Service Provider will use one or more subcontractor(s), the Parties agree that the Data may only be transferred by the Service Provider to subcontractors located in member countries of the European Economic Area and/or third countries recognised by the European Commission as providing an adequate level of protection."

[The following model clause may be used when the service provider is a joint data controller]

"When the Service Provider uses one or more subcontractor(s), the Parties agree that the Data may only be transferred by the Service Provider to subcontractors located in member countries of the European Economic Area and/or third countries recognised by the European Commission as providing an adequate level of protection."

e) Informing the Customer in the case of a request by a foreign administrative or judicial authority

[The following model clause may be used when the service provider is a joint data controller]

"If the Service Provider receives a request from a foreign administrative or judicial authority, he undertakes to inform the Customer thereof immediately."

4) Formalities with CNIL

[The following model clause may be used when the service provider is a data processor]

"The Customer shall accomplish the notification formalities concerning the Processing to the competent data protection authorities. The Service Provider undertakes to give him all useful information for accomplishing these formalities."

[The following model clause may be used when the service provider is a joint data controller]

"The Parties agree that [choose between the Customer and the Service Provider] shall accomplish the notification formalities concerning the Processing to the competent data protection authorities. [The Customer or the Service Provider, depending on what has been decided] shall give the declaring party all useful information for accomplishing these formalities.

[The Customer or the Service Provider, depending on what has been decided] shall give the other party, on request, proof that the required formalities have been accomplished."

5) Security and confidentiality

a) Indication of obligations incumbent on the service provider for security of the data and, when he is a data processor, stipulation that he can only act on the customer's instruction

[The following model clause may be used when the service provider is a data processor]

"In the performance of the Contract, the Service Provider shall act only on the Customer's instructions. In this respect, the Service Provider undertakes not to use the Data on his own behalf or on behalf of a third party.

In accordance with Article 34 of the French Data Protection Act amended, the Service Provider undertakes to take all necessary precautions to preserve the security of the data and in particular to protect them against any accidental or unlawful destruction, accidental loss, alteration, unauthorised diffusion or access, particularly when the Processing includes transmissions of data within a network, as well as against any other unlawful form of processing or communication to unauthorised persons."

[The following model clause may be used when the service provider is a joint data controller]

"In accordance with Article 34 of the French Data Protection Act amended, the Service Provider undertakes to take all necessary precautions to preserve the security of the data and in particular to protect them against any accidental or unlawful destruction, accidental loss, alteration, unauthorised diffusion or access, in particular when the Processing includes transmissions of data within a network, as well as against any other unlawful form of processing or communication to unauthorised persons."

b) Security policy and security measures

[The following model clause may be used when the service provider is a data processor]

"The Service Provider shall communicate to the Customer the security policy for the information systems which he has put in place and inform him of changes to this policy. He shall make available to the Customer the documents relating to the security of his data including, in particular, the necessary technical documentation, the risk analyses produced and a detailed list of the security measures implemented.

The data media and documents supplied by the Customer to the Service Provider remain the property of the Customer.

The data contained in these media and documents are strictly covered by professional secrecy (Article 226-13 of the French Criminal Code); the same applies to all the data whereof the Service Provider shall have knowledge on the occasion of the performance of the Contract.

The Service Provider undertakes to fulfil the following obligations and have them fulfilled by his staff:

- not to take any copies of the documents and information media entrusted to him, with the exception of those necessary for the performance of the present service as stipulated in the Contract with the Customer's prior agreement;

- not to use these processed documents and information for any other purposes than those specified in this Contract;

- not to disclose these documents or information to other entities, whether private or public, individual or legal;

- to take all steps to prevent any misappropriation or fraudulent use of the computer files during the performance of the Contract."

[The following model clause may be used when the service provider is a joint data controller]

"The Service Provider shall communicate to the Customer the security policy for the information systems which he has put in place and inform him of changes to this policy. He shall inform the Customer of the potential risks related to the Processing.

The information media and documents supplied by the Customer to the Service Provider remain the property of the Customer.

The data contained in these media and documents are strictly covered by professional secrecy (Article 226-13 of the French Criminal Code); the same applies to all the data whereof the Service Provider shall have knowledge on the occasion of the performance of the present Contract."

c) Certification

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

Note: Unlike the other elements, the clause below is open to negotiation by the parties. At all events, a service provider who has a certification may offer his customers reinforced guarantees of data protection.

"The Service Provider shall inform the Customer that he has the [enter the name of the certification obtained by the service provider] certification for the perimeter concerned by the Processing carried out by the Customer. The Service Provider shall communicate to the Customer the perimeter concerned by the certification. He also undertakes to maintain throughout the term of the Contract the criteria to meet the requirements of the certification obtained."

d) Reversibility/portability of data

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"At the Customer's request, at any time and for any reason whatsoever, the Service Provider and his subcontractors if any shall give the Customer without delay a copy of all his Data in the same format as the one used by the Customer to communicate the Data to the Service Provider or, failing this, in a structured and widely-used format."

e) Traceability

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"The Service Provider shall make available to the Customer the records of connection to the Data processed by the authorised staff of the Parties and, if applicable, the data subjects, for a period of [insert the retention period for the records of connection by the service provider] months."

Note 1: It is recommended that this period be three or six months, depending on the confidentiality of the data processed.

Note 2: If the service provider participates in the analysis of the data connection records or if he offers the Customer a service of analysis of the data connection records, the following clause should be added:

"*The Service Provider shall inform the Customer of any anomaly which he detects in these connection records.*"

f) Continuity of service, backups and integrity

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"The Service Provider undertakes to take the necessary steps to ensure the preservation and integrity of the documents and information processed throughout the term of the Contract.

He undertakes to use a system for backup of the Data and continuity of service the details whereof are given in the service level agreement appended to the Contract."

g) Service level agreements

[The following model clause may be used whether the service provider is a data processor or a joint data controller]

"The Service Provider commits to the service levels defined in the service level agreement appended to the Contract."

Note: append a service level agreement to the service contract.