ReedSmith

Client Alert

Global Regulatory Enforcement

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Daniel Kadar
Partner, Paris
+33 1 76 70 40 86
dkadar@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Cloud Computing: The French CNIL Takes Position and Issues Partly Binding Guidance

Cloud computing is obviously coming more and more under scrutiny of the Data Protection authorities: just a few weeks after the International Working Group on Data Protection in Telecommunications had issued its "Working Paper on Cloud Computing", the French CNIL issued its own « Recommendations » in that regard, as a conclusion to a broad consultation it had launched at the end of 2011.

On 25 June 2012, the CNIL published on its website a summary article and a 10 page conclusion paper, along with a 21-page "recommendations" document in that regard.

(i) The CNIL observes that cloud computing raises several issues regarding the current data protection legislation (e.g., security, applicable law, data transfer, etc.), which have become a source of its concern since cloud computing is marketed through standard offers that the CNIL compares to adhesion contracts that leave clients with no room for negotiation. The documentation prepared by the CNIL therefore seems to target small- to medium-sized companies considering using cloud computing services, and is aimed at helping them make more informed decisions regarding such services.

But where the International Working Group on Data Protection in Telecommunications proposes an approach through quality certifications and higher standards of protection, the CNIL already delivers guidance and sets a standard of its own, and for all: the "recommendations" are in fact seven principles, to which the CNIL connects five "essential elements that have to be part to a Cloud computing services agreement".

(ii) These seven "recommendations" are:

1. The cloud computing agreement should clearly identify the data and the processing that will occur in the cloud.

The client should establish what type of data is concerned and make the necessary distinction between regular, sensitive, economically strategic data, etc., in order to be provided with adequate protection according to each type of data.

2. The agreement should define its own technical security and legal requirements.

Many cloud offers are standard offers, and the CNIL considers that the client should be in a position to define its own legal, practical, and technical constraints.

3. The agreement should be based on a risk assessment conducted in order to identify the essential security measures for the company.

The CNIL outlines in that regard that ENISA, the European Network and Information Security Agency, provides a complete list of 35 risks relevant to cloud computing data processing.

4. The client to a cloud computing agreement must have been put in a position allowing him to identify the "pertinent" type of cloud relevant to the planned processing.

The CNIL distinguishes between three service models: (1) Saas "Software as Service", (2) Paas "Platform as Service", and (3) Iaas "Infrastructure as Service", as well as between three deployment models: (1) "Public", (2) "Private", and (3) "Hybrid".

5. The client must be able to choose a cloud computing service provider with sufficient guarantees.

In that regard, the CNIL refers to the "essential elements that have to be part to a cloud computing services agreement" (see below).

6. Implementing cloud computing requires a prior extensive review of all internal security policies.

Cloud computing presumes that internal procedures will be fully reviewed according to the risk assessment conclusions.

7. Evolutions over time need to be monitored on a regular basis.

The French Agency recommends periodic evaluations of the cloud computing service, whose context, risks, market solutions and legislation are constantly evolving.

(iii) The binding effect of these "recommendations" is laid out in the middle of the document, in a three-page list of the "essential elements that have to be part to a Cloud computing services agreement".

Five such "essential elements" are listed and detailed. The cloud computing agreement must contain:

1. All information relevant to the data processing (compliance with European data protection principles, addressees, description of IT security failures reporting, sub-contracting conditions, right of access and modification…).

2. The guarantees put in place by the data processor (data retention, destruction at termination date, cooperation requirement with the Data Protection Authorities, possibility to audit, etc.).

3. All necessary information related to the location and transfers of data, as well as the evidence that an "adequate level of protection" is implemented.

4. The obligation to comply with all required notification duties with the CNIL.

5. The essential obligations as to data security and confidentiality (data integrity, back-up, disaster recovery, security policy, etc.).

In order to better implement these "essential elements", the CNIL offers 10 pages (…) of model clauses that *may* be utilized in this agreement.

(iv) Another essential point that the CNIL outlines in its guidance is that, in its view, the cloud computing service provider can hardly escape the legal qualification of **data controller** as soon as this service provider enjoys a large autonomy in the definition of its duties, if it has large monitoring powers over the cloud computing service, if its clients have low controlling powers, and if the level of transparency to the clients is low.

The CNIL outlines this definition of data controller in particular with respect to the data confidentiality and security obligations, the client bearing on his side the notification and data owner information obligations.

(v) Finally, the CNIL outlines that one remaining unsolved question is the applicable law to the cloud computing agreement, in particular regarding cloud computing service providers that are not established in the EU. For these service providers, the CNIL reasserts that French law shall be applicable as soon as this service provider uses technical means on the French territory.

The French Agency therefore seems to already want to impose its own contractual norms. Data protection regulation is now reaching out to the sky.