SQUIRE SANDERS

THE FRENCH DPA ISSUES ITS GUIDELINES ON CLOUD COMPUTING

Since launching its consultation in October 2011, France's Commission nationale de l' informatique et des libertés (CNIL) has bided its time in issuing its long awaited Guidelines. Businesses have had a tough time negotiating with cloud providers over the various compliance issues raised by the data protection legislation. The Guidelines should clarify a number of issues, even if they fail to ease the pressure on cloud providers.

The Guidelines were published on 25 June 2012, shortly after the release of WP 29's checklist for Processor BCRs. They contain recommendations and a list of essential elements that a cloud service agreement should contain (as well as corresponding draft clauses).

The recommendations

The CNIL make a series of recommendations with a view to urging any client, before opting for cloud services, to:

- Carry out a risk assessment;
- Define their security requirements (and adapt their own security policy to cloud);
- Select the most appropriate cloud offer for each type of processing; and
- Carefully choose a cloud provider based on the technical and legal warranties that they are offering.

On the issue of security, the CNIL recognizes that encryption is not yet a technically operational tool (except for IaaS storage).

Once the cloud service agreement is in place, further risk assessments should be carried out at regular intervals.

The CNIL, referring to the risk assessment matrix prepared by ENISA[1], lists the risks that it has identified: loss of governance; lock in; isolation failure; subpoena and access requests by foreign authorities; breach by sub-contractors (supply chain failure); access control management issues (due to under provisioned resources); service failure, insecure or incomplete deletion of data or excessive retention; cloud services termination or cloud provider acquisition; and non-compliance with rules concerning the international transfer of data.

The parties need to define the capacity in which the cloud provider is acting. The cloud provider will normally be considered a "data processor". However, for certain public cloud services such as PaaS or SaaS - for which clients are unable to effectively give "instructions" and monitor the confidentiality and security undertakings of the cloud provider (as a result of non-negotiable T&Cs) - the cloud provider may be considered a joint controller.

In such cases, the CNIL recommends that the client remains the main contact for itself as well as for data subjects. However, the obligations on and the liability of the cloud provider will be increased and it could possibly become the subject of fines by the CNIL.

The contractual requirements

In accordance with the Guidelines, if any or all of these requirements are missing from an agreement with a cloud provider, the client will not be considered compliant with data protection laws and regulations.

Among these contractual requirements, the following are of particular interest (in circumstances where the cloud provider is considered a "data processor"):

- The agreement must have a Service Level Agreement with corresponding penalties or service credits;
- Both parties shall comply with EU data protection principles and French data protection law;
- There must be claim and data breach reporting systems;
- In relation to sub-contracting:
  - The cloud provider must inform the client and obtain their consent
  - The agreement with the sub-contractor must contain equivalent obligations in relation to data protection;

[1] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

- Data should be deleted or returned at the end of the contract;
- The cloud provider must have a duty to cooperate with local data protection authorities (DPAs);
- The agreement must specify that the client has the right to audit;
- The agreement must specify that the cloud provider can only act on instructions of the data controller;
- There must be a clear and exhaustive list of the countries hosting the data centers where the data is processed;
- There must be adequate protection abroad (for example, through the use of EU model clauses or Processor BCRs);
- There must be security requirements and the cloud provider must allow access to information on and details of security measures;
- Handover assistance/portability; and
- Traceability.

Some of these issues are already at the stumbling blocks of negotiations between global clients and public cloud providers. In particular, transparency on security measures and subcontracting arrangements, as well as audit rights, are presented as unworkable solutions that will potentially compromise security. In addition, cloud providers do not want to be obliged to cooperate with DPAs and, more generally have to comply with EU legislation and - pending harmonization through the proposed onerous Regulation - with the various European local data protection laws, which are not as such applicable to the cloud provider.

It will certainly be interesting to see whether these Guidelines are similar to those that should be published by WP 29 in due course.

For additional information (in French) on the Guidelines, please visit the CNIL website:

http://www.cnil.fr/la-cnil/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/

Contact

If you would like to informally discuss any of the issues raised in this review then please contact either

Stéphanie Faber
Of Counsel, Paris
T +33 1 5383 7400
E stephanie.faber@squiresanders.com

Ann LaFrance
Partner, London
T +44 207 655 1752
E ann.lafrance@squiresanders.com