ISSN: 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Op. J. Vol. I, n. I/2015

Crowding It the Cloud, Data Protection and Permissible Business Models

by

Célia Zolynski
Romain Perray

CROWDING IT THE CLOUD, DATA PROTECTION AND PERMISSIBLE BUSINESS MODELS

PRESENTATION

by

Célia Zolynski[*]

Romain Perray[**]

Abstract:

Far larger and more complex than usual personal data processing for example through emails, the development of Cloud Computing brings squarely into play the definitions of both personal data and their processing, within the meaning of EU Directive 95/46 dated 24 October 1995, until the coming enactment of the current draft EU Regulation in this field.

Of course, this situation has also large consequences in the IT sector, essentially on the way Cloud providers can organize their business models, depending however whether they act, in part or in full, as data controllers or data processors.

Under such circumstances, not only companies but consumers as well must think of an appropriate strategy in line with their needs in order to take all benefit of using Cloud systems without any prejudice to a high level of personal data protection.

Keywords: Cloud computing – IT Infrastructures – Public / Private / Hybrid Cloud – Infrastructure as a Service (IaaS) / Software as a Service (SaaS) / Platform as a Service (PaaS) - Business models - EU Directive 95/46/EC - Privacy - Data protection - Article 29 Working Party - Transparency - Accountability - Prior consent

---

[*] Professor of Law at Versailles Saint Quentin/ Paris-Saclay University, co-director of IP/IT law committee of the Network Trans Europe Experts.

[**] Avocat at the Paris Bar / Lecturer at Paris 1 – Panthéon Sorbonne University / Author of Lexis-Nexis and Lamy Practice Guide developments on data protection requirements under French Law.

Having a good understanding of the principles at the heart of privacy and data protection legislation is essential in consequence of the following simple fact: the ubiquity of IT systems in our day-to-day life.

Information and data concerning each of us are collected on a daily basis: they are processed and transferred, whether at work, when we buy goods or services, in the course of a loan application, indeed even for a simple phone call. Almost all of these operations have IT systems at their heart.

For the non-initiated, such situation is usually understood as data being physically transmitted from one location to another. Emails are the case in point. When you draft an email, data (not to mention that a larger number can be personal) are on your computer. When you press send, the email and the data thereto are transferred to the recipient of the email.

But technically speaking, the situation implies far more operations than imagined at first sight. When you draft an email, not only data (whose, again, a larger number can be highly personal even intimate) can be seen from your computer, but they are usually also located on the server which host the mail box. The same is true for the mail box of the recipient of the email. Not to mention all servers through which data go. Still, such situation can be understood as data being physically transmitted from one location to another.

To summarize it, Cloud Computing is a larger and more complex version of this situation. By reference to the definition provided by the Article 29 Working Party which gathers all EU Member States Data Protection Authority, Cloud Computing "*consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space*[1]".

Cloud providers offer a wide range of services ranging from virtual processing systems (which replace and/or work alongside conventional servers under the direct control of the controller) to service supporting application development and advanced hosting, up to web-based software solutions which can replace applications traditionally installed on personal computers. Above all, it includes all types of applications: text processing, agendas, calendars, filing systems for online document storage and, of course, outsourced email solutions.

Although all these things aim at facilitating our day-to-day life, by accessing data from everywhere, such operations also enable those who operate them to have an increasing access and, more and more often, knowledge of the private realm of those whose data are processed.

Even if Cloud Computing did not exist strictly speaking as today, the European Union already considered such possible intrusions in privacy as a main concern in the mid 1990's.

As a result, the EU decided to enact – in line with domestic legislations of some EU Members States such as Sweden, Germany or France[2] which adopted during the 1970's rules in this field – EU Directive No. 95/46 dated 24 October 1995 which aims at providing a balance between the right to privacy through personal data protection and the need for free movement of data.

Only by accessing, transmitting or even hosting end-users' data (whose a larger number can be highly personal even intimate), Cloud providers, in particular those located on the EU territory, face the obligation to comply with the requirements provided under EU Directive No. 95/46.

---

[1] Article 29 Working Party, Opinion 05/2012 on Cloud Computing, adopted 1rst July 2012, WP 196, p. 4.

[2] For more details in the case of France: A. Gruber, *Le système français de protection des données personnelles*, Rev. Les Petites Affiches (Lextenso ed., Paris), 4 May 2007, No. 90, p. 4.

This situation has of course consequences on the way they can organize their business models, depending however whether Cloud providers act, in part or in full, as data controllers or data processors.

Various types of cloud systems and business models

By reference to the presentation made in the Article 29 Working Party's opinion on Cloud Computing, various distinctions can be drawn in this sector, the first being between private and public Clouds.

Distinctions between private and public Clouds

To sum up, private Cloud describes an IT infrastructure that is dedicated to an individual organization. It is very similar to conventional data centres, the difference being that technological arrangements are implemented to optimize use of the available resources and enhance those resources via small investments that are made in a stepwise fashion over time. Usually, it is located at the organization's premises themselves. Alternatively, its management can be outsourced to a third party (most of the time through server hosting). In both cases, the Cloud system remains fully under the Cloud provider's client who therefore acts as data controller. As far as he is concerned, the Cloud provider is only regarded as data processor.

Public Cloud, conversely, is an infrastructure owned by a provider specializing in the supply of services that makes available – and therefore shares – his systems to/among users, businesses and/or public administrative bodies. The services can be accessed through the Internet, which entails transferring data processing operations and/or the data to the service provider's systems. Therefore the service provider takes on a key role as regards to the effective protection of the data committed to his systems. Along with the data, a user is bound to transfer a major portion of his control over those data.

Alongside "*public*" and "*private*" Clouds, there are alternative systems which can be called "*intermediate*" or "*hybrid*" Clouds. In such systems, services provided by private infrastructures co-exist with services purchased from public Clouds. IT infrastructure can also be shared by several organizations within a "*community cloud*", that means for the benefit of a specific user community.

A second distinction can be made between three sorts of service provision models. They usually apply to both private and public Cloud solutions:

The first model is called Cloud Infrastructure as a Service or IaaS. Basically, the Cloud provider leases a technological infrastructure, notably virtual remote servers, the end-user can rely upon in accordance with mechanisms and arrangements such as to replace, for example, the corporate IT systems at the company's premises. Such providers are usually specialized market players. They can rely on a physical and complex infrastructure that is usually located on different geographic areas.

The second model is known as Cloud Software as a Service or SaaS. The provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems. Accordingly, users are ultimately meant to outsource their data to the individual provider. This is

the case, for instance, of typical web-based office applications such as spreadsheets, text processing tools, computerized registries and agendas, shared calendars.

The third service model is called Cloud Platform as a Service or PaaS. The provider offers solutions for the advanced development and hosting of applications. These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties.

With regard to this situation, we can come to a first conclusion in line with the Article 29 Working Party. That is Cloud clients shall be considered as being data controllers, to the extent they determine the ultimate purposes of the processing and decide on their outsourcing in full or in part. Above all, it means that, as such, Cloud clients are fully liable of any breach to Privacy and Data Protection requirements and are subject to all legal duties arising from the EU Directive No. 95/46 as domestically implemented.

In such scenario, Cloud providers will be conversely regarded as data controllers to the extent that they only provide Cloud clients with IT means and/or platform. As true as it can be, such conclusion applies however mainly to private Clouds. The situation can be indeed the complete opposite in public Clouds.

In this latter case, Cloud providers are actually in a very similar position to social networks providers who are regarded by the Article 29 Working Party as data controllers and no longer as data processors[3].

In its opinion on Cloud computing, the Article 29 Working Party has of course taken into consideration this possibility, but also grey areas. According to him "*there may be situations in which a provider of cloud services may be considered either as a joint controller or as a controller in their own right depending on concrete circumstances. For instance, this could be the case where the provider processes data for its own purposes*[4]".

In such circumstances, the question is: what would be the consequences with regard to the permissible business models? We would say almost none. Meaning that almost all business models would be permitted, but – and this is the difference – might be significantly restricted to the extent that cloud providers shall be subject, as data controllers, to a far larger range of obligations as they would be if they only act as data processors.

Obligations potentially affecting cloud providers' business models

Profitability of the business models implemented by Cloud providers might be, above all, affected when they act as data controllers. As indicated previously, doing so requires complying with all duties provided under the EU Privacy and Data Protection Directive as well as domestic legislations.

Among these duties, our attention will focus on the most essential data quality as stated under Article 6 paragraph 1 of EU Directive No. 95/46 which provides that personal data must be processed fairly and lawfully. Basically, it is a principle of transparency.

[3] Article 29 Working Party, Opinion 5/2009 on on-line social networking, adopted 12 June 2009, WP. 163.
[4] *Op. cit.*, p. 8.

From a practical point of view, it means that data controllers must inform fully and clearly individuals whose data are processed. As a result, this obligation is a core principle of Privacy and Data Protection legislation. It constitutes the necessary prior operation in order that individuals become aware not only that their data are processed but also that they have rights to oppose the processing or to access, to modify or to erase their data.

In order to make that clear, Article 10 of EU Directive imposes the duty on data controllers to inform data subjects of:

- the identity of the data controller and of his representative if any;

- the purposes for which the data are intended;

- the recipients or categories of recipients of the data;

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;

- the existence of their rights to access and to rectify the data concerning the data subject;

- the existence, if any, of a data transfer outside the EU.

In certain Member States, such as France, there are more detailed provisions regarding the information to be given to data subjects in cases of data transfers outside the EU, such as mentioning whether or not the transfer in question has been authorized on the grounds of a data transfer agreement previously approved by the CNIL.

If they were adopted in each EU Member States or provided under the draft EU Regulation currently under discussion, such additional obligations can have large consequences on cloud providers' business models.

Informing data subjects all these elements is of utmost importance for one thing. It is a prerequisite to a valid consent. It can indeed challenge the consent of data subjects to agree that their data are placed in one cloud system rather than to another.

Various types of cloud services agreements and business models

Cloud computing creates various levels of risks as regards to data protection. We have to think of a strategy so as to deal with these risks in a contractual manner. This strategy will change

according to the types of Cloud proposed by the providers. It also changes according to the economic relationship existing between the client and the provider, it means whether one is dominating the other or they are on an equal footing. This leads to make out two types of offers: standardized ones and negotiated ones.

Standardized offers

These types of offers cause several problems. A certain number of Cloud offers are set up through pre-formulated standard contracts. These contracts show a clear misbalance between the Cloud client and the cloud provider, in favour of the latter. No possibility of negotiation exists here.

But, nowadays, many of these pre-formulated contracts are criticized for their lack of transparency[5]. Especially, they do not always offer the possibility to identify clearly the own subcontractors of the cloud providers and, thus, where the servers and data will be located. Besides, the divide between the controllers and the processors is blurred. Indeed, Cloud clients rarely have the ability to give instructions to their providers and to check the compliance of how the processing is made.

What are the solutions? So as to rectify this contractual misbalance, Privacy and Data Protection authorities - notably the French CNIL and even the European Commission - advise to adopt contractual standard clauses elaborated in association with the stakeholders[6]. The goal here is to ensure the adoption of safe and fair contractual solutions for the individuals and for the SMEs in order to support Cloud client trust in cloud services. This standardization of the clauses would make the trade within the EU easier by allowing the provider to use the same patterns in every Member State, whereas the European Commission considers that the Cloud offer large business possibilities and has to take a great part into the strategy for the digital single market[7].

This is a perfect illustration of the politics of co-regulation and education promoted by some regulatory authorities as the French CNIL and the EU Commission[8]. Attention must be paid on the implementation of the different modes of regulation – and especially accountability – so as to promote some safe practices in the field of Cloud[9].

---

[5] N. Dubois & C. Hellendorff, *La protection des données et le cloud computing*, Rev. Lamy Droit de l'immatériel (Lamy ed., Paris) 2013, No. 98, p. 121, spec. p. 122.

[6] CNIL, *Recommendations to companies planning to use cloud computing services*, 25th June 2012 available at: www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf) - European Commission, *Unleashing the Potential of Cloud computing in Europe*, COM(2012) 529 final, 27 sept 2012 and, more specifically, *Cloud service level agreement on standardisation Guidelines*, 26 Jun 2014 available at: www.ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines – N. Dubois & C. Hellendorff, *La protection des données et le cloud computing*, op. cit, p. 124; B. Fauvarque-Cosson, *Cloud computing, protection des données personnelles et nouvelles pratiques contractuelles*, Rev. Les Petites Affiches (Lextenso ed., Paris), 18 August 14, p. 41; E. Sordet & R. Milchior, *La définition des contours juridiques du cloud computing*, Rev. Communication, commerce électronique (Lexisnexis ed., Paris), 2012, étude 18, spec. No. 4 - *Adde*, on the proposal of developments in the contractual framework: J-M. Sauvé, *Ouverture*, in *Le cloud computing, L'informatique en nuage*, SLC ed. (Paris), 2014, dir. B. Fauvarque-Cosson & C. Zolynski, p. 9, spec. p. 17.

[7] European Commission, *Unleashing the Potential of Cloud computing in Europe*, *op. cit.*

[8] I. Falque-Pierrotin, *Introduction*, in *Le cloud computing, L'informatique en nuage*, *op. cit.* p. 25 and M.-C. Roques-Bonnet, *Cloud computing: les actions de la CNIL démontrant un nouveau mode de régulation*, Rev. Lamy Droit de l'immatériel, 2013, No. 98, p. 126.

[9] *Cloud service level agreement on standardisation Guidelines*, *op. cit.*, p. 35.

Negotiated offers

Here, contract becomes a real tool to handle risks. It enables the Cloud clients to control their data[10]. It also invites Cloud providers to elaborate a "*tailor made*" offer for their clients. In this view, several points will have to be kept in mind:

- First, the way to contractually secure the qualification of the controller and processor, by setting up a clear separation of liabilities. Due to the risk that a Court reclassifies these situations, attention must be paid to the practices induced by the contract.

- Then must be considered the way to ensure the access to data, to increase the obligation of information, precising where and by whom the data is stored, and even how the user will be able to take part in the selection of the host.

- Same attention must be paid to the way to ensure the transparency of the Cloud provider's practices by providing audit clauses.

- At last but not least, specific precautions must be taken in order to secure the termination of the contract, by thinking especially of the fate of the data. This is the purpose of reversibility provisions: at the termination of the contract, the user is sure that he will have his data back, in an adapted format with guarantees of interoperability, avoiding thus any risk of restriction or absence of access. So that the Cloud client can avoid the service discontinuity and the risk to be technologically linked to the Cloud provider. Reversibility must be considered as essential: essential for the user, given the high economic value of the data; essential for the Cloud provider who on the one hand, must comfort his client and ensure the durability of his business model but who, on the other hand, also must protect his know-how when he transfer his data back (supposing the non-disclosure of his system of database management[11]).

So which system to choose?

Rather than adapting personal data to business model, why not doing the opposite? In fact, an offer adapted to the data must be provided. But not only the personal data is concerned: attention must be paid on every type of "*customer data*", every kind of strategic data of which the company wants to protect the value. One must find a fitting offer and think of the data which are about to be stored in the Cloud. So one need first to identify, then to handle the risks

[10] S. Albrieux, *Réflexions autour de la réversibilité et de la qualification du prestataire de cloud*, in *Le cloud computing, L'informatique en nuage*, *op. cit.*, p. 117 and G. Seligmann, *Big data et cloud computing: nouveaux risques, nouvelles réponses*, Rev. Expertises des systèmes de l'information (Celog ed., Paris), 2013, No. 384, interview.

[11] The cost of the recovering operation, which can be expensive, will have to be taken into account. It definitely is an essential point for the negotiation, since it is determining for the durability of the user's and the provider's business model – A. Cruquenaire & A. Cassart, *L'évolutivité des services de cloud: difficultés juridiques et solutions contractuelles,* Rev. Lamy Droit de l'immatériel (Lamy ed., Paris) 2013, No. 98, p. 108, spec. p. 111.

induced by the nature of the data. Such an approach is promoted by the French CNIL[12] who encourages the user to rate the legal, practical and technical obligations, so as to opt for the relevant offer[13].

According to the nature of the data, a large range of solutions is available:

- Public or hybrid Cloud for non-strategic data in order to make them accessible from everywhere ;

- Private Cloud or intranet for strategic data in order to limit the risk of losing control over data, notably when there are sensitive or subjected to specific rules such as bank data and accounting data[14]. Given that the legal obligations they are subjected to, some of this data will anyway prevent resorting to standardized cloud offers[15].

More generally, the choice of users who will be part of the operation and their localization will have to take into account the attention granted to data. The high geopolitical stakes of the Cloud must be reminded[16]. American providers' domination is facing the promotion of European actors, even if many can regret here the inability of Europe to create a champion in that field, contrary to other strategic fields as aeronautics.

This leads to encourage the achievement of "*risk study*", following the French CNIL and the Article 29 Working Group approach[17].

However, in many cases, Cloud clients will not have the power to negotiate the agreement with providers, or will not be able to combine the different computer infrastructure managing modes. But, this does not prevent them to compare Cloud providers' offers and, then, create some competition between them. These can be an effective way to adapt Cloud offers to Cloud client business models. Alternative which might ultimately be also taken into consideration by non-professional users with regard to the major risks they faced everyday with free Clouds whose financing is based on the re-use of the hosted data[18].

---

[12] CNIL, *Recommendations to companies planning to use cloud computing services*, *op. cit.* – M. Griguer, *Cloud computing and personal data protection: end of discussion?*, Cahiers du droit de l'entreprise (Lexisnexis ed, Paris) 2012, pratique No. 20.

[13] CNIL, *Recommendations to companies planning to use cloud computing services*, cit. –M. Griguer, *Cloud computing and personal data protection: end of discussion?*, *op. cit.*

[14] CNIL, *Recommendations to companies planning to use cloud computing services*, *op. cit.*

[15] CNIL, *Recommendations to companies planning to use cloud computing services*, *op. cit.* - Note the interest of resorting to several offers which permits not to be linked to a single provider to whom the whole data would be given.

[16] A.-S. Poggi & A. Lefèvre, *Les offres Cloud pour entreprises et protection des données à caractère personnel : les recommandations dont les entreprises doivent tenir compte lorsqu'elles choisissent une offre Cloud*, Rev. Lamy Droit de l'immatériel, 2014, No. 106, p. 44.

[17] B. Poidevin, *Le contenu du contrat de cloud computing*, Rev. Lamy Droit de l'immatériel, 2013, No. 98, p. 104.

[18] N. Dubois & C. Hellendorff, *La protection des données et le cloud computing*, *op. cit.* and M. Mossé, *Le nuage saisi par le droit*, in *Le cloud computing – L'informatique en nuage*, *op. cit.*, p. 131, spec. p.141-142 – *Adde*, in this regard, the proposal of P.-Y. Gautier in *Du contrat de depot dématérialisé : le cloud computing, La communication numérique - Un droit, des droits*, dir. B. Teyssié, Panthéon Assas ed. (Paris) 2012, p. 157, spec. N°19-20.