media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 6/2018

**SIMONE CEDROLA**[1]

# GDPR in the Cloud: who is who?

SUMMARY: 1. A brief introduction: what is Cloud Computing? – 2. Data protection in the Cloud. – 3. Conclusion.

## 1. *A brief introduction: what is Cloud Computing?*

Defining the Cloud is not an easy task, a good starting point would be to say that Cloud Computing is not something new. Surely it is a new expression and a new commercial reality, but what it really embraces in practice is the old vision of computing as a utility.[2]

This idea was publicly suggested by John McCarthy in 1961, who believed that computing power would have been sold through the utility business model, in other words like water or electricity.

[1] LL.M. Candidate, Law of Internet Technology, Bocconi University
[2] D. PARKHILL, *The Challenge of the Computer Utility*, Addison-Wesley Educational Publishers Inc., US, 1966

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

The problem was that the hardware, software and telecommunications technologies were not ready to embrace this innovation. But, once the technological means became more advanced, the old idea of computing as a utility came back stronger and under the name of Cloud Computing.

Behind the Cloud there are many interdisciplinary technologies, which are the reason for the difficulties in defining it.

One of the first, but not so complete, definition looks at the Cloud as «a standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way».[3] Although this definition includes both the service and business models, it ignores the deployment models.

However, the most accepted and standardized definition of Cloud Computing is the one by the National Institute of Standards and Technology (NIST): «Cloud Computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models».[4]

In recent times, another well formulated and commonly accepted definition has appeared: «Cloud Computing is a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user requirements».[5]

While the 90s had seen the downsizing of the hardware, that is the substitution of macro computers with mini or microcomputers, the early 2000s were characterized by the return of

[3] J. STATEN, T. SCHADLER, J.R. RYMER, C. WANG, «Q&A: by 2011, CIOs must answer the question, why not run in the Cloud?», *Technical Report, Forrester Research Inc.*, 2009, available here: https://www.forrester.com/report/QA+By+2011+CIOs+Must+Answer+The+Question+Why+Not+Run+In+The+Cloud/-/E-RES55193

[4] P. MELL, T. GRANCE, «The NIST definition of Cloud Computing», *Recommendations of the National Institute of Standards and Technology Special Publication*, National Institute of Standards and Technology, 800-145, 2011.

[5] C. MILLARD, *Cloud Computing Law*, 2013.

macro computers, capable of producing enormous computing power. In addition, the servers are virtualized, and this allows the user to take advantage of the computer's remote computing power.

In other words, in the Cloud Computing model, the user, an individual or a company, renounces the possession of their own hardware and software resources, and accesses the hardware infrastructure and software applications by purchasing them via the Internet, according to their needs.

In the Cloud Computing model, therefore, the idea of the transition from ownership to access rights takes place as an organizational and legal model capable of governing the use of resources in the digital age. Furthermore, this model is not valid only for digital content, but also for IT services and infrastructures.[6] As mentioned above, in the same way in which we take water from the water network, so we can take computing capacity and functionality from the internet.

The NIST also provides for a clear detection of the essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), service models (Software as a service, SaaS; Platform as a service, PaaS; Infrastructure as a service, IaaS), and deployment models (private Cloud, community Cloud, public Cloud, hybrid Cloud).

The interaction between all of these characteristics generates different Cloud models, with different risks.

[6] J. RIFKIN, *The age of access: how the shift from ownership to access is transforming modern life*, Penguin, 2000.

## 2. *Data protection in the Cloud*

The starting point of the main focus of this paper is to ask: why we should care about data protection in the Cloud?[7] The answer is simple, because people and businesses are using it. Individuals and business are using the Cloud a lot. The most common activity they do or provide is Storage space. And what they store is basically data.

Looking at the intersection between Cloud technologies and Privacy laws in the European sector we should be aware of the really near applicability, on May 25th, 2018, of the famous General Data Protection Regulation (hereinafter, GDPR),[8] before this there was the 1995 Data Protection Directive (hereinafter, the Directive).[9]

A general principle underpinning this Cloud – Data Protection relation is that the use of Cloud technologies should not increase the risks involved in the processing of personal data lowering the level of protection.[10]

These risks exist regardless of the service and deployment models, but they can often be more or less serious depending on them.

Firstly, one of the main problems concerns the physical location[11] of data that is not relevant to the service itself. However, the specific location where data is hosted is relevant to the application of national law. On the contrary, for the purpose of the service it is relevant from where data can be accessed.

---

[7] M. BIRNHACK AND N. ELKIN-KOREN, «Does law matter online? Empirical evidence on privacy law compliance», *Michigan Telecommunications and Technology Law Review*, 17, 2011.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=IT

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available here: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[10] European Data Protection Supervisor, Guidelines on the use of Cloud Computing services, March 2018

[11] W. KUAN HON, *Data localisation laws and policy*, 2017.

Secondly, we must take note of the big contractual asymmetry[12] between Cloud Providers and Cloud Clients. This, in fact, does not allow the Cloud Clients to behave as data controllers in compliance with the obligations envisaged for the processing of personal data. As we will see, this asymmetry also generates an unwanted allocation of responsibility in relation to the compliance with the Data protection law.

Thirdly, a problem of allocation of responsibility in the chain of responsibility also arises from the very nature of the Cloud service, which is a field of play where several players cooperate also from different part of the world. In particular, the assessment of requirements such as security and accessibility of data could be complicated precisely in relation to the number of players involved, to the location of these players and finally, in relation to the cross borders processing of personal data.

Lastly, we should be aware of the fact this technology is still developing, so it could be used and developed in so much ways that we cannot even imagine.[13]

Overall, due to the diversity of available Cloud Computing offerings, and in the absence of well-recognised legal and contractual standards covering all layers of Cloud Computing architecture, the data protection impact of each Cloud Computing service must currently be assessed on an ad hoc basis, in order to define the most appropriate safeguards that must be implemented.

2.1) *The allocation of responsibility: who is who?*

In the context of both the Directive and the GDPR we identify three main figures: the data controller, the data processor and the data subject.

The latter is the natural person to which a personal data relates to. According to art. 2 of the Directive a «controller shall mean the natural or legal person, public authority, agency or

[12] 16 STAN. TECH. L. REV. 81, 2012, available here: http://stlr.stanford.edu/pdf/Cloudcontracts.pdf
[13] Some of these issues are underlined in the Sopot Memorandum adopted on 2 April 2012 by the Berlin International Working Group on Data Protection in Telecommunications.

any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law», while a «processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller».

As said above, the identification of the data controller and data processor in relation to the Cloud Computing environment is essential to the applicability of the data protection law.

In this regard, the two main roles in Cloud Computing are Cloud client and Cloud service provider. The Article 29 Working Party (WP29) stated that «the Cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. He should therefore be considered as a data controller».[14] In addition, the Cloud client, as controller, has to comply with the responsibilities set out in the data protection legislation.

The Cloud provider, according to the WP29 «is the entity that provides the Cloud Computing services in the various forms discussed above. When the Cloud provider supplies the means and the platform, acting on behalf of the Cloud client, the Cloud provider is considered as a data processor».[15]

Although these roles appear to be well defined, it should be noted that often it can be very hard to determine if the service provider is the processor or the controller. That is because for an individual is basically impossible to determine the purpose and means[16] of the processing of its data.

In Cloud databases information and personal data are stored and transferred in different centre and the Cloud client has no control over "the means" of the processing.

[14] WP 29 Opinion 05/2012 on Cloud Computing, adopted July 1st 2012.
[15] Vd. supra.
[16] Art. 2, n.1, Data Protection Directive; art 4(7), n. 14, and art. 28(10), GDPR.

There could be also the case in which the Cloud service provider is the data controller i.e. when the Cloud service is free, and the provider collect data to target advertising.

Given that, it is clear that there is not a single and unique way to look at "who is who", but rather there should be a case by case evaluation.[17]

The key point is that the Cloud client, the weakest party, should take appropriate safeguards through the contractual activity. However, as said above the common practice is to have contractual standardisation and therefore the Cloud client has no or very little leeway to modify the technical or contractual means of the service.

On this, the WP29 stated that «the imbalance in the contractual power of a small controller with respect to large service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law».[18] Therefore, the controller must choose a Cloud provider that guarantees compliance with data protection legislation.

However, we should also take into account what has been already assessed i.e. the technological complexity behind Cloud Computing, that is growing year after year, and it makes no longer possible for the Cloud client/data controller to be the only one determining the «purpose and the means» of the processing.

In reality, the Cloud service provider is the one who designs, maintains and operates the infrastructure, be it IaaS, PaaS or SaaS, defining the basic elements of the means, so these characteristics are not in the hands of the Cloud client.

The current, or better, quasi-outdated regime under the Directive obliges the data processors, in this case, the Cloud provides, to comply with just few direct responsibilities mainly related to the security of the processing.[19]

---

[17] P. HUSTINX, «European Data Protection Supervisor, Data protection and Cloud Computing under EU law», *Third European Cyber Security Awareness Day, European Parliament*, 13 April 2010, available at http://www.edps.europa.eu

[18] Vd. n. 13

[19] Artt. 16 and 17, Data Protection Directive.

On this, the WP29 «recognises the difficulties in applying the definitions in a complex environment where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility».[20] In addition, the WP29 stressed the need to «allocate responsibility between controller and processor in such a way that compliance with data protection rules will be sufficiently ensured in practice».[21]

However, with the massive changes provided by the GDPR,[22] specific responsibilities are placed on data processor. The strongest players in the Cloud Computing field, the Cloud providers will now face a radical change of position due to a much stricter liability regime, that could lead also to a direct action by the authority, and due to the huge fines for non-compliance.[23]

In particular, under the GDPR the Cloud service providers are required to «maintain a record of processing activities»,[24] «implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk»,[25] «carry out an assessment of the impact of the envisaged processing operations on the protestino of personal data»,[26] comply with the rules on international data transfers,[27] and cooperate with the national supervisory authority.[28]

The art. 28 of the GDPR is one the most important provisions that will have a strong impact on Cloud Computing technology. This disposition contains the obligatory contractual terms between processor and controller. It has and it likely will have a key role in the partial shift of responsibility from the controller to the processor.

---

[20] WP 29 Opinion 1/2010 on the concepts of 'controller' and 'processor', adopted on 16 February 2010
[21] Vd. supra.
[22] M. WEBBER, «The GDPR's impact on the cloud service provider as processor», *Privacy & Data Protection*, 16, issue 4.
[23] M. MAGGIORE, «Cloud computing: obligations under the Directive v. GDPR», *Data Protection Law & Policy*, June 2016.
[24] Art. 30, n. 14, GDPR.
[25] *Id.*, art 32.
[26] *Id.*, art 37.
[27] *Id.*, art 44.
[28] *Id.*, art 31.

The contract will therefore govern the relation with the Cloud client, and in particular, will define «the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller».[29]

Despite these positive signals of changing the paradigm, the GDPR still embraces the regime of the Directive i.e. controllers are responsible for the acts of processors. In fact, the processor will be treated as controller every time he takes its own decisions about the processing of data. In this case the processor will be held responsible as a controller in respect of that processing activity.[30]

This provision turns out to be excluded in the context of an IaaS Cloud service providers, because the processing activity is carried out by the controller using only the provider's resource, without the latter having any knowledge of which kind of processing is in place.[31]

These new principles and provisions "against" the Cloud service providers have been harshly criticised as burdensome, especially in the context of the IaaS and PaaS due to the broad definition of personal data that makes the Cloud provider fall within the area of the GDPR, even if the processors only provide for the resources and barely have knowledge of the processing activity.[32]

[29] *Id*., art 28 (3).
[30] Art. 28, n. 14, GDPR
[31] K. HON, J. HORNLE, C. MILLARD, «Data Protection Jurisdiction and Cloud Computing: When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing», *International Review of Law, Computers & Technology*, Part 3 26(2-3), 129, 152, 2012.
[32] K. HON, «GDPR: Killing Cloud Quickly?», 2016, available: https://iapp.org/news/a/gdpr-killing-Cloud-quickly/

3. *Conclusion*

In conclusion, to the natural and underlying technical complexity of the infrastructures of the Cloud, the law replies identifying the cases and the conditions upon which a Cloud service provider could be qualified as the data controller.

In other words, sometimes processors can now be directly liable and be obliged to indemnify the data subject.

Although such a change was needed, the GDPR does not provide for a clear discipline with the regard to those Cloud providers, such as IaaS and PaaS, which do not have knowledge of the nature of the data stored and of the means of the processing, and they also lack the possibility to access these data.

Answering the question "who is who?" is essential, especially now that both controller and processor will be subject to the severe administrative fines, up to a maximum of 20 millions of Euro or 4% of the total worldwide turnover[33]. In addition, it is really important, and it will mean a lot for the future of Cloud Computing the fact that processor will now be directly liable to the data they process outside the scope of the relation within the data controller.

The GDPR was necessary to let Europe compete within a fair and regulated framework in the global data economy. The practical consequence is that data protection standard will grow both in Europe and outside Europe, and so it will soon become the number one, or two, element to be taken into consideration when choosing a Cloud provider. Who will better ensure a just contractual agreement with the Cloud client and a high level of data protection without losing the quality of the service will have a good piece of the market.

[33] Art. 83, GDPR.