

Panel IV: Privacy and Cloud Computing

“Data Protection and Cloud Computing under EU law”

Peter Hustinx

European Data Protection Supervisor

Earlier today we have heard about the benefits and opportunities of cloud computing. We have also heard that cloud computing brings along certain challenges, notably to ensure the security of information and safeguard the personal data and privacy of individuals.

This is very relevant because cloud computing services nowadays store and process personal data of individuals, as governments or companies make use of cloud services, or individuals store their own data in the context of email, social networks or otherwise. There are also health related services that allow people to upload their medical records to the cloud and share information with doctors.

In this context, a key question is whether the current legal framework provides for appropriate safeguards to ensure the protection of individuals' personal data.

Current legal framework

The Data Protection Directive 95/46 is most relevant in this context. It sets obligations which are binding upon all those who process personal data. It therefore applies to cloud services where they process personal data that fall within the scope of EU jurisdiction. If this is the case, the Directive applies regardless of where the data are processed.

Let me give two examples of how the Directive applies to cloud services, providing for effective protection of individuals' personal data.

- ***Security obligations:*** Article 17 of the Directive imposes the obligation upon data controllers and processors to apply technical and organizational measures to protect data against accidental or unlawful destruction, loss, disclosure, and other forms of unlawful processing. Cloud computing services are in principle bound by this obligation and must put in place 'state of the art' technical and organizational measures to avoid personal data from being compromised.
- ***Purpose limitation.*** Article 6 of the Directive requires data controllers to process personal data for purposes compatible with those for which it was initially collected. In the context of cloud computing this should deter controllers from using information for incompatible purposes. A service consisting in providing storage of medical records could not use such information for other purposes.

All of this is backed up with supervision and sanctions that may be imposed upon those who fail to comply. So, in principle, we have laws in the EU that provide for safeguards to protect individuals' personal information and privacy, also in case of cloud computing.

However, things are not so simple. Although the principles of the data protection legal framework are applicable, there are some challenges when trying to apply them in practice. This is because of technological developments and new global realities, which were not accounted for when the Directive was adopted.

First challenge: which role do cloud computing providers play?

The Directive puts most of its obligations on the entities that process data as data controllers. Some, but fewer obligations are imposed on data processors, entities that are 'entrusted' by controllers to process data.

In many cases, one can probably argue that cloud providers are data processors. However, in practice, cloud computing services very often not only determine the means, but also to some extent the purposes of the processing, in which case they would be data controllers.

Which role is played by cloud computing providers will need to be determined on a case by case basis, in view of the nature of the cloud services. Some guidance from data protection authorities, particularly from the Article 29 Working Party, would be very helpful in this context. Therefore, I welcome the recent decision of the Working Party to put this subject on its agenda¹.

In my view, even when cloud providers play a mere "processing" role, they will have to engage in a very close cooperation with their clients to ensure that controllers are in a position to fulfil their data protection obligations.

Second challenge: determine whether EU law applies

This is important because the benefits of EU data protection law are relevant only if such law applies.

This is the case (a) if the data controller has a relevant establishment in the EU and (b) if it uses equipment in the EU. Thus:

- A cloud provider established in the EU - or acting as processor for a controller established in the EU - will in principle be 'caught' by EU law.
- A cloud provider which uses equipment (such as servers) in an EU Member State - or acting as processor for a controller using such equipment - will also be caught.
- A cloud provider in other cases - even if it mainly and mostly targets European citizens - would not be caught by EU law.

As this problem is not specific for cloud computing, but much broader, there may be a need to address it in a more comprehensive way. The Data Protection Directive is in

¹ Article 29 Working Party Work Programme 2010-2011, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010_en.htm

the process of being reviewed. In this context, I could imagine amendments to the Directive's provisions on applicable law to ensure that situations as just described do not escape the application of EU law. For example, an additional criterion based on targeting of EU citizens may be considered.

Third challenge: international data transfers

The Directive prohibits transfers of personal data to countries which do not ensure an adequate level of protection. Unless an exception applies, the data controller must adduce adequate safeguards for the protection of personal data: for example, enter into a contract with the recipient of the data ensuring that the data will remain adequately protected.

The problem is that these rules rely on a definition of data transfer from 'point to point'. They require having a contract, and sometimes a notification to the authority for each transfer to a country where the legal framework is not adequate. In practice this is very difficult to implement, particularly in cloud computing that entails the continuous transfer of personal data.

As it happens with the question of applicable law, this challenge is not unique for cloud computing, although cloud computing makes it more acute.

In my view, the solution should also be found in the context of the review of the Directive, in particular in the rules on international transfers. For example, streamlining the rules on BCR or introducing an extended responsibility for controllers with respect to data transfers.

Fourth challenge: ensuring more effective data protection

At this point, I also want to point at a general challenge, in the context of the review of the Directive, i.e. ensuring more *effective* data protection in *practice*, which applies to *all* controllers and processors, particularly those operating in a technologically advanced environment. For this purpose, the Article 29 Working Party has recently

proposed including the principles of 'Accountability' and 'Privacy by Design' in the EU legal framework of data protection².

In the context of cloud computing services, this means that controllers and processors would have to demonstrate that they have taken all the necessary measures to ensure that data protection rules and principles are complied with. This approach would also be very interesting where personal data are entrusted to providers in third countries.

Fifth challenge: processing data for purely personal purposes

A fifth and last challenge refers to cloud computing services provided to end users who use them for purely personal purposes.

We see a tendency to offer cloud computing services to individuals as end users. For example, the cloud is moving data from local desktops to equipment that is remotely accessible and considered as located in the cloud, controlled by third parties. Similar services would be the storage of pictures, calendars, typically the type of information that one would keep at home and use for personal purposes.

In this situation, there is at least some ambiguity whether the cloud provider would be covered by the EU data protection framework, and hence whether individuals' data would be properly protected.

This concern, which was highlighted by the Article 29 Working Party³, is based on the wording of Article 3 of the Data Protection Directive. This article excludes from the scope of application of the Directive data processing carried out "by natural persons in the course of a purely personal or household activity" (the 'household exception'). If the information uploaded to the cloud is not covered by the Directive because it is information of a personal nature, then the processing activities that are carried out on behalf of the individuals involved might not be covered either.

² See Article 29 Working Party Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1st December 2009.

³ See Article 29 Working Party Opinion 168 on The Future of Privacy, mentioned in footnote 2

Obviously, many cloud providing services, even when they cater to end users, will be covered by the existing EU data protection legal framework. However, in other situations, the legal framework may not apply. This problem would also arise to any processing service, carried out on behalf of end users acting in their 'personal capacity'.

In my view, in the context of the review of the data protection Directive, it is necessary to consider a way to fill this gap. The Directive might, for instance, explicitly require that services provided to individuals acting in a purely personal capacity, are bound by the same requirements as 'regular data processors'.

Conclusions

The principles of EU law remain relevant and fully applicable to the provision of cloud computing services. However, there are some important challenges in the way such principles apply. Such challenges are not specific for cloud computing, but it makes them more serious.

To meet these challenges, it may be necessary to use several solutions, which should not be specific for cloud computing but more general.

First, we need interpretation and guidance. The WP29 initiative to describe how to apply the existing laws and principles to cloud computing is welcome.

Second, we need some legislative changes aiming at fixing the identified problems while keeping the main principles unchanged. Particularly, four areas may require amendments:

- *Applicable law*, including a new criterion such as targeting.

- *International data transfers*, including streamlining the use of BCR and possibly extending the responsibility of controllers.

- **Accountability and 'privacy by design'** would give strong incentives to ensure that cloud computing services are privacy friendly, and if necessary even with some 'privacy by default'.

- Last but not least, the need to impose **'processor' obligations** where **services are provided to individuals** acting in a purely personal capacity.