Cloud computing – A new paradigm

The newly developed trend in the field of information technologies – cloud computing – has quickly become popular among consumers as well as international companies. Although cloud computing is considered as a big step forward, some concerns do arise particularly with regard to privacy and data protection. Therefore, the International Working Group on Data Protection in Telecommunications has prepared the Working Paper on Cloud Computing – Privacy and Data Protection Issues, into which Squire Sanders provides insight.

What is cloud computing?

There is no uniform and widely accepted definition of cloud computing, not only due to the fact that no international agreement on common terminology has been concluded yet, but also because the technology of cloud computing is still developing. According to the National Institute of Standards and Technology`s definition, 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."[1] To put it more simply, cloud computing is a model for delivering information technology services in which resources are retrieved from the Internet through web-based tools and applications, rather than a direct connection to a server.

Advantages of cloud computing

Cloud computing offers multiple advantages for enterprises of all sizes. One major advantage is its flexibility as staff can access files and data that they need even when they are working remotely. It also enables collaborative work on files and documents even when the staff are not physically together.

Cloud computing is considered cheaper and enables companies to cut costs, which nowadays seems to be paramount in doing business. There is no need to buy and install expensive software because it's already installed online remotely and accessible to users via an internet web browser. Cloud technology is paid incrementally, saving companies money as they pay only for what they need and when they need it.

In addition, there is no need to take on specialist IT staff, and companies don't have to worry about maintaining and upgrading software or fixing any potential bugs, as all maintenance is done by the cloud service providers.

Using cloud computing offers virtually unlimited storage compared to server and hard drive limits. For more storage space no server upgrades are necessary as the data is stored remotely and virtually and thus the storage space can be easily scaled up and down according to demand. It also saves the energy lost through server underutilization.

Risks of cloud computing

The global and trans-border nature of cloud computing, the enormous amounts of accumulated data, the lack of transparency in data processing in cloud computing, the lack of an international legal framework with respect to cloud computing, and the great pressure for quick capitalization of investment costs under which the cloud service providers are operating might lead to substantial risks with regard to personal data protection. Such risks might include breaches of information security, transfer of data to jurisdictions not providing adequate data protection, violation of laws on and principles of privacy and data protection, and cloud service providers or their subcontractors using the controllers' data at variance with the data controllers' instructions or even for their own purposes, etc. This might result, among other things, in relevant data protection authorities not being able to supervise the processing of personal data and the data subjects not being able to claim their rights stipulated by both the European legislation and respective national laws, or in other words – in intrusion into privacy of individuals.

International Working Group on Data Protection in Telecommunications

The International Working Group on Data Protection in Telecommunications was founded in 1983 in order to improve privacy and data protection in telecommunications and media (the "Working Group"). Since then, the Working Group has adopted numerous recommendations, among others the recent Working Paper on Cloud Computing (the "Working Paper")[2], with the aim to "reduce risks associated with the use of cloud computing services and to promote accountability and proper governance". Even though the recommendations of the Working Group are not binding, they often inspire other data protection authorities such as the Article 29 Working Party.

Recommendations of the Working Group

The Working Group prepared a non-exhaustive list of recommendations for cloud service providers, legislators and users of cloud computing services. The Working Group recognizes the benefits of cloud computing; however in its opinion, these benefits cannot be at the expense of the rights of individuals.

The Working Paper includes the following general recommendations:

- Utilization of cloud computing cannot lead to lowering of data protection standards as compared to conventional data processing;
- Prior to embarking on cloud computing projects, the data controllers should carry out the necessary privacy impact and risk assessments;
- Cloud computing service providers should further develop their practices in order to offer greater transparency, security and accountability and more balanced contractual clauses to promote data portability and data control by users;
- Legislators should reassess the adequacy of the existing legal

in data processing

SQUIRE SANDERS

framework allowing cross-border transfer of data and consider additional necessary privacy safeguards in the era of cloud computing;
- National Data Protection Authorities should continue to cooperate with data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues.

The Working Paper also provides additional guidance on best practices for data controllers and cloud service providers. These are aimed in particular at ensuring that (i) the data controller has full information on where the data processed by the cloud service provider (or its subcontractor) is physically stored; (ii) neither the cloud service provider (nor its subcontractors) transfers the data to locations not previously agreed on with the data controller; (iii) the cloud service provider may not use the data controller's data for its own purposes; (iv) in the case of data breach the data controller is at all times able to fulfill its obligations towards the data subject and respective data protection authorities and take appropriate actions. The additional guidance also calls for establishing of location audit trails and audit trails that automatically record copying and deletions available to data controllers with respect to their stored data.

The New Data Protection Framework for Europe

Some of the recommendations made by the Working Paper are already covered in the European Commission's proposal for a comprehensive reform of European Union data protection rules (the "Proposal")[3] announced at the beginning of this year. The new regulation attempts not only to protect rights of individuals to data protection but also to reflect rapid technological developments and boost European economic development by building trust in the online environment.

These are the terms that one should remember with respect to the Proposal:
- Harmonization. A single data protection regulation throughout the European Union ("EU") should be introduced to eliminate the differences between the national laws of EU Member States that currently cause difficulties to companies operating in more than one EU Member State.
- Single Point of Contact. A data controller processing personal data in more EU Member States will be regulated by the data protection authority in the EU Member State in which the company has its main establishment.
- Reaching out. The new data protection rules should also apply to companies not established in the EU, if they process personal data related to EU citizens and even to non-EU citizens residing in the EU, provided that the processing activities relate to offering of goods and services in the EU or to monitoring of behavior of these data subjects.
- Reporting. An obligation is imposed on the data controllers to notify the relevant data protection authority of data breaches without undue delay and, where feasible, no later than 24 hours after becoming aware of it.
- Forgetting. Data controllers should be obliged to delete all of an individual's personal data when there are no legitimate grounds to retain it.
- Portability. The data subjects should be given the right to obtain a copy of processed data, if processed by electronic means and in a structured and commonly used format and in some cases also to transmit such data to another data controller without hindrance.
- Explicitness. Explicit consents with personal data processing should be required. Moreover explicit parental consent should be given when data of a child under the age of 13 is processed.
- Sanction. The violation of certain data protection rules stipulated in the Proposal might result in a sanction of up to €1 million or up to 2% of the company's global annual turnover.

The Law Still Lagging Behind the Paradigm Shift in Technology

The fact is that cloud computing is becoming one of the future phenomena of the European online environment and there is no doubt that the current European data protection regulation (the "Current Regulation")[4] does not take into account all the unique aspects of cloud computing, and even the Proposal, which attempts to reflect rapid technological developments, does not make it as easy for cloud service providers as it could.

For instance, the Proposal did not in any way change the legal position of cloud service providers. It does not take into account their unique standing as some "virtual data storekeepers" and continues to squeeze them into the definitions of either data controllers or data processors and imposes related obligations on them.

Another major issue of the Current Regulation with respect to cloud computing is the definition of personal data, which makes a substantial portion of data stored in the clouds personal and thus falling within the scope of the data protection regime. The Proposal does not introduce any substantial change in this regard.

On the other hand, European cloud service providers and users will surely benefit from the single supervising authority and unified data protection rules. It is not clear, however, whether non-European users and cloud service providers will consider falling within the scope of the European data protection regime as envisaged by the Proposal as a "benefit".

In the wording of the Proposal there are even more examples of it being not "cloud-friendly". Yet, one has to keep in mind that the main aim of the Proposal is to protect the fundamental right of individuals to protection of their personal data and thus it does not come as a big surprise that its overall approach to the cloud service providers is still more of a "carrot and stick" one. The Proposal does not solve all the issues and loopholes in the Current Regulation with respect to cloud computing, which makes the Working Paper a good lead for European legislators in its ongoing adoption procedure.

JUDr. Jana Pagáčová
Partner, Squire Sanders

Peter Devínsky
Associate, Squire Sanders

1 National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 2.
2 Cloud Computing – Privacy and data protection issues – "Sopot Memorandum" (Sopot (Poland), 23./24. April 2012).
3 Proposal for a Regulation of the European Parliament and of the Council on protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final.
4 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.