CLOUD COMPUTING:
GUIDELINES FOR A KNOWLEDGEABLE USE

Italian Data Protection Authority – June 2011

Table of Contents

1. Foreword

With a view to fostering the appropriate use of new mechanisms for the provision of IT services that entail the outsourcing of data and records, in particular those relying on public clouds, the Italian DPA considers it both desirable and necessary to raise public awareness so as to protect the informational value of personal data.

The guidelines below are meant accordingly to provide initial guidance for all small-sized users with limited economic resources – such as individuals, SMEs, small local authorities, etc. – that are increasingly targeted by the offer of cloud computing services; they are aimed ultimately at fostering the knowledge-based, fully accountable endorsement of cloud-based services.

The precautions that are highlighted in the following paragraphs make up an initial set of safeguards to foster the appropriate processing of personal data via the services in question; as such, they are also addressed to providers, who may want to rely on them in building up the respective services whilst informing users as necessary of the implementation of cloud technologies.

The Italian DPA is well aware that cloud computing raises issues that can hardly be coped with at exclusively national level as they require careful analysis in both European and international forums. This is why the DPA will continue monitoring the evolution of cloud computing, partly because of its manifold impact on the processing of personal data, and also contribute with other institutional decision-makers to the ongoing discussions in specific forums such as the one created by DigitPA [the Italian public body in charge of IT issues in public administrative services] with regard to the implementation of cloud-oriented models in the public sector. Furthermore, the Italian DPA may decide to adopt specific, detailed guidelines for users and providers if this is found to be necessary, especially in connection with the relevant security measures.

2. What Is Cloud Computing?

IT and communication technologies develop uninterruptedly and new, increasingly sophisticated tools and solutions become available daily that rely on the Internet so as to meet the growing demand for computerization and communication.

Against this backdrop, cloud computing can be defined as a set of service models that are becoming popular at a faster pace than other models in both the private and the public sector as well as among citizens at large; this is due to their emphasis on a flexible use of one's own resources (including infrastructures and applications) and/or the resources made available by a specialized service provider. The innovation and success potential of cloud computing results from the fact that the resources in question can be configured and accessed on the Net quite easily, thanks to the advanced maturity of the underlying technologies, and their use proves also quite simple. On the one hand, this makes it significantly simpler to decide on the initial dimensioning of systems and applications; on the other hand, the investments required for upgrading technologies and providing new services can be borne via incremental efforts.

It is by now standard practice to distinguish between "private cloud" and "public cloud" services.

"Private cloud" means an IT infrastructure that is mostly dedicated to an individual organization; it is located at the organization's premises or else its management is outsourced to a third party (usually via server hosting) that is under the data controller's strict authority. A private cloud can be compared to a conventional data centre – 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.

Conversely, a "public cloud" is an infrastructure owned by a provider specializing in the supply of services who makes available – and therefore shares – his systems to/among users, businesses and/or public administrative bodies via the web-based delivery of IT applications, processing capabilities, and memory space. The services can be accessed via the Internet, which entails transferring data processing operations and/or the data as such to the service provider's

systems; thus, the service provider takes on a key role as regards 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. For instance, complexity of the infrastructures and their being located outside national borders might make it impossible both to pinpoint one's own data in the cloud and to know whether and when such data is moved elsewhere on account of organizational, technical and/or economic reasons that are difficult to gauge and manage beforehand. Furthermore, the provider's corporate size might impact on the contractual power of its customers as well as on their actual capability to control – albeit on the basis of an agreement – the sites and facilities where the respective data are hosted.

The acquisition of cloud-based services entails purchasing resources (e.g. virtual servers, disk space) or applications (e.g. email, office tools) from a service provider. - Data is no longer resident on the user's "physical" servers as it is allocated to the provider's systems (apart from local copies); - The service provider's infrastructure is shared among several users, accordingly suitable security measures are fundamental; - Services are accessed via the Internet, which therefore plays a key role as for the quality of the services in question; - The services available from the provider are usually delivered on a consumption basis, which makes it easy to cope with increases in demand (e.g. if additional disk space or processing capability are necessary); - Outsourcing one's own data remotely is not the same as keeping such data on one's own systems; there are both advantages and disadvantages to be considered.

Table: Key features of "public clouds"

Alongside "public" and "private" clouds, there are so-called "intermediate" or "hybrid" clouds where services provided by private infrastructures co-exist with services purchased from public clouds. Reference should also be made to the "community clouds", where the IT infrastructure is shared by several organizations for the benefit of a specific user community.

The potential benefits of cloud computing can unquestionably foster systematization of infrastructures along with the re-organization of information flows and increased cost-effectiveness; in short, they may help bring about modern, more efficient, workable services for both businesses and public administration in what is expected to be a modern country. On the other hand, there is little doubt that cloud computing is no fleeting or fashionable faze; in fact, it is the next step in the evolution of Internet use – which is becoming a portal to access the processing resources made available by a service provider (i.e. the applications made available in web mode) rather than being merely a tool to share documents (such as the web page made available on a remote website).

This evolution is leading to a "change of habits" that is ongoing and is especially remarkable in respect of individual users, who more frequently rely on services provided by third parties (public cloud) to meet their informational requirements – at times without being fully aware of the possible risks. Consumers use social networks to post pictures, information, ideas, and opinions; they use web-based text processing tools; they rely on remote hard disks to access their documents and files at any time, from any place, and by any means; they resort to Internet smartphone applications, which are paving the way to innovative functions (including community functions) by matching user-related geolocation information.

On the other hand, it is unquestionable that much pressure is being put by market operators on businesses and public administration in order for them to purchase outsourced services – leveraging on the prospective savings that may be achieved by relying on third-party usage-based solutions in the place of and/or alongside conventional user-owned data processing assets.

It should be pointed out, however, that resorting to systems that rely by their very nature on the increased use of outsourced services entails data migration from the local systems – placed

under the user's/company's/administrative body's direct control – to the remote systems made available by the service provider.

3. Data Outsourcing to Public Clouds

It was said in the above paragraphs that a public cloud is an infrastructure controlled by an organization that makes it available to third parties by selling usage-based services. A cloud's virtual space and processing capability are shared among several users (including corporate and non-corporate entities), who can access those resources by way of the Internet.

In this paper, cloud computing (or cloud) means a set of technologies and service models that

- Focus on the web-based use and delivery of IT applications, processing capability, and memory space; and
- Focus on the shift of data processing (or data storage, depending on the specific configuration) from the user's computer(s) to the service provider's systems.

Flexibility and simplicity in configuring cloud systems allow their "elastic" dimensioning, i.e. these systems can be adjusted to the specific requirements in accordance with a usage-based approach. Users do not have to manage any IT systems, which are relied upon on the basis of outsourcing agreements and therefore are handled in full by the third party in whose cloud the data are stored. It is often the case that large-sized providers with complex infrastructures come into play; this is why the cloud might span several locations and users might ignore where exactly their data are being stored.

There is a wide gamut of services offered by cloud computing providers; significantly, the number of such services keeps increasing and ranges from virtual processing systems (which replace and/or work alongside the conventional servers located at one's premises) to services supporting application development and advanced hosting – up to web-based software solutions that can replace the applications conventionally installed on a user's PC including text processing applications, agendas and calendars, filing systems for online document storage, and even outsourced email solutions. Any data that is transferred to and stored by a service provider via these web-based systems can be processed by users remotely through the Internet – often without having to install specific software on their systems and/or perform software upgrades and all the other activities related to maintenance and management of IT infrastructures.

4. Different Service Models

Depending on user requirements, there are several cloud computing solutions available on the market; they can be grouped into three main categories or "service models". These models usually apply to both private and public cloud solutions; however, they will be described below mainly from the standpoint of public cloud solutions, which envisage the shared use of the systems made available by third-party service providers.

- IaaS (Cloud Infrastructure as a Service): a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. Such providers are usually specialized market players and can rely actually on a physical, complex infrastructure that often spans over several geographic areas.
- SaaS (Cloud Software as a Service): a 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, etc.; however, the services in question also include cloud-based email applications.

- PaaS (Cloud Platform as a Service): a 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. Again, the services delivered by a PaaS provider make it unnecessary for the user to rely on additional and/or specific hardware or software at internal level.

5. Innovative Solutions and Risk Governance

Cloud computing services are being relied upon to an ever-increasing extent, which is bringing about a pattern change in the use of the Internet. Rather than being a tool for sharing documents, the Internet is becoming a portal to access processing and memory resources owned by remote service providers.

Cloud-based services entail migration of data from local systems – under the user's direct control – to the provider's remote systems; accordingly, the provider's role becomes crucial as for ensuring data security by taking the necessary measures. Still, it should be pointed out that the fact of relying on outsourced services does not exempt business and/or governmental entities from the liability and obligations vested in them pursuant to, in particular, personal data protection legislation.

When processing personal data one should always carefully assess the risks related to data security and availability – irrespective of the specific processing arrangements. Thus, account should be taken of the features applying to any new technology in order to enable the governance of such dangers as may arise from ill-advised usage and/or the implementation of innovative models in the absence of commonly received methods, practices and processes to mitigate criticalities. Regarding Cloud Computing, one should take stock of the specific peculiarities so as to detect any risks inherent in cloud-based services and take effective, specific counter-measures.

Transferring data from local computers – where they are physically available to and directly controlled by the data controller – to remote systems owned by a third-party service provider is fraught with the following criticalities that should be considered carefully alongside the potential benefits deriving from the use of cloud computing:

- By committing their data to the systems owned by a remote provider, users are no longer in exclusive control of such data; confidentiality and availability of information in a cloud depend unquestionably on the security arrangements implemented by the service provider as well;
- The service selected by the user might be the end-product of a transformation chain of services purchased from service providers other than the one with whom the user has entered into an outsourcing agreement; users might not always be in a position to know who may access what data out of the chain of intermediate service providers, especially if the chain is made up of several links;
- Failing appropriate connectivity safeguards, the virtual services might happen to be degraded during traffic peaks or might prove unavailable if, for instance, failures occur; this would make the data handled by those services temporarily non-accessible;
- A cloud is made up of shared systems and infrastructures and is grounded in the concept of leasing resources to multiple as well as multifarious users; providers keep data related to different individuals and organisations, which might pursue different or even conflicting interests and objectives;
- Keeping data in different geographic locations impacts directly both on the law applicable to any disputes between user and provider and on the national legislation regulating processing, storage and security of the data;
- If the service provider relies on proprietary technology it may prove difficult for a user to shift data and documents between different cloud-based systems or to exchange

information with entities that use cloud services managed by different providers; this might endanger data portability and/or interoperability.

Based on the services it offers, a provider takes up responsibility for preserving confidentiality, integrity and/or availability of the data at issue; when entering into a service outsourcing agreement, users should take due account accordingly of the arrangements envisaged by the provider to ensure that any data is processed appropriately in the cloud.

Thus, prior to resorting to a cloud-computing system one should carefully assess the risk-benefit ratio related to the use of such a system; risks can be minimized by carefully verifying reliability of the prospective service provider.

6. Guidelines for a Knowledgeable Use of Cloud-Based Services

- *Firstly, assess risks and benefits*

Before opting for the implementation of cloud-based services, a user should check amount and type of the data to be outsourced - e.g. whether the data include personally identifiable information, sensitive data or high-profile data like genetic or biometric information, or key data for one's business such as confidential project-related data. One should assess in the first place what risks and possible consequences may arise from selecting the cloud option in terms of confidentiality and impact on one's activities. This assessment should ultimately clarify whether it is appropriate to rely on cloud-based services – for instance, only certain types of data might be processed via these services – and what impact such services will have in terms of costs and organizational arrangements for the user - for instance, taking account of the risk that the outsourced data may be unavailable, even if only in part or for a short time, or else get lost or deleted.

- *Check cloud provider's reliability*

Users should reasonably establish how reliable a cloud provider is before migrating their key data to virtual systems; to that end, account should be taken of institutional/business requirements, amount and type of the information to be processed in the cloud along with the attending risks and security measures. Users should assess the provider's financial stability, his references and the guarantees afforded in terms of data confidentiality as well as the measures in place to ensure operational continuity in case of unforeseen failures; this assessment should be performed in the light both of the type of service to be provided and of the criticalities related to the data at issue. Users should also consider the quality features applying to the connectivity services relied upon by the provider in terms of their capability and reliability. Additional criteria to assess a provider's reliability consist in employment of qualified staff, adequacy of the IT and communication infrastructure, and acceptance of liability – as expressly set forth in the outsourcing contract – for security loopholes and/or service breakdowns.

- *Preferably choose services that are big on data portability*

Regardless of whether cloud computing services are relied upon in SaaS, PaaS or IaaS mode, a forward-looking approach should be implemented by preferably choosing services that are based on open formats and standards such as to facilitate migration between different cloud systems possibly managed by different providers. This will prevent unilateral changes to the outsourcing contract by any one of the entities in the supply chain from translating into less favourable contractual obligations and will facilitate, at all events, any subsequent change of provider.

- *Make sure the data are available whenever necessary*

If no stringent Quality-of-Service terms are set forth in the contract with the provider, it is recommended that a copy be kept of any data (whether personal or not) whose loss and/or unavailability might be harmful economically, in terms of image and/or – generally speaking – in respect of the user's mission and objectives. This is especially appropriate if free-of-charge

or low-cost services are relied upon such as remote hard disk services, mail services, document storage solutions, etc.; these services might fail to afford adequate standards in terms of availability and performance compared to professional services. If the data to be processed relate to third parties, which is often the case for companies and public administrative bodies, the implementation of services that do not provide adequate safeguards in terms of operational continuity and confidentiality may affect the informational sphere applying to the individual data subjects significantly. From this standpoint, the data controller should always perform a backup of the data allocated to the cloud, for instance via a local copy in a compressed format. By so doing, it will be possible to handle any risks related to the purchase of services that, though cost-effective, might not be sufficiently reliable.

- *Select the data to be allocated to the cloud*

Some items of information to be allocated to the service provider's systems – e.g. health data, genetic data, financial information, biometric data, or trade secrets – may require special security measures to be in place on account of their inherent features. In this case, the user should assess responsibly whether to rely on the cloud computing service or else continue processing such data in-house – given that migration of the information to the cloud reduces, albeit partially, the user's direct control over such information, which is exposed to partly unforeseeable risks of loss and/or unauthorized access.

- *Never lose sight of your data*

Users should always carefully assess the type of service provided by also verifying whether the data will remain under the provider's physical control, whether the provider is only a broker of services, or whether the services the provider is offering have been designed by relying on technology made available by a third party. Consider, for instance, a cloud-based application whereby the provider ultimately providing the service to the user (in SaaS mode) relies on a data storage service supplied by a third-party provider. In this case, the latter provider's systems will physically host the data allocated by the user to the cloud.

- *Know where the data will actually be located*

Knowing in what country the servers that host the data are located physically is a key factor to establish jurisdiction and applicable law in case of disputes between users and service providers. The fact that a server is located physically in a given country entails that the locally competent judicial authority is empowered to enforce subpoenas and injunctions to access and/or seize data if this is permitted by the applicable domestic legislation. Thus, it is not immaterial for the user to know whether the data are hosted in a server in Italy, in Europe or somewhere outside Europe. Before allocating data to a cloud-based system, a user should always make sure that the transfers of information between the various countries where the clouds are located take place in accordance with the EU principles on personal data protection – which envisage special safeguards as for the adequacy of the protection afforded by domestic laws to such data.

- *Focus on contractual clauses*

If handled appropriately, contractual clauses can support users and providers in determining operational arrangements and SLAs as well as in setting forth the security benchmark for the specific activity/ies. It is fundamental in any case to assess whether the contractual terms applying to delivery of cloud-based services are suitable with regard to the obligations and liability in case the data kept in the cloud are lost and/or mislaid as well as in respect of the consequences if the user decides to shift to a different provider. Priority should be given to clear-cut QoS provisions, which should envisage penalties in case of non-performance by the provider along with the provider's liability for the effects produced by events such as unauthorized accesses, data loss, data unavailability due to failures, etc. . Additionally, it should be verified whether there are third parties in charge of providing services along the supply chain and participating in the delivery of the end-service to the given user; alternatively, one should identify beforehand which providers will be involved in the processing as for the

individual steps. Finally, one should establish the traffic data threshold as set forth in the contract beyond which additional fees are charged.

- *Check data retention policies as related to data storage*

When purchasing a cloud-based service, one should clarify the provider's policies – as laid down in the relevant contract – concerning the retention period of the data in the cloud. On the one hand, users should establish the deadline for final deletion of the data committed to the provider following expiry of the contract; on the other hand, providers should afford suitable safeguards to ensure that no data will be kept beyond the said deadline and/or in compliance with arrangements other than those agreed upon with users. At all events, data will always have to be kept in compliance with the purposes and mechanisms agreed upon and may not be duplicated or disclosed to third parties.

- *Demand and implement appropriate safeguards to protect data confidentiality*

In order to protect data confidentiality, users should also assess the security measures implemented by a provider prior to enabling allocation of data to the cloud. Generally speaking, priority should be given to providers that rely on secure transmission techniques by means of encrypted connections – in particular if personal data and/or confidential data have to be processed – along with identification mechanisms for access-enabled entities; complexity of such mechanisms and arrangements should be proportionate to data criticalities. In most cases, simple identification mechanisms based on username and password will be appropriate – providing suitably complex passwords are relied upon. If the processing concerns particular data categories such as health data, genetic data, income data and/or biometric data or any data whose confidentiality can be considered to be "critical", encrypted storage in the service provider's systems is recommended alongside the use of secure transmission protocols.

- *Train staff appropriately*

The staff in charge of data processing via cloud computing services should be trained specifically on how best to acquire data and allocate them to the cloud, access and use the new outsourced services, and implement the guidelines described herein. This is aimed at mitigating the data protection risks that might arise not only from inappropriate and/or fraudulent behavior, but also from minor mistakes, recklessness and/or negligence. All these events might actually result into unauthorized accesses and data loss as well as into unauthorized data processing operations.