CLOUD COMPUTING

HOW TO PROTECT YOUR DATA WITHOUT FALLING FROM A CLOUD

A Mini-Vademecum for
Businesses and Public Bodies

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CLOUD COMPUTING

HOW TO PROTECT YOUR DATA WITHOUT FALLING FROM A CLOUD

Entrepreneurs as well as forward-looking public bodies make all efforts to provide better and cheaper services to customers and citizens. IT technology, and in particular cloud computing, makes it possible to implement innovative solutions to handle a wide gamut of activities effectively and cost-efficiently. However, this technology also entails criticalities and risks to privacy that should be taken into account. Before outsourcing the processing of data and records or implementing new organizational models, you should ask yourself a few questions and take special care in selecting the solution that can best ensure the security of your institutional and business activities. With this vademecum, the Italian Data Protection Authority is providing guidance to all users – in particular businesses and public administrative bodies. Our objective is paving the way to an analysis of major legal, economic and technological issues in an area that is developing at a breathtaking pace to foster the appropriate use of these new tools for the delivery of IT services.

CLOUD COMPUTING: WHAT IS THAT?

Cloud Computing, or just “Cloud”, is a set of technologies and mechanisms for the use of IT services that make it easier to provide and rely on software and allow storing and processing a huge amount of information via the Internet. Depending on the specific configuration, you can shift either the storage or the processing of data (or both) from your computer to a provider’s systems. Additionally, cloud computing allows benefiting from complex services without having to purchase high-profile computers and equipment or hire staff to programme and run a complex system.

Everything can be committed (outsourced) to external providers at a potentially fractional cost, since the IT resources for the services you need can be shared with other clients in a similar situation.

THE “IT” CAR, OR CLOUD FOR DUMMIES

Option 1 – Do-It-Yourself
If an individual or a company needs a car, they may design it, purchase the individual components, assemble them, and set up a workshop at home or at the company’s headquarters with staff specializing in repairing and maintenance.

Option 2 – Go to a Vendor
You may choose to buy yourself a car and take it to a trusted garage when needed, rent it, lease it, call a cab or rent a chauffeured car. The choice among these options will depend on how you plan to use the car, how often you will need it, what kind of performance you are aiming at, and – by all means – on the moneys in your wallet.

Cloud computing falls under option 2. It has nothing to do with driving a car, as it is rather a way of obtaining IT services. The solutions made available on the cloud are usually more flexible, effective, adjustable as well as cheaper than in-house solutions. Still, they may entail the risk of losing control over your data.

We often make use of cloud technologies without knowing it. Some of the most popular email or word processing services are “on the cloud”.
Actually, many of the functions available on new generation mobile phones (i.e. smartphones) are based in a cloud – for instance, geo-location based services that list the nearest shops or restaurants, or the services allowing you to listen to music and play online, and many more functions and apps.

DIFFERENT CLOUDS FOR DIFFERENT NEEDS

There are various kinds of cloud computing. The differences have to do both with the way the cloud is structured and data is processed (internally or externally to an organization) and with the service models available to clients. Each type of cloud shows peculiar features, which should be assessed carefully by private and public bodies before relying on any cloud-based service.

CLOUD TYPES

Private Cloud
A "private cloud" is an IT infrastructure - a network of computers providing services - that is mostly dedicated to the need of one organization, which hosts the infrastructure in its premises. Alternatively, its management is committed to a third party via a conventional server hosting agreement, which is subject to strict supervision by the data controller. "Private clouds" can be compared to traditional data centres in which additional technological measures are taken to maximize exploitation of the available resources and expand these resources whenever necessary.

Public Cloud
In a "public cloud", the IT infrastructure is owned by a provider specializing in the delivery of services that makes available its systems to users, businesses or public bodies; this is achieved by sharing and delivering, via the Internet, IT applications, processing power and data storage capacity. The services are accessed

via the Internet, which entails shifting either data only or data and their processing to the service provider's systems. Thus, the service provider plays a key role in ensuring effectiveness of the measures taken to protect the information that was entrusted to him. Along with their data, users transfer a major portion of their control over such data if they opt for a public cloud.

Other Types of Cloud
There are other types of cloud with mixed features such as the "hybrid cloud", where some services are provided by a private infrastructure whilst other services are delivered via public clouds, and the "community cloud", in which an IT infrastructure is shared by several organisations for the benefit of a specific user community.

THREE MODELS FOR CLOUD SERVICES

Cloud Infrastructure as a Service - IaaS
The cloud service provider makes available basic hardware and software tools (like memory space, operating systems, virtualization software, etc.) according to a consumption-based model; that is, he makes available remote virtual servers that end-users (whether businesses or public bodies) can rely on to replace or supplement their IT systems as hosted in their own premises. These providers are usually specialized market operators and can count on a complex technological infrastructure that is frequently distributed over a large geographic area.

Cloud Software as a Service - SaaS
The cloud service provider makes available, via the Internet, various software applications to end-users. They may consist in popular office applications that are delivered via the Web, such as calculation sheets or word processing software, IT protocol and document access rules, mailing lists and shared calendars up to high-profile email services.

Cloud Platform as a Service - PaaS
The cloud service provider makes available advanced software development solutions to meet a client's specific requirements. This type of service is usually targeted to market operators that use it to develop and host proprietary applications such as financial, accounting or logistics management applications – either for their own purposes or to provide services to third parties. Again, the services made available by the cloud provider make it as good as unnecessary for the end-users to equip themselves with specific or additional hardware or software.

THE LEGAL FRAMEWORK

THE INTERNATIONAL CHALLENGE

Cloud technology develops at a much quicker pace than legislation – not only in Italy, but worldwide. There is as yet no updated regulatory framework in the privacy sector or in civil and criminal law to take account of all the innovations brought about by cloud computing, so as to afford appropriate safeguards in connection with the legal issues that may arise from the adoption of distributed data processing and storage services.
For instance, the European legislation on data protection dates back to 1995. Some helpful innovations were introduced into the telecom legislative framework by the so-called "Telecom package", and this is bound to also impact on cloud computing.
They consist, in particular, in directive 2009/136 - which amended the 2002 e-privacy directive and whose transposition by EU Member States is in progress. The measures envisaged in the new legal framework include an obligation for telephone companies and Internet providers to notify the competent national authorities and (under certain circumstances) users of any security breaches that entail the destruction, loss or unwanted disclosure of personal data that is processed as part of the service being provided. An additional major change to the whole electronic communications sector – including cloud computing – is expected to take place by 2014, when the new Data Protection General Regulation (COM(2012)11) proposed by the European Commission is likely to come into force. The new Regulation will introduce the same rules throughout

the EU also with regard to third countries, which means that the Italian data protection Act will also be re-drafted from scratch. From this viewpoint, it will hopefully contribute to making the use of cloud-based services both less complex and less risky.
One of the key innovations of the reformation package in question consists in making all data controllers (banks, insurance companies, health care agencies, local authorities, etc.) subject to the obligation to notify security breaches that concern personal data. The individuals affected will be informed without delay of the loss and/or theft of their data, in the appropriate cases.

PRIVACY LAWS AND CLOUDS – FOOD FOR THOUGHT

Until up-to-date, harmonized domestic and international legislation is passed to enable governance of cloud computing without jeopardizing the innovation and development potential of IT "clouds", businesses and public bodies should take special care in assessing the risks resulting from a shift to cloud-based services - including personal data protection issues. This applies to the so-called "central purchasing bodies" as well, that is the entities in charge of purchasing goods on behalf of several public administrative agencies.

Data Controllers and Data Processors
Where a public administration body or a company, acting as the "data controller", moves part or the whole of its processing operations concerning personal data to the "cloud", it should appoint the cloud service provider as the "data processor".
This means that the client will have to always check how any personal data that is uploaded to the "cloud" is used and stored: the client, being the data controller, will also be liable for any wrongdoing committed by the provider. However, a small-sized client such as a SME or a local authority might find it hard to negotiate appropriate terms for the management of "cloud-based" data; still, claiming that the client was unable to negotiate more stringent contractual terms or supervision mechanisms will not be enough to justify violations. Indeed, a client of cloud-based services can apply to other providers, who may afford more robust safeguards especially concerning data protection. Additionally, the Italian data protection Code provides that the data controller is empowered to control the data processor's (here, the cloud provider's) conduct by checking that the processor complies with the instructions issued with regard to the personal data to be processed.

Data Flows outside the EU
The Italian privacy Code includes detailed rules to transfer personal data outside the EU and forbids – in principle – transferring personal data "even transiently" to a non-EU country if no adequate level of protection is afforded by the legal system of the country of transit and/or destination of the data.
This may often be the case if one relies on public cloud services as opposed to private cloud and/or hybrid cloud services.

Thus, the data controller – usually the client purchasing cloud-based services – will have to also take due account in its determinations of where the data are stored and what processing operations are expected to be performed abroad. For instance, transferring data to the US may be easier if the cloud provider has signed up to data protection schemes like the so-called Safe Harbor – which is a bilateral EU-USA agreement including shared, secure rules to allow personal data to be transferred to companies established in the USA.
The limitations on cross-border data flows also impact on "intra-group" data flows in a multinational setting; here, the availability of robust "binding corporate rules" to protect personal data can allow data transfers by respecting data subjects' privacy.

Data Security
The data controller is required to make sure that technical and organizational measures are in place to minimize the risk that data may be destroyed or lost (even by accident), that it may be accessed by unauthorized entities or processed unlawfully or in a way that is not compatible with the purposes for which it was collected,

or that it may be modified because of unauthorized or unlawful actions. For instance, a client should make sure that data is always "available" – that is, it can be accessed at any time – and "confidential" – that is, it may only be accessed by those authorized to do so. To secure data, one should focus not only on how it is stored, but also on how it is transmitted – for instance, by using encryption technology.

Data Subjects' Rights
Any public administration body or company deciding to rely on cloud-based services to manage users' and customers' personal data should not forget that the Italian privacy Code empowers data subjects – that is, the individuals the data relate to – to exercise specific rights.
For instance, data subjects have the right to know which data concerning them are held by a public body or a company; for what purpose(s) such data were collected; and how they are processed. They may apply for an intelligible copy of the personal data relating to them and have such data updated, rectified or supplemented.
In case of a breach of the law, data subjects may also have their data blocked, erased or anonymized.
In order to comply with these requests, the client of cloud-based services – being the data controller – will have to adequately supervise not only the provider, but also any sub-processors the provider may decide to have recourse to.

ASSESSING RISKS, COSTS, AND BENEFITS

In selecting the type of cloud and service model that best fits in with your needs, you should be especially careful.
This is particularly important if you opt for a public cloud, where basically all of the processing is outsourced and your most valuable information is well beyond your direct control. The cloud concept may sound vague and "virtual"; in fact, cloud technologies allow handling very tangible services such as a company's supply chain, the census register of a local authority, medical examinations and lab tests, your online banking activities, and much more. Nobody would leave their wallet with their personal IDs and their wages to any Tom, Dick or Harry; nor would you entrust your accounts book or customer and vendor contracts to an unknown accountant who promised you would save a lot by doing so - without first making sure how these valuable records will be kept or used.

Thus, "saving" should not be the only variable in making your choice.
There is a handful of major cloud computing providers; basically all of the remaining companies that offer cloud-based services and infrastructures avail themselves of such world leaders. This means that the negotiating power of an individual company or a small public administrative body is considerably downsized, so that it is difficult to turn technological flexibility into contractual flexibility. You might then want to join forces with other public bodies and/or companies with the same needs (for instance via your trade or sector-related association) so as to build up your contractual power.
Before opting for a given type of "cloud", you should check for the amount and types of information to be outsourced – will that include personal data along

with sensitive personal data, or will it consist in information that is key to your business/activity, such as confidential or patented projects or industrial secrets?
You should assess the possible risks and consequences resulting from your choice. It is true that clients are often unable to negotiate changes to the provider's "Terms of Service"; still, they can certainly select a different provider. Cloud providers could also benefit in terms of opportunities from laying down "privacy-friendly" contractual clauses and/or relying on prior independent certification of their compliance with EU personal data protection laws.
There are some basic questions to be posed so that you can estimate the impact of these technologies on your company / your public body in terms of costs and organizational arrangements.

SECURITY

What security measures were put in place by the provider to protect the data?
A cloud service provider can often count on protection systems against viruses, hacker attacks or other IT dangers that are more effective than those a user could individually afford. However, you should determine what measures were put in place by your cloud provider. Before deciding for your cloud partner, keep in mind that you may lose your direct, exclusive control over your data if you hand them to a remote provider.

ROLES AND RESPONSIBILITIES

Who is actually providing the service you are about to purchase?
Is it a company or a group of companies?
The service you chose might be the end-result of a "transformation chain" of services that are purchased from service providers other than the provider you are contracting with. If the chain is especially long or complex, you might not be in a position to know who can access what data out of the many intervening service providers.

SERVICE AVAILABILITY AND DISASTER RECOVERY

If the Internet connection is down or impaired, can you continue using the services you need without using the cloud?
How long does it take to restore service?
Is there a disaster recovery plan for your key services?

The virtual service might happen to be degraded following IT attacks or during traffic spikes, and it might even be down following extraordinary events or failures that make data temporarily inaccessible – if no adequate safeguards for network connectivity are in place. Thus, you should carefully consider how your company / your public body would be impacted by a breakdown of the service, whatever its duration, take account of the costs (both direct and indirect) you may have to bear if data become inaccessible, and lay down – beforehand – a disaster recovery plan with your cloud provider.

DATA RECOVERY

Can data on the cloud get lost or be destroyed?
Natural disasters or cyber-attacks might undermine the operation of some data centres.

It is especially important to rely on data recovery procedures and gauge the financial and organizational impact of the loss and/or erasure of any data that is only available on the cloud.

CONFIDENTIALITY

Are there confidentiality safeguards for our data if a competitor shares the same cloud-based services?
Providers handle data from individuals and organizations that might have different or conflicting/competing interests and requirements.
Thus, you should assess the safeguards afforded to ensure confidentiality of the information you commit to the cloud.

SERVER LOCATION

In which country is the data uploaded to the cloud ultimately kept?

Can one decide to only rely on servers that are located in the national territory, or in EU countries?
The location of data storage/processing impacts directly both on the applicable law – in case of disputes between client and provider – and on the national rules applying to data processing, storage, and security.
Knowing this will ensure greater transparency in the client/provider relationship. Additionally, one should not forget that privacy laws only allow "exporting" data from the EU under specific circumstances and if adequate protection measures are in place for data subjects by comparison to the protection afforded under EU legislation.
Thus, a cloud-based service might entail unforeseen additional costs resulting from the client's limited control over his data, or else – which is more likely – on account of national and international litigation.

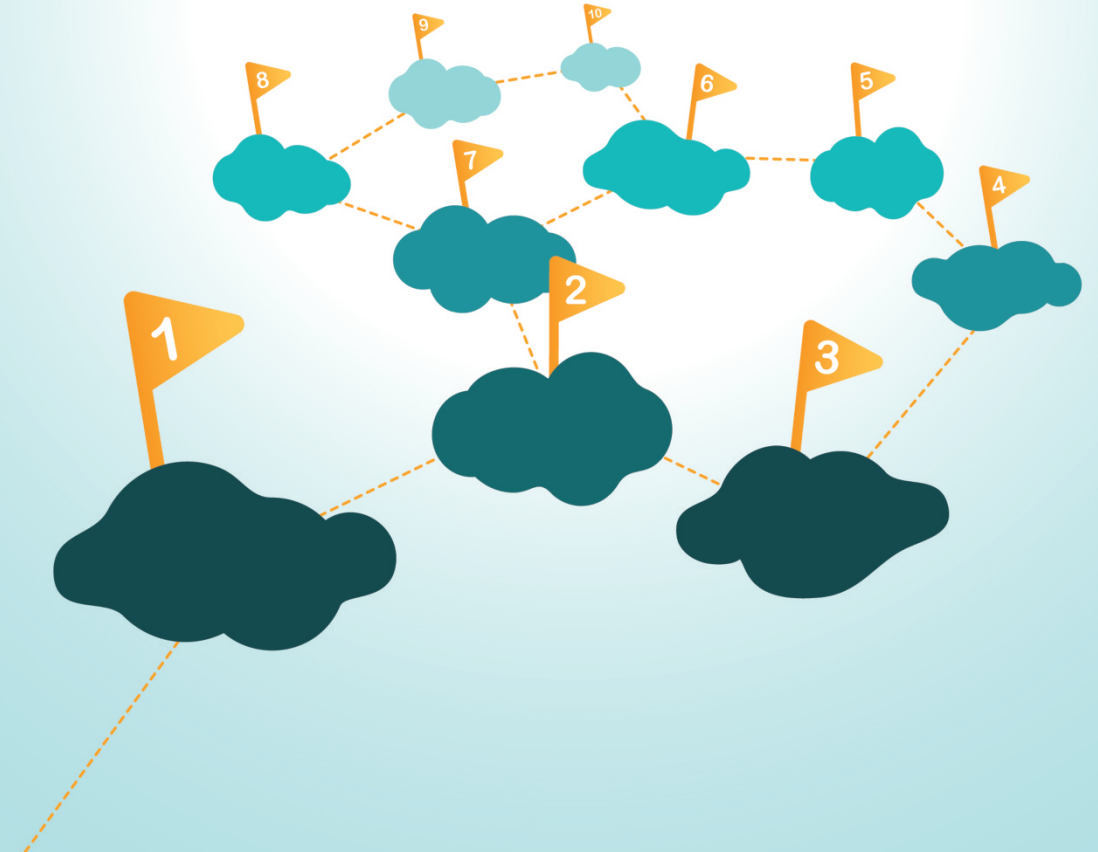
MIGRATION

Does the cloud provider rely on proprietary technology? Can data be exported easily?
In some cases, the fact that the service provider relies on proprietary technology may make it difficult for the client to migrate data and documents between different cloud-based systems, or to exchange information with entities that use cloud services from different providers – that is to say, data portability and/or interoperability may be jeopardized.
This is a scenario that might result into less-than-straightforward business strategies. For instance, a cloud service provider might initially submit a very appealing offer to a client including adequate data protection safeguards; having taken the client on board, the provider might then change the terms of service to its own advantage on the assumption that the client will be bound to accept the new terms since it is practically impossible for him to easily shift the data to another provider and terminate the contract.

INSURANCE

If it is found that a data breach occurred or data were lost, can the provider ensure prompt payment of damages?
Because of the lack of clear-cut regulations, it may prove both difficult and costly to get the appropriate compensation in case of damage following data breach, data loss, or (temporary) discontinuation of the cloud-based service.
Availability of an insurance policy and/or simplified mechanisms for settling (international) disputes may translate into added value for small-sized users.

TEN RULES TO CHOOSE KNOWLEDGEABLY



1

CHECK HOW RELIABLE YOUR PROVIDER IS

Users should establish how experienced, skilled and reliable their provider is before moving their most valuable data to the cloud; they should take account of their business or institutional requirements, type and amount of the information to be allocated to the cloud, risks and security measures in place. Depending on, among others, the type of service to be provided and the importance of the data, users should assess the provider's corporate structure; the provider's references; the legal safeguards afforded to ensure data confidentiality along with the measures in place to prevent service breakdowns following unexpected failures.
Additionally, users should assess the quality of the connectivity services the provider relies upon in terms of their capacity and reliability. Users might also want to consider whether the provider employs skilled staff, how adequate the provider's IT and communications infrastructure is, and to what extent the provider accepts to be liable for damages – which should be set forth explicitly in the terms of service – in case of security breaches and/or service breakdowns.

2

PREFER SERVICES WITH ENHANCED DATA PORTABILITY

Clients should prefer cloud computing services that rely on open formats and standards to facilitate migration between cloud systems managed by different providers. Data portability means you can withdraw from the service without incurring costs and inconveniences that are difficult to gauge in advance.

Additionally, this will reduce the risk that a provider may change the terms of the cloud service contract unilaterally to the client's detriment by taking advantage of his stronger negotiating power.

3

MAKE SURE DATA IS AVAILABLE WHENEVER NECESSARY

Clients should request that their contract with the cloud provider includes clear-cut, adequate safeguards on availability and performance of cloud services. Choosing a service that does not afford adequate confidentiality and continuity safeguards may impact substantially not only on the cloud client, but also on the data subjects – think of public administrative bodies or any company delivering services to third parties.
This is why the data controller – who is usually the cloud client – will have to make sure that he can keep a copy of any data allocated to the cloud apart from any underlying cost-containment objective; this is especially appropriate if the loss and/or unavailability of such data might prove seriously harmful not only to the controller's finances and/or image: think of highly sensitive information such as health care or judicial data, or any data on taxation and personal income.

4

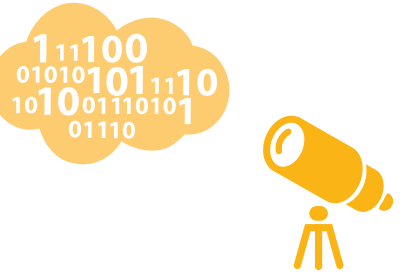
SELECT WHICH DATA SHOULD BE MOVED TO THE CLOUD

Some items of information require – by their very nature – specific security measures to be in place: this is the case of information protected by industrial secrecy rules as well as of sensitive data such as information relating to health, ethnic origin, political opinions or membership of trade unions. Since moving data to the cloud reduces, in all cases, the user's direct control over such data, which is exposed to the (at times hardly foreseeable) risk of being lost or accessed unlawfully, users should evaluate responsibly whether to rely on cloud computing services (particularly public cloud services) or have recourse to other types of outsourcing or even continue processing that data "in house".

5

NEVER LOSE SIGHT OF YOUR DATA

Users should always carefully consider the type of service being offered and check whether the cloud provider that is party to the contract will be holding the data factually or else that provider is actually a broker of services or relies on technologies made available by a third party.
This might occur, for instance, with a cloud-based application where



the provider of the data processing service ultimately relies on a storage service purchased from a third party: this will entail that the client's data will he hosted factually in the physical systems owned by the third party in question.
Thus, to gauge the quality of cloud-based services one should establish who does exactly what out of all the entities involved in providing those services.

6

KNOW THE PHYSICAL LOCATION OF YOUR DATA

It is important for users to know whether their data will be moved to and processed by servers in Italy, the EU, or a non-EU country.
This information may be essential to determine jurisdiction and applicable law in case of disputes between users and service providers; above all, it is fundamental to check the protection afforded to the data.
Transferring data to countries where no adequate safeguards are in place in terms of security and confidentiality might make the processing of personal data unlawful and cause irreparable damage to the institutional activities of a public body as well as to a company's business. Before uploading data to the cloud and allowing data transfers to non-EU countries, users should check that this transfer takes place in accordance with the safeguards laid down in Italy's and EU's legislation on personal data protection.
For instance, if the cloud provider is a US-based company, one should check that it is a member of the Safe Harbor scheme – which includes rules agreed upon with EU institutions to enable the processing of personal data.
It is also helpful to check that any non-EU cloud service provider has subjected its security and data processing procedures to specific certification schemes such as those regulated by ISO security standards.
Additionally, one should check whether the outsourcing contracts submitted by the provider include the "standard contractual clauses" approved specifically by the European Commission to transfer personal data to third countries.

7

BE ALERT TO YOUR TERMS OF SERVICE

It is important to assess whether the terms of service laid down in the cloud contract are appropriate; this is true, in particular, for the obligations and liability applying to loss and/or unauthorised disclosure of the data kept on the cloud as well as for the mechanisms to withdraw from the service and shift to a different provider.
Special emphasis should be put on the specification of clear-cut quality standards along with the respective penalties, so that the provider is made liable for non-performance as well as for the consequences of specific events such as unauthorised access, data loss, unavailability due to malfunctioning, etc.
To be on the safe side, check whether sub-contractors are involved in delivering cloud-based services and/or processing the data.

8

CHECK FOR HOW LONG AND IN WHAT MANNER DATA IS RETAINED

Before relying on cloud-based services, one should probe into the provider's policies regarding data retention on the cloud and make sure that they are laid down contractually. If the law does not

provide for the erasure of the controller's data immediately the cloud contract expires, one should establish the deadline for the provider (= the data processor) to erase any data that was committed to him. The provider must ensure that no data will be kept beyond such deadline or in breach of what was explicitly set out with the client. At all events, all data must be kept in compliance with the purposes and arrangements agreed upon.

9

DEMAND ADEQUATE SECURITY MEASURES

In order to protect data confidentiality, one should also consider the security measures put in place by the cloud service provider.
Generally speaking, preference should be given to providers that rely on secure data storage and transmission mechanisms as based on encryption – especially if highly sensitive information is to be processed – along with robust mechanisms to identify access-enabled entities.

10

TRAIN STAFF APPROPRIATELY

Both the client's and the provider's staff should be trained appropriately if they are tasked with processing data via cloud computing services so as to reduce the risks of unauthorised access, data loss and – more generally – unlawful processing operations.
Training should include the technical information to enable the knowledgeable selection of cloud technologies along with the practical steps of the processing such as uploading data to the cloud and processing such data.
Data protection may be jeopardized not only if staff behave unfairly or fraudulently, but also if they make trivial mistakes or work sloppily or negligently.

ONE MORE CAVEAT ON PROCESSING FOR PERSONAL OR HOUSEHOLD PURPOSES

The Italian Privacy Code does not apply to an individual who processes personal data for personal purposes and does not disseminate such data on the Internet or does not disclose such data systematically to several individuals.
Still, it should be recalled that individuals are also expected to keep personal data with due care to prevent that the loss of such data may harm other individuals.
New mobile technology devices like smartphones and tablets have considerable memory capacity and often rely on unprotected cloud-based services that allow them to be used for both private and professional purposes – which has increased the risk of losing control over one's personal data.
This means that you should keep your IT devices with care even if you use them for personal purposes; you should also make sure that no third party may access – even by chance – personal data kept on those devices.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ITALIAN DATA PROTECTION AUTHORITY

Piazza di Monte Citorio, 121
00186 Rome - Italy
phone +39 06 696771
fax +39 06 696773785

For additional info:
Ufficio per le relazioni con il pubblico
(Front Desk)
Mon-Fri 10-13 on location
or call +39 06 696772917/9
e-mail: urp@garanteprivacy.it

**Edited by Servizio relazioni
con i mezzi di informazione
(Media and Outreach Service)**

www.garanteprivacy.it

VERTIGO DESIGN

Printed by IAG Mengarelli – July 2012