GDPR

Alessandro P Giorgetti
Studio Legale Giorgetti

Italy and the General Data Protection Regulation (GDPR)

Introduction

The right to an individual's data protection is fundamental, being enshrined in article 8 of the Charter of Fundamental Human Rights as well as article 16 of the European Union Treaty. Therefore, all subjects who collect, manage, store, transfer or treat personal data, regardless of whether they are sensitive or not, must adopt a risk management policy in order to ensure that their storage, use and elaboration is made in compliance with the law to ensure the protection of such data and personal information when potentially endangered by computer fraud, technical problems or mistakes of any kind.

Technology has radically changed our way of living and working, expanding the space beyond the boundaries of our homes and businesses. People today interact, thanks to smart phones, tablets and other electronic equipment, with other people, household appliances, computers and production machines, thanks to the exchange of data.

However, such data, despite being intangible, can be violated, stolen and manipulated for criminal purposes, or simply damaged or destroyed through human error or negligence. Data breaches, therefore, constitutes any event where sensitive data and personal, medical, or financial information are, actually or even only potentially, endangered. Sources of data breaches can be cybercrime, but also technical problems and human errors. In any event, the consequences for the victims can be significant and the damages, from loss of profit to the recovery costs or to reputational damage, can be huge and become a source of potential collective actions. Defence costs resulting from violations or loss of data can be very high and include legal fees, consultancy expenses, as well as costs incurred informing customers of what happened and the due corrective measures, before taking into account fines and sanctions provided by the law.

According to the latest Breach Level Index report by Safe NetGemalto, more than 5.3 billion pieces of data have been lost or stolen in the last three years, which is more than 3.8 million pieces per day and 2,600 pieces every minute.

The Center for Strategic and International Studies estimates that computer attacks cost about €500 billion a year, and in Italy alone they have been valued at between €800 and €900 million. However, damage to reputation alone would amount to more than €8 billion in Italy, which is equivalent to about 0.6 per cent of GDP, and the losses owing to system failure would exceed €14 billion.

In order to prevent or limit these losses, the EU dictated precise rules to safeguard the security of personal data with:

- Community Directive 95/46/EC laying down general principles for the free movement of personal data within European territory;
- Community Directives 2002/58/EC and 2009/136/EU concerning the processing of personal data and the protection of privacy in electronic communications, which introduced precise rules about online personal data collection and the use of cookies; and
- General Data Protection Regulation (GDPR) No. 2016/679 of the European Parliament and of the Council of 27 April 2016, which repealed and replaced Directive 95/46/EC.

The GDPR

The new Regulation will become mandatory in all EU member states, two years after its publication in the Official Journal of the European Union, on 25 May 2018.

The GDPR has introduced new principles on the protection of individuals with regard to the processing of personal data and to their free circulation within the European Union; but interestingly, in addition it has extended the efficacy of the rules on personal data processing outside of it, as long as the data processing concerns the supply of goods or services to EU citizens.

This is the first significant change because social networks, web platforms (even in clouds) and search engines will become subject to the Regulation, despite their location, and even if they are managed by companies outside the European Union.

Other important innovations include the following obligations on the holder of the personal data to:

- define the retention times of the data and indicate their source, if used;
- promptly notify the guarantor of any breach of his or her own database;
- draft the Data Protection Impact Assessment (DPIA), a risk assessment document related to data management incorporating the principles of privacy by design and privacy by default introduced by the GDPR; and
- to ensure the accountability of the data privacy officer (DPO) by way of an appropriate organisational chart and human and financial resources.

New roles and responsibilities

The privacy protection required by the GDPR imposes that compliance and governance programmes are accepted and adopted by the entire company.

A report published by the think tank Centre for Information Policy Leadership (CIPL) recommends integrating the data security requirements into all stages of each business process from design to release. Notwithstanding this clear message, confusion reigns over who has the responsibility of setting the rules to comply with the GDPR requirements. The CIPL report stresses that almost one-third (32 per cent) of the respondents believe that the person responsible should be the chief information officer (CIO), 21 per cent the chief information security officer (CISO), 14 per cent the CEO and 10 per cent the chief data officer (CDO). In reality, personal data management is no longer just a fulfilment of a managerial obligation, but it has transformed into a process that impacts the organisation of each company so that all the above figures shall cooperate and play an important role in their specific area of competence.

For example, in the event of a technical accident or data breach, the responsibility for data encryption and permanently secure confidentiality, integrity, availability and flexibility of the processing as well as the timely restoring of access to personal data rests with the CIO and the CISO. Whereas the CDO shall have responsibility to report the accident and manage the client relationship; third parties and the supervisory authority (SA) shall investigate the event. Finally, the CEO shall supervise the entire system and shall provide adequate financial and human resources to meet the need assessed with the DPIA.

The officers shall also ensure that anyone acting under their authority and having access to the processed data is instructed and capable to act in full accordance with the GDPR requirements. According to a Microsoft study on phishing emails, 23 per cent of the electronic messages of this type are regularly opened, 11 per cent

of victims open the link contained within the email giving hackers full access to their systems, and in 60 per cent of cases the attack is successfully completed within minutes.

Therefore, an adequate document management system will be developed through the compulsory establishment of a data processing registry, where all actions carried out, or accidents, can be tracked and documented according to the accounting principles or to the GDPR rules, to ensure that each data operation conforms to the provisions therein.

The Regulation also introduces the DPO as being a new professional figure who can be an employee of the company or an external consultant. This position is not merely that of a manager, but a professional figure whose skills shall vary from legal, informatics and organisational expertise. Besides overseeing the simple formal controls on data processes, the DPO shall support the decision-making process of the personal data holder and shall interact with the SA.

For public authorities and public agencies, as well as for all enterprises that process data of a significant number of people, or data that, by their nature and purpose, is sensitive or at risk, like banking and insurance, it is mandatory to have a DPO whose appointment will normally last for four years.

The national SA and the European Data Protection Board (EDPB)

All EU member states shall apply a single set of rules, but each member state will establish an independent SA to hear complaints, conduct investigations,sanction administrative violations and so on. In Italy, the current SA is called the 'Garante della privacy'.

The SA in each member state will cooperate with each other providing mutual assistance.

If a company has more establishments throughout the EU, the competent SA shall be the one of the place where the main management activities take place. The main authority will act as a one-stop shop to oversee all data management activities of that company within the EU.

The EDPB will coordinate and superintend all national SAs including the Italian one.

The Italian SA in this perspective has actively participated with the article 29 Data Protection Working Party that has developed the guidelines for the correct and homogeneous implementation of the GDPR. In particular, the article 29 Data Protection Working Party on 13 December 2016 adopted, as revised on 5 April 2017, the following guidelines:

- on the DPO;
- on the right to data portability:
- for identifying a controller or processor's lead supervising authority; and
- on the DPIA and determining whether processing is likely to result in a high risk for the purposes of Regulation No. 2016/679.

Data breaches and sanctions

To guarantee rule compliance, in case of breaches the GDPR provides that the competent SA can impose heavy sanctions as:

- a warning in writing in cases of first and unintentional breaches or non-compliance;
- regular periodic data protection audits;
- a fine of up to €10 million or up to 2 per cent of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater; and
- a fine of up to €20 million or up to 4 per cent of the annual worldwide consolidated turnover of the preceding financial year in case of an enterprise part of a group, whichever is greater, depending on the breach or non-compliance and the gravity of the consequences for the owners of the lost or damaged data.

To prevent breach or non-compliance the DPO must make a DPIA. The document should include an analysis of the risks involved, identify any existing risk, an action plan for their resolution and an annual review of the actions taken to ensure their control and risk reduction. By imposing the DPIA, the SA encourages the establishment of risk management mechanisms and certification procedures for data protection. Therefore, adherence to a code of conduct or to an approved quality certification mechanism could become means by which to demonstrate compliance with the Regulation's security requirements.

In the event of a breach, the DPO must notify the event to the SA within 72 hours of the event and, if the violation caused damage to the affected parties, to report it without delay. The strict timing poses major problems. In fact, it is estimated that about 300,000 variants of malware are discovered every day. Such malware typically includes programs designed to carry out specific attacks to destroy data, steal information and even compromise the activity of victims.

According to a Ponemon Institute study, an average of 205 days is necessary to identify a flaw in security systems and, in many instances, the violation was only discovered after the hackers blackmailed the **victim**. The latter example occurred at the European Central Bank (ECB) in July 2014, when, following an attack, thousands of addresses and pieces of personal data on European citizens were captured, but the attack was discovered only after the attackers contacted the ECB for a redemption. The variety and complexity of malware makes identifying the attackers immediately very difficult and is now a serious danger for the DPO if he or she does not report an attack within the allotted time. In fact, for data loss, fines of up to €20 million are foreseen for individuals and companies not belonging to groups and up to 4 per cent of the consolidated total turnover for corporate groups.

Italy and data protection

At present, IT security in Italy is grossly inadequate to meet the level of sophistication of current cybercrime. In spite of this, a Dell and Dimensional Research report proved that only 9 per cent of IT and business professionals are ready for the GDPR, and a study by the Milan Polytechnic Security and Privacy Observatory confirmed that,

Studio Legale Giorgetti

Alessandro P Giorgetti **giorgetti@giorgettilex.com**

Via Fontana 28
20122 Milan
Italy

Tel: +39 02 545 7734 / +39 02 545 7923
Fax: +39 02 551 8028 2
info@giorgettilex.com
www.giorgettilex.com

less than a year from the GDPR being fully in effect, Italian companies are still late in meeting the new security requirements.

The Ponemon Institute published the results of its 2016 Cost of Data Breach Study revealing that the public sector and the private retail outlets are the most-hacked sectors, probably because of the large amount of sensitive data collected combined with low levels of security.

According to the Cyber Intelligence and Information Security Center at the Sapienza University in Rome, which conducted national research, found in contrast that despite all the financial organisations having been attacked, breaches were only successful in a mere 17 per cent of cases. This proves the higher degree of security that characterises banks and insurance companies in general. Finally, the industrial sector remains the least likely area to be attacked, but only 29 per cent of enterprises would be able to detect an advanced persistent threat.

Despite the efficiency of the security systems adopted, it is estimated that most of the incidents are not even detected by the victims.

In this context, the GDPR imposes on private companies and public bodies, that they operate with an approach fully integrated for the treatment of personal data, which is no longer based on the simple concept of compliance, but characterised by a pre emptive analysis followed by appropriate risk management and, eventually, the remedial action plan.

To address and improve such a situation, on 13 October 2016, the Italian SA published the Code of Ethics and Conduct in Processing Personal Data for Business Information Purposes, which joined the already available Guidelines on processing personal data in performing debt collection and the Guidelines on data breach notifications.

Following the large-scale implementation of the Guidelines and actions set for May 2018, according to a Veritas survey, nearly 40 per cent of businesses fear that they will not be able to comply with the new regulations, while just under one-third (31 per cent) are worried about brand-reputation damage caused by inadequate data policies.

This situation opens a few important scenarios for the insurance market because new forms of liability will emerge posing serious problems. Are the GDPR sanctions insurable or not? Is the DPO liability falling within the scope of the existing directors' and officers' insurance or will a totally new liability policy be necessary? How does one quote a risk for which there are no statistics? How can damages to clients and third parties be insured and is there any insurer that can provide capacity, hence cover for the damage to the company or stockholders if a fine of 4 per cent of the consolidated total turnover for corporate groups were to be imposed?

Despite the difficulties the GDPR will pose in Italy, it will be an opportunity for prudent but capable insurers to benefit from the opportunities that this new regulation will introduce to Italy, Europe and the wider world, having expanded its operation well beyond EU member states.