GDPR

Alessandro P Giorgetti
Studio Legale Giorgetti

Italy and the General Data Protection Regulation
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 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 owing to smart phones, tablets and other electronic equipment with other people, household appliances, computers and production machines, thanks to the exchange of data.

However, this 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, constitute any event where sensitive data or 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 damage, from loss of profit to the recovery costs 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 SafeNet Gemalto, the total number of records compromised in the first half of 2018 was 3,353,172,708, marking an increase of 72 per cent over the year 2017. Of the incidents reported, 21 were data breaches where encryption was used, less than half the figure for the previous year. 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 million 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.

To prevent or limit these losses, the Europan Union 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 EU 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
On 25 May 2018, the Regulation entered into force in all EU member states, two years after its publication in the Official Journal of the European Union.

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
- 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 chief executive officer 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 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 GDPR requirements. A Microsoft study on phishing emails proves that this type of electronic message is regularly opened, with about 9 per cent of victims opening the link contained within the email, giving hackers full access to their systems, and in about half of cases the attack is successfully completed within minutes. However, at the 2018 Safer Internet Day, Microsoft released its second Digital Civility Index, which shows that people's digital interactions and responses to online risks appear to be improving around the world.

Therefore, an adequate document management system must 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 set forth in 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, are sensitive or at risk, like banking and insurance, it is mandatory to have a controller and a DPO whose appointment will normally last for four years.

The national SA and the EDPB

When the GDPR entered into force, the Article 29 Data Protection Working Party, created under the previous legislation, was substituted by 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 and sanction administrative violations, and so on. In Italy, the current SA is the Italian Data Protection Authority.

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

If a company has more establishments throughout the European Union, the competent SA shall be where the main management activities take place. The main authority will act as a comprehensive entity overseeing all data management activities of that company within the European Union.

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

The Italian SA has actively participated with the Article 29 Data Protection Working Party in developing 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, which are in great part still effective and the guiding principle of reference:

- on the DPO;
- on the right to data portability;
- on 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 the case of breaches, the GDPR provides that the competent SA can impose heavy sanctions as:

- a warning in writing in the 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 the 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 the 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.

Since the GDPR entered into force a few fines have already been issued, the greatest of which to date is the recent €50 million fine imposed by the French data protection authority on Google for processing personal data for advertising purposes without the required consent under the GDPR. But, other European SAs have been active too in sanctioning data breaches. In Germany, the regulators imposed a €20,000 fine on a company for failing to protect employee passwords with cryptographic hashes, while in Austria, a €4,800 fine was issued for operating an unauthorised CCTV system overseeing a public pavement and finally, on 1 February 2019, the UK SA issued fines totalling £120,000 to a UK referendum campaign company and to an insurance company for serious data breaches.

To prevent breach or non-compliance the DPO must make a DPIA. The document should include an analysis of the risks involved, an identification of 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. It is estimated that several hundred thousand variants of malware are discovered every day. Such malware typically includes programs designed to carry out specific attacks to destroy data, steal information or compromise the activity of victims as in cases of CryptoLocker attacks.

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. A recent example is what occurred from 2014 to September 2018 at Starwood Hotels, when, following an attack, personal details of roughly 500 million guests were captured, but the attack was discovered only in November 2018 following deep forensic investigations on the company's computerised booking system. 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. 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

Six months after the GDPR being fully in effect, Italian companies are still late in meeting the new security requirements and, at present, IT security in Italy is grossly inadequate to meet the level of sophistication of current cybercrime.

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

The Research Center of Cyber Intelligence and Information Security 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 data risk analysis followed by appropriate risk management and, eventually, a 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 (together, the Guidelines).

Following the large-scale implementation of the Guidelines and actions of May 2018, according to the last 2017 Veritas survey, nearly 39 per cent of businesses fear that they will not be able to comply with the new regulations, while just under one-third (27 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. Does DPO liability fall within the scope of the existing directors and officers (D&O) insurance or will a totally new liability policy be necessary? If yes, which one: a D&O policy, a cyber-policy, or an errors and omissions policy tailor-made for the new professional? How is a risk that has no statistics quoted? How can damage 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?

In this context, are GDPR fines insurable? A recent study concluded that GDPR fines are insurable in only two out of 30 European countries reviewed: Finland and Norway, whereas in 20 jurisdictions GDPR fines would generally not be regarded as insurable, including the United Kingdom, France, Italy and Spain. In the remaining eight jurisdictions it is unclear whether GDPR fines could be insurable. A lot will depend on the specific individual case; for example, the conduct of the insured and whether the fine is considered to be of an administrative sanctioning or a criminal nature.

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.

Studio Legale Giorgetti

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

Via Fontana 28
20122 Milan
Italy

Tel: +39 02 54 57 734 / 923
Fax: +39 02 55 18 02 82
www.giorgettilex.com