Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cyber Security

Italy
LCA Studio Legale

chambersandpartners.com

2019

ITALY

The 'Law & Practice' sections provide easily accessible information on navigating the legal system when conducting business in the jurisdiction. Leading lawyers explain local law and practice at key transactional stages and for crucial aspects of doing business.

Law and Practice

Contributed by LCA Studio Legale

CONTENTS

Contributed by LCA Studio Legale ***Authors:*** Gianluca De Cristofaro, Chiara Bocchi

LCA Studio Legale has an Intellectual Property & Data Protection department composed of 15 professionals, who assist national and foreign companies in the protection, exploitation and enforcement of their IP rights, as well as in all privacy and personal data-protection issues including: ordinary privacy fulfilments; compliance process to the new European General Data Protection Regulation (No 679/2016); approval process of Binding Corporate Rules in the case of transfer of personal data to third countries; cybersecurity threats; corporate know-how protection; training of company personnel on data protection regulation compliance and litigation and arbitration on privacy-related issues. LCA regularly organises seminars and conferences on data protection and cybersecurity issues.

Authors

Gianluca De Cristofaro is a partner and co-head of the Intellectual Property & Data Protection department. His practice covers data protection and cybersecurity, information technology and internet law and misleading and comparative advertising. He has extensive experience in consultancy and litigation regarding data protection matters and he assists clients in complex cybersecurity projects. Together with the other members of the IT Group, he is currently involved in assisting Italian and multinational companies in the compliance process to the new European General Data Protection Regulation (No 679/2016), e-commerce projects and e-payment deals at both contentious and non-contentious level.

Chiara Bocchi is an associate specialising in privacy and personal data protection and litigation, arbitration & ADR. She assists data controllers on both ordinary privacy fulfilments and on the implementation of new and ground-breaking processing activities, assessing their impact on data protection and working with the Supervisory Authority, drafting the due compliance documents and advising on the implementation of appropriate technical and organisational security measures. She is directly involved in the implementation process of Regulation (EU) 2016/679 (so-called "GDPR") of many international group of companies and, in this context, in the approval process of Binding Corporate Rules as appropriate safeguard to the transfer of personal data to third countries. She is a member of the International Association of Privacy Professionals (IAPP) and holds the Certified Information Privacy Professional/Europe (CIPP/E) certificate.

1. Basic National Legal Regime

1.1 Laws

As regards personal data protection and cybersecurity, Italy's main law is the Personal Data Protection Code or Privacy Code (Legislative Decree No 196 of 30 June 2003: Codice in materia di protezione dei dati personali o Codice Privacy), which constitutes the transposition of directive 95/46/EC and directive 2002/58/EC, and repeals Law No 675 of 31 December 1996 (the very first Italian data protection law). The Privacy Code is the consolidated statute on both data protection and cybersecurity, and it is complemented by guidelines, recommendations, orders and codes of conduct issued and approved by the Italian Personal Data Protection Authority (referred to as Garante per la protezione dei dati personali or Garante).

In addition, and prior to, the Privacy Code, the Constitution of the Italian Republic (which lists all fundamental principles governing Italy) also provides for personal data protection: namely Article 2, stating that: "The Republic recognises and guarantees the inviolable rights of the person, as an individual and in the social groups where human personality is expressed." Moreover, Article 15 expressly qualifies as inviolable: "The freedom and confidentiality of correspondence and of every other form of communication," thus including electronic communication. General principles applying to data protection can also be found in the European Convention on Human Rights adopted by the European Court of Human Rights (namely Article 8, granting the right to respect for private and family life) and in the Charter of Fundamental Rights of the European Union (Article 7 concerns family life, whereas Article 8 expressly addresses everyone's right to protection of personal data); moreover, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the so-called "Convention 108") of the Council of Europe shall also be mentioned.

A number of other national laws may address specific categories of personal data, adding requirements for lawful processing. For instance: the processing of portrait photos is subject to both the Privacy Code and Copyright Law (ieLaw No 633 of 22 April 1941); video surveillance systems have to comply with both the Privacy Code and the so-called Statuto

dei Lavoratori or Workers' Statute (ie Law No 300 of 20 May 1970).

Save for the above, the basic principles governing personal data processing are found under Sections 3 and 11 of the Privacy Code. According to such principles, personal data shall be:

- processed lawfully and fairly (lawfulness and fairness);
- collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes (purpose limitation);
- accurate and, when necessary, kept up to date (accuracy);
- relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed (proportionality);
- limited to cases in which the purpose sought cannot be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in the case of necessity (data minimisation); and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (limited storage period).

Data subjects shall, in any case, be informed of the main features of the processing, prior to processing; if personal data is not collected directly from data subjects, an information notice shall be given at the time of recording such data or, if their communication is envisaged, no later than when the data is first communicated. Such information shall include, inter alia: the identity and the contact details of the controller; the purposes of the processing; the obligatory or voluntary nature of providing the requested data, and the consequences in the event of refusal; the recipients or categories of recipients of the personal data, and the scope of dissemination; the transfer of personal data to a third country; and a brief description of the rights granted to data subjects according to the applicable data protection laws.

The legal basis for processing is, in most cases, the consent of a data subject: however, the consent might not be necessary where any other lawful basis for processing applies (ie if the processing is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract).

Data controllers shall further process personal data in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Data processors, if any, shall be duly appointed in writing and given instructions by the data controller.

1.2 Regulators

The Garante is the main authority in charge of verifying whether data processing operations are carried out in compliance with the laws and regulations in force. Such tasks shall be discharged, inter alia, by: asking data controllers, data processors, data subjects or third parties to provide information and produce documents; ordering data controllers or data processors to adopt such measures as are necessary or appropriate; prohibiting unlawful or unfair data processing operations, in whole or in part, or blocking such processing operations, and taking other measures as provided for by the legislation applying to the processing of personal data; giving opinions whenever required; and preferring information on facts and/or circumstances amounting to offences to be prosecuted ex officio, which it has come to know either in discharging or on account of its duties.

The Garante shall act either ex officio, or after receipts of reports and complaints lodged by other data subjects or the associations representing them. Investigations shall be carried out both through requests for information and documents and through access to data banks and performance of audits on the spot as regards premises where the processing takes place. The Privacy Unit of the Financial Police is the public authority that usually conducts such inspections on behalf of the Garante.

A plan of the future activities of the Garante is issued on a yearly basis: this document states the business field on which the investigations of the Garante are mainly focused in the relevant period.

1.3 Administration Process

Data subjects may apply to the Garante to point out an infringement of the relevant provisions on the processing of personal data; to call for a check on the mentioned provisions; or to lodge a complaint with a view to establishing the specific rights granted to data subjects by the applicable data protection law.

Any claim concerning data protection shall also be filed, alternatively and not cumulatively, to the civil courts (save for the fact that infringement of data protection provisions might result also in criminal offences). The two remedies differ in that: proceedings in front of the Garante do not require any formality, but the Garante is not entitled to provide for monetary compensation for damages; judicial proceedings have no fixed term, whereas the term provided to the Garante is 60 days from the date on which the complaint was lodged, to be extended by no more than 40 additional days if the enquiries are especially complex or the parties agree thereto (and, if no decision on the complaint is rendered within such a term, the complaint shall be regarded as dismissed).

A complaint filed to the Garante shall refer, with as many details as possible, to the facts and circumstances on which it is grounded; the date of the request made to the data controller; the remedies sought as well as to the identification data concerning the data controller and claimant; and the domicile of choice for the purposes of the relevant proceedings, including the address where communications shall be served. Any documents that may be helpful in evaluating the complaint must also be attached to it.

The Garante shall be responsible for communicating the complaint to the data controller within three days. The data controller may notify both the complainant and the Garante within ten days that he or she will voluntarily comply and, in this case, a declaration of no case to answer shall be returned. The data controller and the data subject have the right to be heard and submit pleadings or documents.

The Garante may order, also ex officio, that one or more expert assessments are carried out.

Measures taken following a complaint (or ex officio) shall include: the partial or total blocking of some of the data (also provisional, during proceedings), or the immediate termination of one or more processing operations; the order that the data controller abstain from unlawful conduct; and further remedies to enforce the data subject's rights and set a term for their implementation.

The decision may be challenged by the data controller or the data subject, as the case may be, by filing a petition to the judicial authority. Challenging shall not suspend enforcement of the decision.

1.4 Multilateral and Subnational Issues

Personal data protection has a high importance in the European Union (EU): aiming to grant the same level of personal data protection in the whole EU, national laws have been, at first, harmonised through Directive 95/46/EC and Directive 2002/58/EC, and then standardised, through the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the so-called General Data Protection Regulation or GDPR). The GDPR is binding and applicable as of 25 May 2016, but it becomes enforceable from 25 May 2018 after a two-year transition period.

Being a member of the EU, Italy shall abide by European regulations and directives and shall disapply any national laws inconsistent with EU rules and principles: this is why the Privacy Code is the transposition of Directive 95/46/EC and Directive 2002/58/EC, and this is why the Italian Government has been put in charge of the task of amending the Privacy Code in compliance with the new rules.

The Garante is used to issue guidelines, orders and measures (such as general authorisations) to clarify the scope of application of the Privacy Code and to supplement the same: such acts are published in Italy's Official Journal, and therefore have a regulatory nature.

Data controllers and data processors have to comply with the same and their application might be enforced either ex officio or on data subjects' instance.

1.5 Major NGOs and Self-Regulatory Organisations

Among non-governmental organisations (NGOs), Federprivacy (Federazione Italiana Privacy or Italian Privacy Federation) must be mentioned. This association gathers privacy professionals and provides training on privacy issues.

Collective organisations representing specific categories of individuals for general purposes may draft codes of conduct, to be approved by the Garante.

1.6 System Characteristics

Italy is highly regulated, due to the fact that it follows the EU model: European systems are more developed than non-EU countries.

Compared to other Supervisory Authorities, the Garante is one of the most active in verifying and ensuring the compliance to data protection rules and principles.

1.7 Key Developments

In the last few months, no key developments have occurred in Italian national law or in the regulation field.

As anticipated, on 25 May 2018 the GDPR entered into full force and effect: this means that, by this date, any EU Member State must have implemented due measures to ensure the effectiveness of the new rules, either by disapplying any non-consistent national law, or adopting any necessary new laws.

Ever since the adoption of the GDPR, Supervisory Authorities on a national level, and Article 29 Working Party (ie a group bringing together representatives of Supervisory Authorities of all EU Member States, as well as of the European Data Protection Supervisor and the European Commission; according to the GDPR, the Article 29 Working Party is going to be substituted by the European Data Protection Board) on a European level, have committed to ensuring the effective implementation of these issuing guidelines to data controllers and data processors to help with understanding and applying the new rules. The guidelines adopted so far by the Article 29 Working Party concern the right to data portability, data protection officers (DPOs), data protection impact assessments, the Lead Supervisory Authority, the application and setting of administrative fines, data breach

notification and automated individual decision-making and profiling. Further guidelines have been drafted, but not yet adopted, and concern transparency, consent and adequacy referential.

In addition to guidelines concerning the GDPR, the Article 29 Working Party "Opinion 2/2017 on data processing at work" issued on 8 June 2017 has to be mentioned. Among other relevant issues, this document directs data controllers' attention to the fact that employees' consent is highly unlikely to be a legal basis for data processing at work, unless employees can effectively refuse without adverse consequences: indeed, employees are seldom in a position to give, refuse or revoke consent freely, given the dependency inherent in the employer/employee relationship.

As far as the transfer of personal data to non-EU Member States is concerned, in October 2017 the Irish Judges asked the European Court of Justice for a preliminary ruling on whether to strike down the data transfer mechanism used by Facebook (as well as by other tech groups) to transfer personal data of Facebook's European users to the United States, ie the so-called "standard contractual clauses": the awaited decision is going to have a huge impact on the legitimate grounds for data transfers among companies that are part of the same group.

1.8 Significant Pending Changes, Hot Topics and Issues

On 25 October 2017, with Law No 163, the Italian Government was put in charge of amending – within six months – the Privacy Code as necessary to be consistent with the GDPR, in particular: repealing what is inconsistent with the new rules; co-ordinating the existing provisions with the GDPR; updating the Privacy Code to execute the provisions of the GDPR that are not directly applicable; and adjusting the penalty system. The Garante shall also issue any due decision to execute the GDPR properly.

At the end of January 2018, the European Commission issued its guidance on direct application of the GDPR (addressed mainly to citizens, business and organisations) and warned Italy: the concern was that Italy would not duly (ie by 25 May 2018) implement the GDPR in a timely manner.

The general principles governing data protection in the GDPR are basically the same as in the Privacy Code, with a higher attention to data controllers' accountability: therefore, no material changes are awaited.

This assumption has been confirmed by the Garante in its very first operative guide for the application of the GDPR: it is for this reason that most of the orders, guidelines and measures issued so far are likely to remain applicable; and it is for the same reason that the category of persons in charge of the processing, ie the natural persons that have been authorised by the data controller or processor to carry out processing operations (incaricati del trattamento), have already been confirmed. It must be noted that persons in charge of the processing are a peculiarity of the Italian system only, since their category has been added by Italian legislators to those of "data controllers" and "data processors" while transposing directive 95/46/EC (in other EU Member States, the category of "data processors" includes that of "persons in charge of the processing").

The Garante will issue draft agreements with data processors and joint controllers, and a formal repeal of the duty to notify certain processing operations is also awaited. Clarifications on the role of DPOs have been issued only regarding the public sector, with a draft appointment agreement as well.

The GDPR has been adopted together with "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA". This directive was to be transposed by 6 May 2018: the consequent amendments to the Privacy Code will affect Articles 53-58, concerning processing by the police and state defence and security.

As far as Italian national law is concerned, the so-called Registro delle Opposizioni (Opt-Out Register) was amended with Law No 5 on 11 January 2018 – effective from 4 February 2018. This register collects, on a voluntary basis, data subjects' telephone numbers in case data subjects do not want their data processed for direct marketing or advertising purposes, or else for carrying out market surveys or interactive business communication. The main changes concern the possibility to include not only phone numbers, but also mobile numbers and, in both cases, irrespective of them being contained in publicly available paper or electronic directories, and the duty of data controllers to check, at least once a month, whether phone and mobile numbers have been included in the register, since a subsequent inclusion serves as waiver of the consent to processing.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Neither privacy officers nor DPOs are ruled under the Privacy Code: as far as Italy is concerned, such roles are some of the most relevant news introduced by the GDPR (whereas the national laws of some EU Member States already provide for DPOs).

Privacy officers' and DPOs' tasks are currently performed – in Italy – either by data controllers or data processors (such as external consultants): no special requirements are therefore needed to cover such roles, provided that they are in all cases selected among entities that can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing and also related to security matters. Amendments are going to be introduced while adopting the necessary measures to ensure consistency of Italian national law to the GDPR.

According to European regulation, DPOs shall own expert knowledge of data protection law and practices, shall be able to fulfil the tasks of providing advice and monitoring compliance to data protection laws, and shall be bound by a duty of confidentiality. DPOs may either be staff members of the controller or processor, or be third-party providers acting on the basis of a service contract: in both cases, they shall be independent (iethey shall not receive any instructions regarding the exercise of their tasks, and shall not be dismissed or penalised by the controller or the processor for performing the same tasks) and report directly to the highest management level of the controller or the processor and, while they might perform other tasks and duties, they shall in all cases avoid any conflicts of interest. It shall be noted that a group of undertakings might appoint just one DPO, provided that it is easily accessible by each member entity.

The appointment of a DPO is compulsory in just three cases: the processing is carried out by a public authority or body; the core activities of the controller or the processor consist of processing operations requiring regular and systematic monitoring of data subjects on a large scale; the core activities of the controller or the processor consist of processing on a large scale of sensitive data or judicial data. The contact details of the appointed DPO shall be communicated to the Supervisory Authority.

The Article 29 Working Party, in its "Guidelines on Data Protection Officers (DPOs)" of 13 December 2016 as revised on 15 April 2017, recommended the appointment of DPOs in general, both as good practice and as proof of the data controllers' or data processors' accountability. The Garante seems to agree with this recommendation.

The Privacy Code requires data controllers to ensure a minimum level of data protection, adopting at least the minimum security measures listed under its Annex B.

Unlike the Privacy Code, the GDPR does not force the adoption of minimum security measures: privileging an accountability-based approach, it requires data controllers and data processors to identify and implement appropriate technical and organisational measures in order to ensure a level of data protection appropriate to the risks for personal data, both at the time of determination of the means for processing (privacy by design) and at the time of the processing itself (privacy by default), taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as all the risks for the rights and freedoms of individuals. In this new framework, Annex B (if and when not repealed) shall just be a guideline for the Garante to issue codes of conduct and best practices, and it will not represent any kind of checklist for the minimum level of protection to be ensured.

The duty to conduct privacy impact analyses is a new requirement introduced by the GDPR.

The Privacy Code provided for the so-called Documento Programmatico sulla Sicurezza or DPS (ie Security Policy Document), which – in brief – was constituted by a description of processing activities and an assessment of the related risks for data subjects, and had to be drafted (and updated yearly by March 31st) by each and every data controller processing personal data with electronic means. The duty to draft, and keep updated, the DPS was repealed in 2012 when this document became optional (save for the fact that data controllers shall always assess the risks related to the processing being carried out, which is necessary in order to ensure the identification and the consequent adoption of due security measures).

In some ways, the GDPR has reintroduced the duty to carry out the DPS: indeed, it requires the adoption of both records of processing activities and data protection impact assessments.

As to records of processing activities, they are not compulsory for enterprises or organisations employing fewer than 250 persons unless the processing carried out is likely to result in a risk to the rights and freedoms of data subjects; the processing is not occasional, or the processing includes sensitive data or judicial data. Nevertheless, the Garante has already suggested that each and every data controller and data processor maintain records of processing activities in any case, as proof of their commitment to an effective protection of personal data.

The information to be included in records of processing activities are the main features of the processing, ie name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organisations; transfers of personal data to a third country or an international organi-

sation and the safeguards thereto; the retention periods of the different categories of data; and a general description of the technical and organisational security measures in place.

As to privacy impact analyses, the GDPR provides for assessments of the impact of the envisaged processing operations on the protection of personal data (data processing impact assessments or DPIAs) to be conducted by data controllers prior to processing, where that type of processing is likely to result in a high risk to the rights and freedoms of natural persons. DPIAs are compulsory in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects; processing on a large scale of sensitive data and judicial data; and a systematic monitoring of a publicly accessible area on a large scale. Supervisory Authorities are expressly empowered to extend or reduce this list.

DPIAs shall include, at least: a description of the processing and the relevant purposes; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects; and the security measures to address the risks.

The Article 29 Working Party has recently issued guidelines on DPIAs ("Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679" adopted on 4 April 2017 as last revised and adopted on 4 October 2017) to help data controllers and data processors in understanding when DPIAs are needed and how to conduct them. When in doubt about whether to carry out a DPIA, the advice is to proceed.

Data subjects shall in all cases be duly informed – in an intelligible format – of the features of the processing at the time when personal data is obtained; where the data is not collected directly from data subjects, the information is due at the time of recording that data or, if their communication is envisaged, no later than when the data are first communicated. According to the GDPR, the information shall be given, at the latest, within one month from collection of the personal data.

The information to be provided shall include: the identity and the contact details of the controller; the purposes and the modalities of the processing; the obligatory or voluntary nature of providing the requested data, and the consequences in the event of refusal; the recipients or categories of recipients of the personal data, and the scope of dissemination (if any); the transfer of personal data to third countries; and a brief description of the rights granted to data subjects according to the applicable data protection laws.

The GDPR adds further compulsory information, such as the legal basis for the processing and the period for which the personal data will be stored. Such features of the processing, although not to be provided to data subjects under the Privacy Code, were nevertheless to be duly taken into account due to the need to comply with general data protection principles.

Any privacy policy shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It used to be either oral or written (as it would have been much easier to prove that it was actually provided if it was written down or otherwise recorded) but the GDPR requires, as a condition precedent to an oral privacy policy, the specific request of the data subject and that the identity of the data subject is proven by other means. The GDPR also allows the provision of privacy policies in combination with standardised icons (not yet issued), which are supposed to ensure an easily visible, intelligible and clearly legible overview of the intended processing.

It must be noted that any news introduced by the GDPR to the privacy policy is consistent with the Privacy Code.

Data subjects shall always, at any time, exercise the rights granted under the applicable data protection law, including the rights to access their personal data and to have the same data corrected or deleted.

Any request shall be issued to the relevant data controller, and will not be subject to any formalities; a standard form is published on the website of the Garante, for a data subjects' convenience.

Data controllers shall not unreasonably refuse to act on the request of data subjects for exercising their rights, and shall reply without undue delay and, in any case, within 15 days of receipt of the request; this term may be extended up to one month (or three months, according to the GDPR) taking into account the complexity of the request and, in the event of no reply, data subjects shall be entitled to lodge a complaint to the judicial authority.

Information and actions to data subjects shall be free of charge, unless data subjects' requests are manifestly ungrounded (iethe data controller does not own any personal data of the requesting data subject): in such cases, the controller may charge a reasonable fee, taking into account the costs actually incurred for the enquiries made in the specific case.

It has to be noted that any news introduced by the GDPR to the rights granted to data subjects appears to be consistent with the Privacy Code.

The use of personal data and identification data shall be minimised in such a way as to rule out their processing if legitimate purposes can be achieved by using either anonymous data or suitable arrangements to allow the identifying of data subjects only in cases of necessity.

Anonymisation, de-identification and pseudonymisation may also be, on a case-by-case basis, adequate security measures and appropriate safeguards to be implemented to ensure protection of personal data: for instance, pseudonymisation combined with encryption can reduce the likelihood of individuals being identified in the event of a breach and, therefore, the need to notify the breach to data subjects according to the GDPR.

In the case of a breach of personal data protection laws, data subjects may suffer damages and they shall be entitled to compensation under Article 15 of the Privacy Code (and Article 82 of the GDPR), reverting to Article 2050 of the Italian Civil Code: this last rule provides compensation for damages which have occurred under "hazardous activities," thus leading to the inference that processing shall be deemed a hazardous activity.

The damages shall be either material or non-material. As to non-material damages, no classification is required: according to Italian case law, any possible category of non-material damages (ie reputational, emotional, embarrassment, etc) is just a description, since non-material damages are and shall remain unitary and subject to no duplication due to the use of different names.

2.2 Sectoral Issues

Sensitive data means personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life.

Under the GDPR, sensitive data is addressed as "special categories of personal data", and also expressly includes genetic data and biometric data processed for the purpose of uniquely identifying a natural person.

Under the Privacy Code, sensitive data shall be processed only with both Garante's prior authorisation and a data subject's prior consent. The consent shall be given freely and specifically with regard to a clearly identified processing operation, and shall be given in writing (whereas the consent for the processing of personal data, when needed, might just be documented in writing). The same safeguards apply to genetic data: although not expressly included among sensitive data, they are granted the same highest protection due to their eligibility to reveal sensitive issues of individuals (and, in addition, a prior notification is always required).

Neither the authorisation nor the consent is necessary in particular circumstances, such as: data contained in CVs sent on a voluntary basis; the data of members of religious denominations and entities having regular contact with those denominations for exclusively religious purposes; and data concerning the affiliation of trade unions and/or trade associations.

Consent shall not be necessary in the case of processing that is: necessary to comply with specific obligations and/or tasks laid down by laws, regulations or European legislation in the employment context; necessary to protect a third party's life or bodily integrity; necessary for carrying out the investigations by defence counsel, or else to establish or defend a legal claim, provided that the data is processed exclusively for those purposes and therefore for no longer than is necessary; carried out for lawful purposes by not-for-profit associations, bodies or organisations of a political, philosophical, religious or trade-unionist nature, with regard to personal data concerning members and/or entities having regular contacts with those associations, bodies or organisations.

In all the aforementioned cases, save for the fact that no consent on the part of the data subject is required, the Garante's authorisation remains compulsory. To ease data controllers' tasks and duties, the Garante is used to issue general authorisations on a yearly basis to the processing of sensitive data (an example of general authorisation is the one issued for the processing of sensitive data in the employment context) and of genetic data: where the processing complies with that general authorisation, no need for an ad hoc authorisation will arise.

The GDPR, unlike the Privacy Code, does not require any prior authorisation from the Supervisory Authority, but prohibits the processing of sensitive data (addressed as "special categories of personal data") except for in the following circumstances: the data subjects gave consent; the processing is necessary to execute an employment relationship (including the assessment of the working capacity of the employee), for medical diagnosis, for the provision of health or social care or treatment or the management of health or social care systems and services, for reasons of public interest in the area of public health, or to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; the processing is necessary for reasons of substantial public interest, on the basis of union or Member State law; the processing relates to personal data which is manifestly made public by the data subject; the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; the processing is carried

out in the course of its legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed to third parties without the consent of the data subjects.

According to the GDPR, the processing of sensitive data also requires the maintenance of records of processing activities and, when on a large scale, data protection impact assessments as well as the appointment of a DPO. EU Member States are expressly empowered by the GDPR to introduce further conditions, including limitations, with regard to the processing of genetic, biometric and health data: this may lead to a confirmation of the need of Garante's prior authorisation to the processing.

Financial Data
Financial data, as long as it allows the identification of data subjects, is considered personal data.

Guidelines were adopted in 2007 by the Garante for the processing of customers' data in the banking sector. This document is mainly focused on ensuring that personal data is not unlawfully communicated to third parties (ie because phone calls or interviews have been conducted in an inappropriately loud voice in the presence of third parties; because no measures have been deployed to prevent third parties from being apprised of personal information, including appropriate waiting lines in the areas intended for the performance of banking operations; or because banking information has been communicated to third parties that had not been authorised by the data subject to carry out operations on their behalf).

It should be noted that certain communications of financial data are mandatory under Italian law, for instance for the purpose of anti-money laundering (which requires the processing of information related not only to individual banking operations, but also to a wider amount of personal data insofar as they are necessary to detect abnormal/unusual operations), for countering terrorism by financial means and for taxation offences, or to the credit bureau managed by the Bank of Italy (Banca d'Italia). Further communications may be due also to judicial authorities in pursuance of the law and/or to creditors in connection with enforcement proceedings, or following requests for access to banking documents; additionally, the "negative" personal information required to carry out processing operations in pursuance of the "Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments" (adopted by the Garante in 2004) may be communicated to the managers of private credit reference agencies.

Health Data
Health data is sensitive data: therefore, it is subject to special safeguards provided for this category of data.

The Privacy Code grants simplified arrangements to public and private healthcare bodies to inform data subjects, to collect the relevant consent and for the processing of personal data. As to sensitive data, simplifications consist of the processing being allowed with the data subject's consent, also without the Garante's authorisation, if the processing concerns data and operations that are indispensable to safeguard the data subjects' bodily integrity and health; and for this same purpose but without the data subject's consent, based on the Garante's prior authorisation, if the processing concerns either a third party or the community as a whole. Security measures are also addressed, recommending the adoption of solutions aimed at: respecting precedence and order in calling up data subjects, setting up appropriately spaced waiting lines by having regard to the use of voice, messages and/or barriers, and preventing third parties from unduly getting to know information disclosing health during an interview; implementing procedures, including training of staff, to prevent third parties from establishing a link between a data subject and a given ward or department and, generally speaking, ensuring medical care activities – including collection of a patient's history – from being carried out in privacy-unfriendly situations due to the specific arrangements and/or the premises selected.

Guidelines have been adopted by the Garante to address particular cases:

- "Guidelines on electronical medial dossiers" in 2015 which focuses on security measures to ensure protection of personal data and provides for the duty to notify any data breach within 48 hours from discovery);
- "Guidelines on Online Examination Records" in 2009;
- "Guidelines on the Electronic Health Record and the Health File" in 2009;
- "Guidelines on processing personal data for dissemination and publication on exclusively health-related websites" in 2012 which addresses the managers of websites that deal exclusively with health-related issues, such as specific forums, blogs and social networks dealing with health-related issues via ad hoc profiles that may be created by private entities for raising awareness and/or exchanging views, as addressed merely in the context of disseminating knowledge of and popularising such issues);
- "Guidelines on processing personal data to perform customer satisfaction surveys in the healthcare sector" in 2011 (clarifying that sensitive data shall be processed as long as the processing of anonymous data does not allow the sur-

vey to achieve the respective purpose and the medical data is indispensable to achieve that purpose); and
- "Guidelines for Data Processing within the framework of clinical drug trials" in 2008.

A brand new rule of law (Law No 167 of 20 November 2017) also has to be noted: it allows the communication of health data to multinationals, in aggregate (ie anonymous) form and subject to Garante's prior authorisation, for research and statistical purposes. Concerns have been raised, but not by the Garante which believes that data subjects' protection is properly ensured.

Communications Data
Text messaging might be used to send marketing communications but only with a data subject's prior consent.

It should be noted that the consent - if any - to receive marketing communications via automated calling or further systems without human intervention (iefax, SMS, e-mail, MMS, recorded calls) includes the consent to receive marketing communications via traditional means (iepaper mail), but not vice versa.

Soft spam exemptions do not apply to the processing of phone numbers: therefore, a phone number collected in the context of the sale of a product or service shall not be processed for direct marketing of a data controller's own products or services without the data subject's consent.

Special provisions apply to providers of call centre services (either directly or through third parties), for both inbound and outbound calls: the customer shall be informed of the country in which the call centre operator is located; when the call centre's operators are located outside the EU, a prior notice shall be delivered to the Garante (as well as to the Ministry of Labour or Ministro del Lavoro e delle Politiche Sociali, the National Labour Inspectorate or Ispettorato Nazionale del Lavoro and the Ministry of Economic Development or Ministero dello Sviluppo Economico) and the customer shall be granted the opportunity to choose to communicate with operators located in Italy or within the EU by an immediate forward of the call.

All call-centre providers must also be enrolled in the Registro degli Operatori di Comunicazione or ROC (Register of Communication Operators) managed by AGCOM (Autorità per le Garanzie nelle Comunicazioni or Supervisory Authority for Communications). In addition, pursuant to Law 5 on 11 January 2018, providers of call centre services shall update their phone numbers using the prefixes that will be indicated by AGCOM: the aim is ensuring that data subjects are easily able to identify calls dialled for statistical purposes or for marketing purposes.

Internet
It is highly unlikely that no personal data is collected through a website (at least all websites have a "contact us" section), therefore a privacy policy is compulsory. In order to be effective, it must be easily accessible from each section of the website.

An information notice concerning cookies (technical, analytic and/or profiling cookies) must also be provided: its form and contents are described further in this document.

According to Legislative Decree No 70 of 9 April 2003 (transposing directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market - Directive on electronic commerce), a website must also clearly state the identification and contact data of its owner.

The same provisions are also deemed applicable to mobile applications. The relevant privacy policy shall also be available on the marketplace (ie it shall be readable before downloading the app).

Tracking cookies, or profiling cookies, shall be installed provided that website users: i) have been properly informed thereon, both with an initial "short" notice in an overlay banner on the home page (or on any other landing page) and with an "extended" notice to be accessed via a clickable hyperlink and from every website page; and ii) have granted their consent, either expressly by accepting the use of such cookies or implicitly by continuing to use the website.

More precisely, the short information notice to be provided via the home page banner shall include: a statement that the website uses profiling cookies to send advertising messages in line with the user's online navigation preferences; a statement that the website allows sending third-party cookies as well, if any; a clickable link to the extended information notice, where information on technical, profiling and analytics cookies must be provided along with tools to select the cookies to be enabled; a statement that, in the extended information notice, the user may refuse to consent to the installation of cookies and that, if the user continues browsing by accessing any other section or selecting any item on the website (ie by clicking a picture or a link), he or she consents to the use of cookies.

The home page banner containing this short information notice shall be of a sufficient size to be easily readable. It must also give rise to a discontinuity in the browsing experience: the banner shall only cease being displayed if the user takes action by selecting any item on the page underneath the banner, or by clicking on the banner itself expressly to accept cookies. The short information notice might not be

displayed in the case of further visits by the same user: this shall be without prejudice to the user's right to refuse consent and/or change the relevant cookie options at any time.

A prior notification to the Garante of the use of profiling cookies is due and must be forwarded directly by the publisher, unless tracking cookies are provided by third parties: in this latter case, these third parties are the ones bound to file the notification. It should be noted that the duty to notify this, and other processing, to the Garante should be abolished by the GDPR; however, a brand new law (ie Law No 205 of 27 December 2017, effective from 1 January 2018) introduced a new notification obligation for data controllers processing personal data through automated means or new technologies on the basis of a legitimate interest, and such processing is subject to the prior check of the Garante.

Data subjects' consent is required not only for tracking cookies, but also for analytics provided by third parties. More precisely, analytics cookies are assimilated to profiling cookies (therefore, a double-layered privacy policy and a notification to the Garante are also needed) if no measure to reduce cookies' identifying ability is implemented and if the third party matches the information collected via cookies with other information already owned.

It is important to keep track of users' consent: to this end, an ad hoc technical cookie might be used since it is not deemed as privacy-intrusive.

As far as technical cookies are concerned, the provision of a cookie policy is sufficient (ie no banner, notification and/or consent are required).

Video and Television

As far as video and television is concerned, the Garante has focused on data protection issues concerning interactive television services, recommending that data controllers: give data subjects clear, easy-to-understand and exhaustive information on all the features of the processing (also through a first, "short" notice giving access to a second, "long" notice if a data subject wishes to have more details); collect data subjects' consent for marketing and profiling purposes (if any), as well as for the communication of data to third parties; and implement adequate security measures to ensure effective protection.

Social Media, Search Engines, Large Online Platforms

No ad hoc regulation is in place concerning social media, search engines and large online platforms: it might be said that this field is self-regulated, being mainly based on codes of conduct adopted by providers themselves. An exception is the already mentioned Legislative Decree No 70 of 9 April 2003, which is mainly focused on the responsibility of contents providers for users' content. General rules of law, such as the Privacy Code and criminal provisions, shall also apply.

The Garante has addressed the topic on several occasions, recommending that providers implement adequate security measures but focusing mostly on the attempt to increase data subjects' awareness of the risks of communicating personal data to social networks. Such risks are related to the unavoidable dissemination of data published on the internet and to the consequent difficulty of an effective deletion: no social network account is actually completely private, and acts of third-party users cannot be provided for.

The Privacy Code entitles data subjects to have, at any time, their personal data deleted when processed unlawfully and to object, on legitimate grounds, to the processing of their personal data even though it is relevant to the purpose of the collection: these are deemed the grounds of the right to be forgotten, ie the right to obtain the de-listing of links to web pages published by third parties containing information relating to them from the list of results displayed following a search made on the basis of a person's name. In brief: the right not to be publicly reminded long after the relevant event.

The right to be forgotten has always been acknowledged and granted by Supervisory Authorities and national courts, as well as by the European Court of Justice. Reference shall be made, inter alia, to the so-called "Google Spain Case" (C-131/12) which, after recognising that search engine operators process personal data and do it as controllers, highlighted that: "[…] it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question." The Article 29 Working Party issued guidelines on the interpretation of this decision (which were adopted on 26 November 2014).

These principles are also commonly applied by the Garante in the balance of an individual's right to be forgotten with the public interest to be duly informed. In a very recent decision, the Garante requested Google to delete, from the list of search results by name, an article referencing a criminal conviction, since the data subject had meanwhile been reinstated and the news was outdated. On the contrary, the Garante has confirmed the lawfulness of search results that, although referring to the same legal case, provide further information of actual public interest also in light of the role of the data subject, who is still holding high-level public office.

The GDPR expressly rules the right to be forgotten. When grants to data subjects to have their personal data erased and no longer processed (except if further retention is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation, for reasons of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims) and, where the personal data was made public, it forces the data controller to take any reasonable steps to inform other controllers who are processing the same personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, that personal data.

Hate speech and abusive material are addressed both by data protection laws and criminal laws.

A special law has recently been adopted concerning cyberbullying: it is Law No 71 of 29 May 2017, which grants to persons below 18 years of age the right to obtain erasure of defamatory online contents from a website and/or social network concerned within 24 hours from the request. It should be noted that the purpose of this law is to prevent, rather than to repress, acts of cyberbullying, and this aim is pursued through proper school education.

As to disinformation, the Garante is currently fighting against fake news by incrementing users' awareness.

The right to data portability is properly ruled under the GDPR, being new to Italy. It is defined as a data subject's right: i) to receive personal data previously provided to a controller in a structured, commonly used and machine-readable format, and to store that data for further personal use (without necessarily transmitting the data to another data controller); and ii) to transmit that data to another controller.

The right to data portability shall be exercised when the processing is based on a data subject's consent, or on a contract to which the data subject is a party, and it is carried out through automated means; moreover, it will concern just the personal data of the requesting data subject (which do not concern other data subjects) which has been knowingly and actively provided to the controller by the data subject itself, also by virtue of the use of a service or a device (ie a person's search history, traffic data and location data, or other data such as the heartbeat tracked by a wearable device). Consequently, inferred data and derived data created by a data controller on the basis of the data provided by a data subject are excluded from the scope of the right to data portability.

This right shall be exercised without prejudice to any other right granted to data subjects according to the applicable data protection law: therefore, data subjects can continue to use and benefit from the data controller's service even after a data portability operation, also because data portability does not automatically imply the erasure of the data.

These and further issues on the right to data portability are addressed in the "Guidelines on the right to data portability" as adopted on 13 December 2016, and as last revised and adopted on 5 April 2017 by the Article 29 Working Party.

A case involving Facebook (discussed in 2016) must be mentioned, being the Garante's first decision towards the social network and the one in which the Garante confirmed that it is empowered to protect individuals' personal data processed by Facebook.

The claim concerned a fake Facebook account. The Garante ordered the social network: i) to inform the data subject whose data was unlawfully processed by the fake account of the personal data that concerned him, as well as the source of the personal data, the purposes and methods of the processing, the identification data concerning the data controller, data processors and the entities to which the data had been communicated; and ii) to cease any further processing of the data provided to the social network by the fake account, and to store those already used to enable the due investigations by the public authority. Facebook also had to notify the Garante of the remedial actions that would be implemented.

Children's Privacy

According to Italian law, persons below 18 years of age need to act under their parents' authorisation (or that of whoever holds parental responsibility): therefore, any consent to processing of children's data shall be obtained from whomever has the relevant parental responsibility.

The GDPR lowers the threshold to 16 years of age, at least as far as the offer of information society services is concerned. Data controllers are required to make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration the available technology.

Generally speaking, schools and educational institutions are bound by a duty of publicity and transparency: for example, examination marks and results of state exams are public data, and data concerning academic performance shall be communicated and disseminated subject to the guidelines of the Ministry of Education or Ministero dell'Istruzione, dell'Università e della Ricerca. To help in complying with both the duty of transparency and the duty to ensure data protection, the Garante issued the guide "Privacy-Proof School" in 2016, and the "Guidelines on processing of personal data included in administrative acts and documents by public bodies for purposes of publication and diffusion on the web" in 2011.

The Privacy Code provides special provisions, which aim to facilitate vocational orientation and training as well as employment in Italy and abroad, allowing high schools and similar educational bodies to communicate or disseminate data on the evaluation and marks obtained by students (whether at mid-term or in the final term), and further personal data other than sensitive or judicial data, also to private entities and by electronic means, upon the data subjects' request, provided that such data is relevant in respect of the mentioned purposes and that data subjects have been duly informed thereon.

2.3 Online Marketing

Commercial and marketing communications might be sent only upon a data subject's prior consent: the possibility to ground marketing on a different legal basis for the processing (such as, for instance, the need to perform obligations resulting from a contract to which the data subject is a party, or to comply with specific requests made by the data subject prior to entering into a contract) is remote. Guidelines are still to come from the Article 29 Working Party on the interpretation of "legitimate interest of the controller": according to the GDPR (see recital 47), the legitimate interest of the controller might be a suitable basis for the processing of personal data for marketing purposes, thus excluding the need to collect data subjects' consent.

The consent is deemed to be effective: if it is given freely (needless to say that the consent is not free when the consent check box is pre-flagged) and specifically with regard to a clearly identified processing operation; if it is documented in writing; and provided that data subjects are aware of all the relevant details of the processing (the contents of the privacy policy have been discussed above).

A separate consent is required for each purpose being sought and for each processing operation at issue: therefore, a specific consent shall be collected for marketing, profiling, and disclosure of the data to third parties, which shall be clearly identified either by name or business or commodity category. It shall be noted that the definition of "marketing" includes advertising materials, direct selling, performance of market surveys and commercial communications, since all these aims are mostly instrumental to the achievement of a single purpose (ie the marketing purpose), but it does not include either profiling or behavioural advertising.

The information notice and consent request must clearly also identify the means of delivery of marketing communications: in particular, it shall be clear whether the data controllers will use conventional marketing channels (ie paper e-mail), or automated calling or further systems without human intervention (ie fax, SMS, e-mail, MMS, recorded calls), or both.

Data subjects shall be duly informed of their right to revoke consent at any time for one or more of the purposes for which their data is processed, as well as to object to the use of one or more contact details.

The above issues are addressed in the "Guidelines on Marketing and against Spam" published by the Garante in 2013.

Behavioural advertising is allowed only upon a data subject's prior consent: this processing operation corresponds to a specific purpose (since it is based on a profiling activity), and therefore it shall not be deemed included in the definition of "marketing" thus requiring a separate, specific consent.

In addition, to date, a prior notification to the Garante is due in the case of profiling done through electronic means. It must be noted that the duty to notify processing operations to the Garante should be abolished by the GDPR; however, a brand-new law (ie Law 27 No 205 of December 2017, effective from 1 January 2018) introduced a new notification obligation for data controllers processing personal data through automated means or new technologies on the basis of a legitimate interest, and such processing is subject to the prior check of the Garante.

Location-based advertising is ruled in the same way as behavioural advertising: data subjects shall be informed of the collection of the data of their geographical position, and shall be granted a separate, specific consent thereon; moreover, as of today a prior notification to the Garante is due in the case of location data concerning individuals or objects which are collected by means of an electronic communications network.

2.4 Workplace Privacy

As to the processing of employees' personal data, the Garante issued several guidelines: "Guiding Principles Applying to the Processing of Employees' Personal Data for the

Purpose of Managing Employment Relations in the Private Sector" in 2006; "Guiding Principles on the Processing of Employees' Personal Data in the Public Sector" in 2007; and "Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context" in 2007. All these guidelines aim to clarify employers' (ie data controllers') duties and employees' (ie data subjects') rights under the applicable data protection law, provided that sectorial provisions such as the Workers' Statute remain unaffected.

Among other issues, the Garante clarified in particular that: the companies included in corporate groups are separate, autonomous data controllers with regard to the processing of employees' personal data and, where subsidiaries and related companies entrust their parent company with the task of fulfilling legal obligations related to employment, social security and benefits, the parent company will have to be appointed as data processor; employees' consent is necessary to communicate their personal data (concerning, for instance, an employee's recruitment, status or position, or the imposition of disciplinary sanctions, or an employee's transfer) to third parties such as employers' associations, family members and relatives; employees' consent is also necessary to publish personal information (ie pictures, identification data, CVs) on the corporate intranet, since such a dissemination of personal data is regarded as basically unnecessary to fulfil obligations arising from the employment contract except as otherwise provided by law. On the contrary, the posting on the corporate notice board of work instructions, shift schedules for workdays and holidays, or provisions on work organisation are permitted processing operations, being necessary to fulfil obligations arising from the employment contract; the obligation to wear a badge might require the prior approval of trade unions' organisations (at least in the private sector).

As to the use of internet and electronic devices, the Garante suggested adopting internal guidelines, to be duly brought to employees' attention (ie by publication on the intranet, or in workplaces). These guidelines shall clarify, for example: whether certain types of conduct are not permitted in terms of "browsing" the internet (ie downloading music files and/or software); to what extent the use of e-mail and network services is allowed for personal purposes; what information is recorded on a temporary basis and who is lawfully entitled to access such information (including external entities); whether and what information is kept for longer, due to the making of back-up copies; and which consequences, of a disciplinary nature, may be drawn upon by the employer in the case of the misuse of e-mail and internet services.

The contents of e-mail messages are a type of correspondence that is subject to confidentiality safeguards, not only under data protection laws (since they might concern, in addition to work-related information, the private life and/or personal sphere of both employees and third parties), but also pursuant to Constitutional principles (and additional safeguards provided under criminal provisions): it goes by the premise that an employer is not entitled to read e-mails sent and/or received by employees on their business account. Exceptions might nevertheless be legitimate, since the employer may reserve the right to ensure that work duties have been actually discharged and/or that work tools are used appropriately.

To reconcile this aim with employees' dignity and freedom, employees shall be clearly informed on whether, to what extent, and how controls are carried out with the privacy policy to be given when establishing the employment relationship, and the purposes of such controls have to be clearly stated as well (ie specific organisational, production and/or occupational safety requirements, or establishment or defence of judicial claims). Moreover, internal guidelines shall be adopted by the employer and made known to employees (ie on the intranet, by posting them in the workplace etc) to make clear that company devices (ie personal computer, mobile phone, business email address) must be used only for professional purposes, so that employees cannot reasonably contend that incoming and/or outgoing e-mails are kept confidential. These guidelines also have to describe in full details the specific control procedures.

Employers also have to comply with Article 4 of the Workers' Statute, which requires the agreement of trade unions for the deployment of equipment suitable for distance monitoring such as hardware and software systems intended to control electronic communications and/or to keep track of employees' activities (ie systematic scanning and recording of e-mail messages). Although equipment normally used to the execution of the employment relationship shall be deemed exempt from trade-union approval, this exemption shall be interpreted restrictively: therefore, it cannot be applicable to avoid trade-union approval for software used to monitor employees' e-mail, since this kind of software (unlikely the personal computer) is not necessary for the fulfilment of employees' obligations.

Labour organisations and trade unions act as a representative of their respective members, to protect their rights and interests. According to the Workers' Statute, they shall be informed of, and are empowered to be consulted and approve, the deployment – by the employer – of equipment intended to distance controls of the employees, either directly or indirectly.

A new law that entered into force on 29 December 2017 amended the rules concerning the public sector (incrementing the protection of the employee) and introduces similar rules for the private sector. As to the latter, the amendment concerns companies which have adopted the internal cor-

porate model of organisation and management (commonly referred to as the Model) according to Legislative Decree No 231, on 8 June 2001, against corporate crimes (the so-called Law 231): the Model shall ensure protection of the privacy of the employee, whose identity shall remain confidential during the management of the reporting of misbehaviour and/or of the breach of the Model; in addition, the employee shall not be subject to discriminatory acts due, either directly or indirectly, to the reporting, and penalties shall be provided against whoever breaches the measures to protect whistle-blowers.

Although anonymous reporting is discouraged, appropriate safeguards to ensure the protection of personal data of both the employee and the subject of the reporting have not been drawn up by law: they shall, therefore, be assessed by each data controller. A privacy notice describing the features of the Model shall obviously be in place.

In its "Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context," the Garante advises on how to deal with the business e-mail accounts of former employees to reconcile the employer's need to access information necessary for the management of the business with an employee's expectation of confidentiality. The measures to be implemented include the immediate de-activation of the relevant account and automatic messages to inform third parties of the new address to which communication concerning the business of the employer should be addressed. Employees shall be duly informed of the procedure adopted by the employer with internal guidelines to be disseminated.

Employees' personal data shall be processed also through surveillance systems: where cameras frame workstations, they might constitute remote control means thus requiring a prior trade union agreement according to Article 4 of the Workers' Statute.

As for surveillance systems, it has to be noted also that they shall comply with the Garante's decision on video surveillance on 8 April 2010: in the event of non-compliance, a prior checking request has to be lodged to the Garante to ensure the lawfulness of the surveillance system. One feature to be highlighted is the retention period of the data regarding storage of the images collected: pursuant to the proportionality principle, recordings shall be stored just for a few hours up to a maximum of 24 hours; specific technical requirements, or high-risk activities (ie bank), might be allowed to have higher retention periods, which shall not exceed one week. Whenever the retention period has to be extended, a request for prior authorisation must be lodged to the Garante.

2.5 Enforcement and Litigation

There are no legal standards for regulators to allege violations of data protection laws: an assessment is made on a case-by-case basis. Actual circumstances shall all be taken into account when addressing a possible breach of privacy laws, for instance: the nature, gravity and duration of the infringement; the categories of personal data concerned; and actions, if any, taken to reduce the relating consequences.

Under the Privacy Code, administrative sanctions may range from EUR6,000-EUR36,000 (omission of the prior information notice to data subjects) to EUR20,000-EUR120,000 (failure to submit the notification to the Garante), up to EUR25,000-EUR150,000 (breach of the obligations of providers of publicly available electronic communications services).

Repeated infringements, also on different occasions, in connection with large databases, might attract a fine ranging from EUR50,000-EUR300,000, which shall be in addition to those of each single breach. In the most serious cases, such as violations concerning several data subjects, the upper and lower thresholds of the applicable fines shall be doubled. Moreover, the fines may be increased by up to four times if they seem ineffective on account of the offender's economic status, and publication of the injunctive order, in whole or in part, in one or more newspapers shall be also provided.

It should be noted that the GDPR has increased fines up to EUR20 million, or in the case of an undertaking, up to 4.00% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The Italian Government has already been put in charge of adapting the existing penalties system accordingly.

In recent years Samsung was fined by AGCM (Autorità Garante della Concorrenza e del Mercato or Antitrust Authority) up to EUR975,000 for an aggressive commercial practice consisting of an unlawful processing of personal data of individuals collected during a contest.

To participate in the contest a data subject had to buy a certain product and then subscribe to an online platform and also consent to the processing of their personal data for marketing purposes. But the privacy policy was issued only after the purchase, at the time of subscription to the online platform: ie when data subjects were forced to consent to the processing of their personal data for marketing purposes to avoid having made an unnecessary purchase.

The importance of this case is that an unlawful processing has been considered as an aggressive commercial practice.

Very recently, Telecom Italia SpA was fined by the Garante up to EUR840,000 for processing of phone numbers in the absence of the due consent.

The unlawful activity consisted in calling former customers, who did not grant their consent to marketing communications, to ask whether they changed their mind and wanted to start receiving marketing communications.

This case shall be borne in mind when deciding how to renew already-collected consent which are not compliant to the GDPR: it is reasonable to argue that the renewal of the consent shall be requested only to those data subjects who granted the same consent, meaning that data controllers shall not be entitled to "take a chance" and contact also data subjects who did not grant their consent.

There are no legal standards to authorise private litigation for alleged violations of data protection laws.

As discussed above, data subjects may apply to the Garante: i) to lodge a circumstantial claim, in order to point out an infringement of the relevant data protection law; ii) to lodge a report, if no circumstantial claim may be lodged, in order to draw the Garante's attention to possible breaches; or iii) to lodge a complaint to exercise the rights provided to data subjects by the applicable data protection law.

In all such cases, where claims, reports and complaints are found to be clearly unsubstantiated, groundless or inadmissible, the Garante might discharge them after the preparatory phase of the proceedings. The verification is on a case-by-case basis and actual circumstances are taken into account.

Broadly speaking, the more information on the alleged breach that is provided, the more chances it has to be examined. Such information should include: identification data concerning a data controller and claimant and the domicile of choice for the serving of the relevant communications; a description of facts and circumstances; any supporting documents; and remedies sought.

Individuals can elect to be represented by not-for-profit organisations, thus leading to representative actions on behalf of a single individual or a group of individuals. According to the GDPR, Member States are entitled to enlarge the powers of such organisations.

In the last year or so there are no major private litigation cases worth mentioning, however it is important to stress that in 2016 the Garante issued penalties for EUR3,289,896 in the aggregate.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Law enforcement access to data for serious crimes is allowed without a prior judicial order, in cases where it is necessary for purposes of justice or for police purposes.

The Privacy Code grants specific derogations to judicial offices, to the Higher Council of the Judiciary, other self-regulatory bodies and the Ministry of Justice, to the police and other public bodies or public security entities, when processing is provided by laws or regulations and if it is carried out for purposes of justice or for police purposes. Such derogations include – inter alia – the exemption to provide the information notice to data subjects, to notify the processing to the Garante and to transfer personal data outside the European Union only under appropriate safeguards.

Personal data shall be considered for processing for purposes of justice if the processing is directly related to the judicial handling of matters and litigations, whereas processing for police purposes shall mean any processing of personal data that is directly related to the discharge of police tasks, such as for the prevention of criminal offences, the protection of public order and public security and judicial police activities.

This issue is addressed on a case-by-case basis, since different requirements might apply.

Privacy is protected by limits to law enforcement access to data as described above, as well as by further provisions applicable to processing by public authorities and judicial authorities as provided under the Privacy Code. For instance, data subjects are entitled to lodge a complaint to the competent court asking for the deletion of personal data processed by police authorities in breach of the law, and are also entitled to exercise further rights provided by data protection laws; general principles on data protection (ie fairness and lawfulness, purpose limitation, data minimisation and accuracy and limited storage periods) are also applicable. In addition, where the processing of personal data carries higher risks of harming data subjects, measures and precautions to safeguard data subjects are required and shall be laid down by the Garante during a check to be performed prior to the start of the processing (see Articles 54-56 of the Italian Privacy Code).

Further safeguards are ensured by granting to the Garante its institutional powers, such as verifying whether data processing operations are carried out in compliance with laws and regulations in force; receiving reports and complaints; and taking steps as appropriate with regard to complaints lodged by other data subjects or the associations representing them

(see Article 154 of the Italian Privacy Code): should the processing fail to comply with laws or regulations, the Garante shall draw the data controller's or processor's attention to the due measures and verify their implementation.

Validity and enforceability of documents, records and measures based on personal data in breach of the relevant laws or regulations might be excluded under the applicable civil or penal laws (see Article 160 of the Italian Privacy Code).

3.2 Laws and Standards for Access to Data for National Security Purposes

Law enforcement access to data is allowed without a prior judicial order when processing operations are carried out by public bodies for purposes of defence or of granting state security, as expressly required by laws that specifically provide for such processing operations.

The Privacy Code grants specific derogations to public bodies in these cases, since only a few provisions are applicable: inter alia, those ruling general principles governing protection of personal data, the duty to adopt the due security measures, and the duty to notify the processing to the Garante (see Article 58 of the Italian Privacy Code).

This issue is addressed on a case-by-case basis, since different requirements might apply.

Privacy is protected by limits to law enforcement access to data as described above, as well as by further provisions applicable to processing by public bodies for purposes of defence or relating to state security.

Safeguards are again ensured by granting to the Garante its institutional powers.

Validity and enforceability of documents, records and measures based on personal data in breach of the relevant laws or regulations might be excluded under the applicable civil or penal laws (see Article 160 of the Italian Privacy Code).

3.3 Invoking a Foreign Government

A foreign government access request might be a legitimate basis to collect and transfer personal data if grounded on important reasons of public interest, which shall be recognised by EU law or by the law of the Member State to which the controller is subject.

Judicial offices, the police and other public bodies or public security entities are not bound by the provisions regarding the transfer of personal data when acting within the scope of their institutional purposes, but shall nevertheless comply with the general principles on data protection (such as, inter alia, fairness, purpose limitation and data minimisation).

3.4 Key Privacy Issues, Conflicts and Public Debates

Government access to personal data raises concerns in that data subjects perceive it as an undue intrusion in their private life, since it results as imposed and unavoidable and, in most cases, it is hidden and not disclosed until a sanction is applied.

Further concerns relate to retention periods and security measures: private entities might be required to store personal data for a long period of time to grant government access to the same data in case of need, but long retention periods might increase the risk of cyber attacks and data breaches.

4. International Considerations

4.1 Restrictions on International Data Issues

Provided that data subjects have been duly informed thereon, the transfer of personal data is free among EU Member States: due to the harmonisation of European data protection laws, it is taken for granted that data subjects receive an adequate level of protection in all of the EU.

The transfer of personal data to non-EU Member States is prohibited if the laws of the destination country or transit of the data do not ensure an adequate level of protection of individuals, or if suitable safeguards are not in place to protect data subjects.

4.2 Mechanisms That Apply to International Data Transfers

A transfer of personal data to a third country may take place where the European Commission has decided that an adequate level of protection is granted, or if data controllers and data processors provide appropriate safeguards such as the implementation of binding corporate rules and/or the signature and execution, between the data exporter and the data importer, of the standard data protection clauses adopted by the Commission. Among the adequacy decisions of the Commission, the so-called Privacy Shield must be mentioned: this is an agreement between the EU and the United States, providing for the specific commitments of public and private entities to ensure the effective protection of European data subjects' personal data.

Further exceptions to the prohibition to transfer data outside the EU include: a data subject's consent; the performance of obligations resulting from a contract to which the data subject is a party; the need to safeguard a substantial public interest that is referred to by laws or regulations; investigations by defence counsel, or establishment or defence of a legal claim; safeguarding a third party's life; and responding to a request for access to administrative records or for

information contained in a publicly available register, list, record or document.

4.3 Government Notifications and Approvals

As long as adequate safeguards for the protection of personal data as required by the Privacy Code are in place, no government notifications or approvals are required to transfer data internationally. The Garante is empowered to authorise data transfers in cases where none of the above circumstances applies.

Special requirements might apply to categories of personal data of a more sensitive nature (ie judicial data, or information covered by business and industrial secrecy): an assessment will be carried out on a case-by-case basis.

4.4 Data Localisation Requirements

Data subjects shall be duly informed of the location of their personal data.

There is no general duty to maintain data in-country: there are just limits to the transfer of data outside the EU, whereas data transfer among EU Member States is free (provided that data subjects have been duly informed thereon).

4.5 Sharing Technical Details

No software code or algorithms or similar technical detail is required to be communicated to the government. Nevertheless, the Garante (as well as any other relevant public authority, as the case may be) is entitled to ask data controllers and data processors for such information, in the case of inspections and audits (carried out either ex officio or not), while examining instances or requests for ad hoc authorisations, or for further lawful reasons (ie judicial needs).

4.6 Limitations and Considerations

Under the Privacy Code, the transfer of personal data by private entities to foreign countries for foreign government data requests, foreign litigation proceedings and internal investigations is subject to the same safeguards discussed above. It should be noted that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring the transfer of personal data may only be enforceable under an international agreement in force between Italy and/or the EU and the requesting third country.

4.7 "Blocking" Statutes

Data protection law prohibits data transfers unless appropriate safeguards are in place: this is the main blocking statute to international data transfers.

Further prohibitions might be grounded on special requirements provided by sectorial laws (ie labour laws or trade-secret provisions).

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The processing of big data analytics shall abide by the general principles of transparency, fairness and lawfulness, purpose limitation, data minimisation and accuracy, limited storage periods and security, as well as to any further relevant provisions (ie those concerning the profiling of data subjects). Due to the connected risks for protection of personal data, a prior authorisation of, or consultation with, the Garante (according to Article 17 of the Privacy Code) might also be necessary when dealing with big data analytics; if used in the employment context, big data analytics are also subject to the Workers' Statute and the relating limits to the monitoring of employees.

On 30 May 2017, the Garante, the AGCM and the AGCOM started a common survey on big data, aimed at identifying risks and at defining rules to protect personal data, consumers and the digital economy.

Automated Decision-Making

The GDPR broadens the protection ensured by the Privacy Code (Article 14) to data subjects against decisions based solely on automated processing (including profiling), granting to individuals the right to obtain human intervention on the part of the controller, to express their point of view and to contest a decision based on an automated process.

Save for the above, automated decisions are legitimate – according to the GDPR – only if: data subjects have been duly informed thereon and have granted their consent; the decision is necessary for entering into, or the performance of, a contract between data subjects and the data controller; the decision is authorised by applicable law. Automated decisions are also subject to a DPIA.

Profiling

Profiling has been addressed by the Garante mainly in relation to marketing and advertising, to highlight that a specific consent needs to be collected from data subjects. The Garante has also issued "Guidelines on processing for online profiling purposes," advising data subjects to adopt a double-layered information notice. It has to be said again that profiling is subject to prior notification to the Garante, but such a duty should be abolished by the GDPR; however, as already highlighted, a brand new law (ie Law 27 No 205 December 2017, effective from 1 January 2018) introduced a new notification obligation for data controllers processing personal data through automated means or new technologies on the basis of a legitimate interest, and such processing is subject to the prior check of the Garante.

Special provisions are included in the Privacy Code (Article 14) and concern judicial or administrative acts or measures involving the assessment of a person's conduct, which cannot be based solely on the automated processing of personal data aimed at defining the data subject's profile or personality.

As to the GDPR, profiling is duly described in its preambles, where the controller is recommended to use appropriate mathematical or statistical procedures and to implement technical and adequate organisational measures to ensure, in particular, the prevention of discriminatory effects on natural persons, and where it is emphasised that profiling based on sensitive data is only allowed under specific conditions.

The Article 29 Working Party Party "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" adopted on 3 October 2017 as last revised and adopted on 6 February 2018 have also to be emphasised.

Artificial Intelligence (Including Machine Learning)
Artificial intelligence is not yet ruled under either national law or European law.

Among the issues raised by this topic, those concerning copyright have to be duly taken into account.

Internet of Things (IoT)
Talking about Internet of Things, or IoT, the Garante drew data controllers' attention on the need to ensure effective data protection by design and by default. The Authority also reminded data controllers of the need duly to inform data subjects and to collect an effective consent, in particular in the case of profiling purposes.

All the risks related to IoT have been assessed in the Article 29 Working Party "Opinion 8/2014 on Recent Developments on the Internet of Things" adopted on 16 September 2014.

Although not directly connected to IoT, blockchains have to be mentioned due to the possible future concerns that might arise on data protection: indeed, the "block" constituting "chains" records personal data virtually forever, and this is likely to result in a breach of the data minimisation principle unless appropriate safeguards are in place.

Autonomous Decision-Making (Including Autonomous Vehicles)
On 4 October 2017, the Article 29 Working Party adopted the "Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)."

C-ITS "is a peer-to-peer solution for the exchange of data between vehicles and other road infrastructural facilities (traffic signs or other transmitting/receiving base stations) without the intervention of a network operator," aimed at understanding the surroundings and consequently preventing accidents. The broadcast messages exchanged by the vehicles have been recognised as personal data: concerns have been raised on the need to ensure transparency (data subjects shall be aware of the processing), and the anonymisation of data and adequate retention periods; in addition, the suitable legal basis for processing has been identified in the compliance to legal obligations, thus calling on EU Member States to adopt any relevant provision.

The systems at hand might also imply the monitoring of drivers, which shall be avoided.

Facial Recognition
Facial recognition entails the processing of biometric data and is subject to the same rules, which are addressed below.

Facial recognition has also been dealt with by the Article 29 Working Party, which issued some opinions thereon (and on biometric data in general, as well) highlighting, inter alia, that facial recognition might also involve sensitive data processing.

Biometric Data
Even if the Privacy Code, unlike the GDPR, does not include biometric data among sensitive data, it is granted special protection due to the possible risks arising from its processing. Such protection shall be defined within the framework of a check to be performed by the Garante upon a data controller's due request prior to the start of the processing (according to Article 17). A notification to the Garante is also due, save for the fact that notifications are going to be abolished by the GDPR (and save for the new duty to notify processing of personal data through automated means or new technologies based on the legitimate interest of the data controller, effective as of 1 January 2018).

Biometric data is increasingly used for recognition purposes. Due to the number of requests for authorisation received, and aiming to ease data controllers' tasks and duties, in 2014 the Garante issued the "Guidelines on Biometric Recognition and Graphometric Signature": any processing of biometric data which conforms to these guidelines is not subject to the prior authorisation of the Garante. The guidelines also introduce the duty to inform the Garante of any biometric data breaches within 24 hours of becoming aware of such an event, using the draft format provided.

Validity and effects of the graphometric signature are duly addressed under Legislative Decree on 7 March 2005, No 82 (Codice dell'Amministrazione Digitale or CAD, Digital Administration Code) and in the relating implementing ministerial decrees (ie DPCM on 22 February 2013). It is im-

portant to highlight that these rules state that data subjects shall be given an exhaustive, written information notice on the graphometric signature, and have to grant their written consent thereto.

Geolocation
Geolocation is one of the processing operations to be notified to the Garante in advance.

When referred to employees (ie to monitor the use of fleet vehicles), Article 4 of the Workers' Statute shall apply: therefore, unless the equipment used to collect the location of the employee is necessary for executing the obligations arising from the employment contract, processing shall only be legitimate subject to an agreement with trade unions.

Recently, discussions arose on the possibility to locate individuals via electronic devices (such as smartphones and tablets) using just an algorithm: this might result in a risk for data subjects, since the collection of their physical location is not voluntary (there is no need to enable the location feature on the device).

Drones
The use of drones raises a number of privacy issues. The risks for data protection are mainly related to a lack of transparency of processing operations due to the difficulty in knowing which equipment is on board and by whom and for what purposes personal data is being collected, as well as to a potential severe interference with the most intimate sphere of individuals due to the ability of drones to avoid obstacles and achieve unique viewpoints.

Drones are electronic devices: therefore they have to comply with both privacy by design and privacy by default principles. The owner should always be visible, thus being contactable by those individuals who do not want to appear in photos and videos recorded by drones, it being understood that the publishing of photos and videos is subject to the prior and specific consent of the persons portrayed. Special attention shall be paid to respect and protect the intimate sphere of third parties, for example avoiding any recordings of other people's conversations or private spaces (ie a house or private garden): such conducts might also breach criminal laws.

Applicable provisions include regulations issued by Ente Nazionale per l'Aviazione Civile o ENAC (National Civil Aviation Entity). Rules on CCTV systems might also be applicable, especially to drones used for surveillance purposes.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators
The main law concerning cybersecurity is the Privacy Code, soon to be updated according to the GDPR. In this field, the new regulation provides for news such as a general duty to notify data breaches to the Supervisory Authority, and an increased controller's accountability, in that no minimum security measures are provided being a controller's responsibility to assess and to implement technical and organisational measures appropriate to ensure protection of personal data (taking into account the state of the art and the costs of implementation, nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of individuals).

In March 2017, Italy adopted the National Plan for Cyber Protection and Cyber Security (Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica) for the purposes of the Decree of the Presidency of the Council of Ministers on 17 February 2017, concerning guidelines for national cyber protection and cybersecurity. The actions planned include the issuance of laws and regulations, as well as the due transposition of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union (the so-called Network Information Security Directive or NIS Directive) by 9 May 2018. The transposition of Directive (EU) 2016/680 on the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties might also imply news in the cybersecurity field.

Circular No 2 of 18 April 2017, issued by Agid (Agenzia per l'Italia Digitale or Agency for Digital Italy), should be mentioned: it provides for minimum ICT security measures for public authorities, which were to be implemented by 31 December 2017. Similar rules for the private sector are still to come.

The CAD and the implementing ministerial decrees might also provide for security requirements.

Moreover, the Criminal Code also concerns cyber crimes: for instance, whoever accesses electronic systems protected with security measures shall be imprisoned for up to three years, according to Article 615-ter Criminal Code.

Among others, Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (EIDAS Regulation), and Directive 2013/40/EU of European

Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, are also relevant.

On a European level, ENISA (European Union Agency for Network and Information Security) is an advisory board for the EU on cyber issues, actively contributing to a high level of network and information security within the union. It works together with EU Members and private entities to provide advice and solutions, in the form of studies on hot topics such as data protection issues and new technologies, and to support policy-making and implementation while collaborating directly with operational teams.

ENISA liaises actively with the Multi-Stakeholders Platform on ICT standardisation, an advisory expert group on all matters related to European ICT standardisation, and the CEN-CENELEC Focus Group on Cybersecurity (CSCG). The CSCG was created by European Standardisation Organisations (CEN, CENELEC and ETSI) to provide support in the analysis of technology developments and in the issuance of a set of recommendations for international standards setting, with the final aim of ensuring growth of the digital single market.

From an international point of view, OSCE (Organisation for Security and Co-operation in Europe) is also active in cybersecurity: its aim is to increase trust among Member States and to reduce risks arising from the use of information technologies.

The Garante is in charge of receiving data-breach notifications under the GDPR and of checking the adequacy of the organisational and technical measures adopted by data controllers to ensure the protection of personal data, as well as to recommend actions and impose fines in case of infringements of the applicable law.

Agid (Agenzia per l'Italia Digitale or Agency for Digital Italy) is in charge of ensuring the execution of the Italian digital agenda and also ensuring compliance with the European digital agenda. Its tasks include, among others, the issuance of opinions, guidelines and technical rules, aimed at easing and encouraging the use and the diffusion, and to grant uniformity, of information technology in the public sector.

Supervisory authorities, such as AGCOM, Banca d'Italia (the central bank of Italy) and IVASS (Istituto per la Vigilanza sulle Assicurazioni Private or Institute for Private Insurances Supervision), are empowered to issue regulations and guidelines, and these might also concern cybersecurity matters: among others, Order on 17 December 2013 of Banca d'Italia (as updated on 21 July 2015) provides for the security requirements of information systems,

CNAIP (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche or National Anti-Cybercrime Centre for the Protection of Critical Infrastructures) also must be mentioned: its tasks are focused on cyber-crime prevention and suppression.

Many CERTs (Computer Emergency Response Teams) support individuals and private and public entities in case of cyber threats, providing information, increasing awareness, cooperating with public and private entities and helping to deal with cyber breaches. Among others:

- CERT Nazionale (or National CERT) supports individuals and private entities;
- CERT-PA (or Public Administration CERT) supports public entities. It is part of Agid; and
- CERTFin (or Financial CERT) is active in the banking and financial field.

CINI (Consorzio Interuniversitario Nazionale per l'Informatica or Inter-university Consortium on Information Technology) also has to be mentioned, being the main reference point for academic research on information technology. In partnership with CIS Sapienza (ie the Research Centre of Cyber Intelligence and Information Security of Sapienza Rome University), it published the "2016 Italian Cybersecurity Report" where essential cybersecurity controls were addressed.

Finally, CLUSIT (Associazione Italiana per la Sicurezza Informatica or Italian Association for Cyber Security) aims to increase the awareness of cybersecurity among companies, public authorities and private citizens, also by joining the drafting of laws and regulations in this field and by offering certification programmes for ICT professionals.

6.2 Key Frameworks

Unless otherwise provided, all recognised standards are not compulsory requirements: they shall just be deemed as tools to be used by controllers to identify the appropriate security measures to be implemented; in addition, being provided by independent and expert bodies, and being based on usual practice, they may also serve as a blueprint for auditing and checking compliance of an organisation to security best practices. It is important to point out that standards shall not be used as checklists, and their actual appropriateness shall in any case be duly assessed.

UNI (Ente Nazionale Italiano di Unificazione or Italian National Unification Entity) is an Italian private, not-for profit entity, recognised by both the Italian Government and the European Union, which issues voluntary technical standards concerning all business sectors. UNI represents Italy to both CEN (European Committee for Standardisation) and ISO

(International Organisation for Standardisation), which are further standardisation bodies.

Among many others, ISO 27001 seems the preferred standard to infer security measures to data protection. It is deemed as a comprehensive specification for protecting data under the principles of confidentiality and integrity and it offers a set of best-practice controls based on actual risks. It is not (or, at least, not yet) officially recognised as appropriate and accredited for the purposes of the GDPR, but it may well help in proving the commitment of the controller in complying to data protection law.

6.3 Legal Requirements

A written information security plan may be, on a case-by-case basis, an appropriate security measure according to Article 32 GDPR. Its contents shall be decided by the data controller, in accordance to the accountability approach, and in compliance with the general principles governing data protection.

Incident Response Plan

An incident response plan will be drafted and will take into account the duty to notify data breaches, provided by the GDPR: it therefore enables the controller to detect a breach and to notify the same to the Garante, when needed, within 72 hours after having become aware of it, as well as to adopt any due measures to mitigate consequences of the breach.

Appointment of Chief Information Security Officer, or the Equivalent

According to Garante's "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator," issued in 2008 (as further amended), a "system administrator" is "a professional in charge of managing and servicing a processing system and/or components thereof. For the purposes of this decision, the scope of the above definition will be enlarged to include other professionals that can be equated in terms of data protection risks – such as database administrators, network and security equipment administrators, and the administrators of complex software systems."

These tasks shall be carried out by individuals whose experience, skills and reliability, and the ability to comply in full with the relevant applicable legislations, have been duly checked in advance. The standards are the same as those applying to data processors: therefore, the appointment has to be on an individual basis, and the scope of the tasks of the system administrator have to be duly detailed.

A list of all appointed systems administrators and their identification data has to be drafted by the controller and duly updated at least annually; with the same frequency, the controller shall also check the activities of system administrators.

Involvement of Board of Directors or the Equivalent

The board of directors (or the sole administrator, as the case may be) is the managing body of a company and is ultimately responsible for ensuring that appropriate measures are in place to manage cyber risks effectively.

Conducting Internal Risk Assessments, Vulnerability Scanning, Penetration Tests, etc

Internal risk assessments, vulnerability scanning, penetration tests and the like may be, on a case-by-case basis, appropriate security measures according to Article 32 GDPR. The actual measures to be implemented and their features shall be decided by the controller, according to the accountability approach of the GDPR, and always bearing in mind general principles of data protection.

GDPR provisions on DPIAs, as well as Article 4 of the Workers' Statute, shall also apply, to ensure that the measures at hand do not result in a high risk to the rights and freedoms of individuals and/or in unlawful controls of employees.

Insider Threat Programme

An insider threat programme shall abide by the laws and principles concerning control and the monitoring of employees. A data protection impact assessment might also be needed.

Vendor and Service-Provider Due Diligence

Vendors and service-providers shall be appointed only after a due check of their ability to provide sufficient guarantees to implement appropriate technical and organisational measures, according to the relevant laws. Their tasks shall be duly detailed, and compliance thereto shall be monitored: controls are also in the controller's interest, since liability for vendors and service-providers' acts and/or omissions is vested in the controller.

When vendors and service-providers process personal data, they shall be appointed as data processors and all the relating provisions shall also apply.

Training

Personnel training is a general duty of employers towards employees. Its subjects varies according to the individual tasks: it might also then concern cybersecurity and data protection.

Training has a crucial role in raising employees' awareness on the importance of data and effective protection.

6.4 Key Multinational Relationships

Major multinational relationships involving Italy are those relating to being a Member of the EU. The EFMS (European Forum for Member States on public policies for security and resilience in the context of Critical Information Infrastructure Protection) must be mentioned as it promotes the exchange between Member States of good practices, information and experience on public policy matters relevant to security and resilience in the context of critical information infrastructure protection.

It should also be noted that artificial intelligence, standards and cybersecurity were on the agenda of a recent meeting of the G7 (of which Italy is a member), which stressed their importance as public assets to be duly protected.

6.5 Key Affirmative Security Requirements

As to technical and organisational measures, the GDPR provides for some examples which shall not be deemed as minimum compulsory requirements including: pseudonymisation and encryption of data; the ability to ensure confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of an incident; and processes for regularly testing, assessing and evaluating the effectiveness of the measures in place. The controller and the processor shall, in no case, be relieved of the duty to assess and implement measures appropriate to the single case.

Adherence to approved codes of conduct and certification mechanisms shall help in demonstrating the commitment to comply with data protection laws. As of today, no code of conduct or certification has been approved by the Garante.

Material business data shall benefit from know-how protection measures, when applicable.

Like data protection technical and organisational measures, know-how measures also need to be appropriate and duly assessed on a case-by-case basis.

ENISA published analyses and recommendations on critical infrastructure (available at www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis).

Further requirements shall be defined as soon as the NIS Directive is implemented.

There is no legal security requirements to prevent denial of service attacks: reference shall be made to general data protection principles and rules, as well as to recognised standards.

6.6 Data Breach Reporting and Notification

Under the Privacy Code, personal data breach is defined as "a security breach leading, accidentally or not, to the destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in the context of the provision of a publicly available communications service." With guidelines and measures, the Garante ruled further cases of data breach, such as those concerning biometric data processed for identification purposes, health data contained in electronic medial dossiers and data processed by public entities.

The GDPR further broadens the definition of data breach, since it concerns all data controllers (and is not limited to communications service providers anymore).

The Garante - in its operative guide for the application of the GDPR - has already confirmed that the duty to notify a data breach will be applicable to all data controllers: for this reason, the issue at hand is addressed below taking into account the new rules in light of the guidelines on data breach issued by the Article 29 Working Party.

All personal data processed by a data controller and/or a data processor may be the subject of a data breach, which might be either a "confidentiality breach" (in the case of disclosure); an "availability breach" (in the case of loss of access or destruction); an "integrity breach" (in the case of alteration); or all of them at the same time.

No system is excluded from data breaches: although data breaches are more likely to occur in a case of processing with electronic means, also the processing without electronic means might be affected.

Security Requirements and Medical Devices

As to medical devices, two new regulations must be mentioned: Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU. These Regulations entered into force on 25 May 2017, but will apply after a transitional period of three and five years respectively.

Although the new rules are a step forward, it has to be noted that they do not address security requirements in full detail. Reference shall then be made to data protection rules embodied by the Privacy Code and the GDPR, especially those concerning sensitive data (medical devices unavoidably process sensitive data), as well as to general standards

(ieISO 27000 series and ISO 80001): that is to say that data controllers and processors will have to assess the risks arising from medical devices and implement any adequate security measures to ensure protection against cyber attacks, both by design and by default, according to the accountability principle. It must be noted that the ability to detect a breach shall be one of such measures, as well as due agreements with any data processor who shall promptly and without delay notify the controller of the breach.

Security Requirements and Industrial Control Systems (and SCADA)
Like medical devices, Industrial Control Systems (like SCADA) do not benefit from rules listing due security requirements: general data protection principles, as well as general standards, shall help in assessing the due security measures to be implemented.

ENISA drafted a report collecting most of the applicable standards. This report is published on ENISA's website (www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada).

Security Requirements and IoTs
Once again, no consolidated set of rules clarifies security requirements for IoT.

Article 29 Working Party, in its guidelines on IoT, recommended the performance of security assessments of systems as a whole, the application of principles of composable security, the use of certification for devices and the implementation of internationally recognised security standards taking into account all specific operational constraints. The data minimisation principle has to be strictly followed.

The recommended security requirements include "network restrictions, disabling by default non critical functionalities, preventing use of un-trusted software update sources (thus limiting malware attacks based on code alteration) […]built-in from the very outset, in application of the "Privacy by Design" principle."

Reference must also be made to a recent ENISA report (published in November 2017), detailing possible security requirements with the double approach of the GDPR: by design and by default (this report is published on www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot).

Criteria to Report
Government Authorities
Data controllers shall notify data breaches to the Garante "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (Article 33 GDPR): that is to say that controllers shall duly assess the breach to understand its possible consequences. The term for the notification is 72 hours after having become aware of the breach; any delay must be duly justified.

The information to be provided includes: the nature of the data breach; the categories and approximate number of data subjects concerned and of personal data records concerned; the name and contact details of the contact person (ieDPO) who shall provide more information; possible consequences of the breach; and measures taken or proposed to mitigate effects of the breach.

Any data breach shall be documented to enable the Garante to verify data controllers' compliance with the relevant provisions.

Individuals
The data breach has to be communicated to data subjects, without undue delay, if it is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 34 GDPR), or if it is required by the Garante. The aim is to provide individuals with due information on the measures to take to protect themselves.

No communication is due in cases where: appropriate preventive technical and organisational measures were applied to the data concerned, for instance to render the same data unintelligible to unauthorised persons; appropriate subsequent measures were taken to exclude the risks to rights and freedoms of data subjects; and the communication would result in a disproportionate effort, in which case a public communication shall nevertheless take place.

Other Companies or Organisations
The GDPR does not provide for the duty to notify the data breach to companies or organisations which are not directly concerned by the breach itself.

In the case of companies or organisations acting as data processors, they shall inform the controller immediately of any data breach in order to let the controller examine the breach and timely notify the same to the Garante, if needed.

6.7 Ability to Monitor Networks for Cybersecurity
Network monitoring shall be permitted according to applicable data protection rules and principles.

The monitoring of workplace communications has been previously addressed and the same provisions also apply in the case of cybersecurity measures which might imply the controls of the employees, since the rights of freedoms of the individuals always have to be granted.

6.8 Cyberthreat Information Sharing Arrangements

CERTs are in charge of receiving and spreading information on cyber threats and attacks.

The NIS Directive expressly entitles entities other than operators of essential services and digital service providers to notify, on a voluntary basis, a breach having a significant impact on the continuity of the services which they provide.

The notification shall be to CERTs or to the different competent authority that is going to be appointed during transposition of the NIS Directive.

6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

Article 29 Working Party established a task force to investigate the UBER data breach case. The task force is led by the Dutch Data Protection Authority, and brings together representatives of Italian, French, German, Spanish and Belgian data protection authorities, as well as of the ICO (ie the United Kingdom independent body in charge of granting information rights). It will co-ordinate national actions and initiatives on the case.

The UBER data breach occurred in 2016, but was only notified in November 2017. Tens of millions of users worldwide are concerned by the breach.

LCA Studio Legale
Via della Moscova 18,
20121 Milan
Italy

Tel: 0039 027788751
Fax: 0039 0276018478
Email: info@lcalex.it
Web: www.lcalex.it

6.10 Other Significant Issues

Data breaches have been discussed above taking into account GDPR requirements.

Controllers must remember that data breach notifications may also be due under further regulations and/or provisions concerning specific business fields: for instance, EIDAS Regulation, NIS Directive or measures and guidelines of the Garante (such as those on biometric data processed for identification purposes and discussed above). The notification of data breaches according to the GDPR shall be additional to, and not a replacement of, any further duty to notify data breaches.