Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Italy
LCA Studio Legale

chambers.com

2019

Law and Practice

Contributed by LCA Studio Legale

Contents

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 European General Data Protection Regulation (No 679/2016) and the relevant national provisions issued thereon; 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; 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 head of the Intellectual Property & Data Protection group. His practice covers data protection and cybersecurity, IT and internet law and misleading and comparative advertising. He has extensive experience in consultancy and litigation regarding data protection matters and assists clients in complex cybersecurity projects, e-commerce projects and e-payment deals at both contentious and non-contentious level. He has assisted many international groups of companies in the compliance process regarding the General Data Protection Regulation (GDPR) and in the approval process of Binding Corporate Rules as appropriate safeguard to the transfer of personal data to third countries. For his extensive experience in data protection in 2018 Gianluca was heard as expert by the Italian Senate on the draft of legislative decree that will amend the Italian Privacy Code, in order to make it compliant with the new European Regulation on personal data protection (GDPR). He is a member of the International Association of Privacy Professionals (IAPP).

Chiara Bocchi is a senior associate specialised 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 has assisted many international groups of companies in the compliance process regarding the General Data Protection Regulation (GDPR) and 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 laws are:

- Regulation (EU) 2016/679 ('General Data Protection Regulation' or 'GDPR');
- Legislative Decree 196/2003 ('Privacy Code'), which constitutes the transposition of Directive 95/46/EC and Directive 2002/58/EC, and repealed Law 675/1996;
- Legislative Decree 65/2018, transposing Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the European Union ('NIS Directive'); and
- Legislative Decree 53/2018, transposing Directive (EU) 2016/681 on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

The Privacy Code has been amended and complemented by:

- Legislative Decree 51/2018, transposing Directive (EU) 2016/680 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 (repealing Council Framework Decision 2008/977/JHA); and
- Legislative Decree 101/2018, adapting the Italian legislation to the GDPR and providing for transitional provisions (or 'GDPR Adaptation Decree').

Further to such amendments, the GDPR became the first source of data protection provisions in Italian legislation; the Privacy Code only provides additional provisions, basically where the GDPR entitled EU Member States to do so.

All of the above are complemented by guidelines, recommendations, orders, general authorisations and codes of conduct issued and approved by the Italian Personal Data Protection Authority ('Garante per la protezione dei dati personali' or 'Garante') and by the European Data Protection Board ('EDPB'), ie, a body of the Union – set up by the GDPR – having legal personality that brings together the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives, as well as a representative of the Commission (without voting rights).

The EDPB substituted the Article 29 Working Party ('Art-29WP') from the date the GDPR entered into force (25 May 2018), endorsing the guidance already provided by Art29WP and developing additional guidance.

Principles applying to data protection shall also be found in the Constitution of the Italian Republic, which lists all fundamental principles governing Italy, and in other national laws, which may address specific categories of personal data, adding requirements for lawful processing, eg, Law 633/1941 ('Copyright Law') and Law 300/1970 ('Workers' Statute').

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;
- the Charter of Fundamental Rights of the EU; and
- 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, which is the sole binding instrument on data protection at an international level.

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 controllers, processors, data subjects or third parties to provide information and produce documents;
- carrying out investigations and accessing premises where processing operations take place;
- notifying the controller or processor of an alleged infringement;
- ordering controllers or 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;
- issuing opinions whenever required;
- imposing fines; and
- reporting information on facts and/or circumstances amounting to offences to be prosecuted.

The Garante shall act either ex officio, or upon receipt of reports and complaints lodged by other data subjects or the associations representing them.

1.3 Administration and Enforcement Process

Data subjects may apply to the Garante to report 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.

Any claim shall be filed, alternatively and not cumulatively, to the civil courts (save for the fact that infringement of data protection provisions might also result 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 monetary compensation for damages; and judicial proceedings have no fixed term, whereas the term provided to the Garante is nine months from the date on which the complaint was lodged, to be extended up to 12 months if the enquiries are especially complex (and to be suspended if the co-operation procedure under Article 60 of the GDPR is started).

The decision may be challenged by filing a petition to the judicial authority. Challenging shall not automatically suspend enforcement of the decision.

1.4 Multilateral and Subnational Issues

To grant the same level of personal data protection throughout the EU, national laws have been harmonised through Directive 95/46/EC and Directive 2002/58/EC, and then standardised through the GDPR.

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 transposed Directive 95/46/EC and Directive 2002/58/EC, and was amended by the GDPR Adaptation Decree.

The latter also determines the transition period and expressly states that its provisions and further Italian laws shall be applied and interpreted according to EU relevant laws. Likewise, guidelines, recommendations and orders issued and approved by the Garante shall be deemed to remain in force insofar as they are consistent with the GDPR. Existing codes of conduct and general authorisations for processing of 'sensitive' data are expressly subject to a review process.

The Garante issues guidelines, orders and measures to clarify and supplement the legislation, as well as to simplify data protection fulfilments (in particular for small and medium-sized enterprises). These are published in Italy's Official

Journal ('Gazzetta Ufficiale'), and therefore have a regulatory nature. Controllers and processors are obliged to comply with these and their application might be enforced either ex officio or on the request of data subjects.

1.5 Major NGOs and Self-Regulatory Organisations

Of the non-governmental organisations (NGOs), Federprivacy (Italian Privacy Federation), Istituto Italiano Privacy (Italian Privacy Institute), Asso DPO (Data Protection Officer Association) and Associazione Nazionale per la Protezione dei Dati (National Association for Data Protection) deserve mention. These associations provide membership to privacy professionals, offer training on privacy issues and strengthen contacts with the Garante.

Many NGOs were established soon after the entry into force of the GDPR – a sign of the increased awareness of the importance of data protection, thanks to the new European regulation.

Collective organisations representing specific categories of controllers or processors for general purposes may draft codes of conduct, or amend or extend existing ones, for the purpose of specifying the application of privacy legislation. Codes of conduct shall be approved by the Garante, prior to their registration and publication. In relation to processing activities in several EU Member States, the prior opinion of the EDPB shall be sought and, if it confirms compliance of the code with the GDPR, the Commission shall give validity to the code within the EU by way of implementing Acts.

To date, the Garante has confirmed the consistency and, therefore, the effectiveness of some codes of conduct already approved under the Privacy Code – for example, those on data processing for journalism, for scientific research or statistical purposes, for defensive investigations and for the establishment, exercise or defence of legal claims, and for archiving purposes in the public interest or historical research purposes.

1.6 System Characteristics

Following the EU model, Italy is highly regulated, and European systems are indeed more developed than non-EU countries.

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

1.7 Key Developments

The major development in the past year has been the adaptation of the Italian legal system to the GDPR. The GDPR Adaptation Decree was eagerly awaited and came as a surprise, as early rumours announced the repeal of the Privacy Code, whereas it only amended the Privacy Code and added some transitional provisions.

In parallel, the Garante has issued various guidelines and templates concerning:

- data protection officers (DPOs), both in the private and in the public sector, a draft appointment agreement for DPOs and an online procedure for the communication of their contact data;
- records of processing activities, and a template addressed to small- and medium-sized enterprises;
- processing requiring a data protection impact assessment (DPIA), in addition to those provided by the GDPR;
- data breaches, providing a dedicated email address for due notification;
- a template to help data subjects in exercising their rights under the GDPR; and
- various information sheets summarising the main duties of controllers.

These guidelines are in addition to those issued by Art29WP and the EDPB, concerning:

- DPO;
- DPIAs;
- consent;
- transparency;
- automated decision-making and profiling;
- data breaches;
- records of processing activities;
- right to data portability;
- criteria to identify the lead supervisory authority;
- criteria for application and setting of administrative fines;
- certification and identifying certification criteria;
- derogations to the transfer of personal data to third countries;
- territorial scope of the GDPR; and
- accreditation of certification bodies.

Art29WP also started the review process for the approval of binding corporate rules (BCRs).

Accredia has been designated as the Italian certification body in charge of issuing certifications pursuant to Article 43 of the GDPR.

1.8 Significant Pending Changes, Hot Topics and Issues

Brexit is probably the hottest topic on the horizon for the next 12 months. The consequences for data protection are not yet clear but will undoubtedly be of paramount importance as the UK will become a third country.

The e-regulation, ie, a regulation repealing Directive 2002/58/EC (and further amendments) concerning data

protection in the electronic communications sector, is also eagerly awaited, and a proposal is currently under discussion.

A brand new proposal has been put forward to merge the Garante with AGCOM (the supervisory authority for communications), aimed at strengthening their respective powers and actions.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Although some EU countries had already implemented DPOs, as far as Italy is concerned, the role of DPO is newly introduced by the GDPR, whereas the role of privacy officer remains unlegislated.

Privacy officers shall, nevertheless, be selected among entities that can appropriately ensure, on account of their experience, capabilities, reliability and compliance, that provisions are in force, as applied to processing and related to security matters. Their tasks might be performed either by controllers or processors (such as external consultants), or by the so-called designated subjects (or 'soggetti designati'), ie, people who are part of a controller's or processor's organisation and have been put in charge of specific functions concerning personal data processing by the controller or the processor. Designated subjects were introduced under the GDPR Adaptation Decree.

DPOs shall have expert knowledge of data protection law and practices, be able to provide advice and monitor compliance with data protection laws, and be bound by a duty of confidentiality. DPOs may be either 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, avoid any conflicts of interest and report directly to the highest management level. A group of undertakings might appoint just one DPO, provided that it is easily accessible by each member entity.

According to the Administrative Court (TAR) of Friuli Venezia-Giulia (order no 287/2018), DPOs shall have a strong judicial background, thus recommending that preference is granted to jurists rather than IT experts (at least in the public sector).

Under the GDPR, the appointment of a DPO is compulsory in just three cases, which are:

- where the processing is carried out by a public authority or body;
- where 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; and/or
- where the core activities of the controller or the processor consist of processing 'sensitive' data or 'judicial' data on a large scale.

Italian laws provide for the appointment of a DPO for competent judicial and police authorities.

Art29WP and the Garante recommend the appointment of DPOs in general, both as good practice and as proof of accountability.

Processing shall be lawful only if and to the extent that it is compliant with the basic principles of processing (Article 5 of the GDPR determines such principles as lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability), and that one legal basis for the processing applies.

Legal bases are listed under Article 6 of the GDPR. They include:

- the data subject's consent;
- the need to perform a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
- compliance with a legal obligation to which the controller is subject;
- the need to protect the vital interests of the data subject or of another natural person;
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- the pursuance of the legitimate interests of the controller or a third party.

To rely on legitimate interest, the so-called balancing test shall be carried out in advance to ensure that rights and freedom of the data subject do not prevail against the interest of the controller. In their guidelines on transparency, Art29WP recommended to identify the specific interest pursued, providing the data subject with information from the balancing test or, at least, confirming that they can obtain information on the balancing test upon request.

Where consent is relied upon, it shall be freely given, specific, informed, unambiguous and demonstrable. Art29WP's guidelines on consent provide further advice.

The GDPR does not force the adoption of minimum security measures (including technical and organisational measures). Preferring an accountability-based approach, it requires controllers and 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.

Some examples are provided under Article 32 of the GDPR.

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 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' and 'judicial' data; and
- systematic monitoring of a publicly accessible area on a large scale.

Art29WP has issued guidelines to help controllers and processors understand when DPIAs are needed and how to conduct them. When in doubt about whether to carry out a DPIA, the advice is to proceed.

Supervisory authorities are expressly empowered to extend or reduce the list of cases in which DPIAs have to be carried out. The Garante adopted its list, and confirmed that controllers can use the open-source software developed by the CNIL (the French Data Protection Authority) as guidance.

Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the supervisory authority prior to processing.

Data subjects shall be informed of the main features of the processing of their data, prior to processing. The information to be provided is stated under Articles 13-14 of the GDPR, covering the main features of the processing.

Any privacy policy shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It can be either oral (when requested by the data subject) or written.

Data subjects shall, at any time, exercise their rights as granted under the applicable data protection law. Any request shall be issued to the relevant controller and will not be subject to any formalities; a standard form is published on the website of the Garante for data subjects' convenience.

Controllers shall not unreasonably refuse to act on the request of data subjects for exercising their rights, and shall reply without undue delay, within one month of receipt of the request; this term may be extended up to three months, taking into account the complexity and number of the request(s).

Where the request of the data subject is rejected, the controller shall inform the data subject without delay – and at the latest within one month of receipt of the request – of the reasons for not taking action, the possibility of lodging a complaint with a supervisory authority, and of seeking a judicial remedy.

Information and actions provided to data subjects shall be given free of charge, unless data subjects' requests are manifestly unfounded or excessive (ie, the controller does not own any personal data of the requesting data subject). In such cases, the controller may either charge a reasonable fee, taking into account the costs actually incurred for the enquiries made in the specific case, or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive nature of the request.

The Privacy Code provides for some limits to the rights granted to data subjects, which cannot be invoked in the case of risk of a severe bias to rights protected by anti-money laundering provisions, to defensive investigations or for establishment, exercise or defence of legal claims, or to the identity of whistle-blowers.

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 using suitable arrangements to allow the identification of data subjects only when necessary.

Anonymisation, de-identification and pseudonymisation may be considered adequate technical security measures, or an appropriate safeguard, on a case-by-case basis. 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.

When dealing with profiling, automated decision-making, online monitoring or tracking, Big Data analysis and artificial intelligence, data protection provisions shall be taken into account as all these activities imply personal data processing.

The GDPR introduced restrictions on automated decision-making, broadening the protection previously ensured by

the Privacy Code to data subjects against decisions based solely on automated processing, including profiling. These include requesting controllers to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least by 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. Data subjects shall be provided with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject, at the time of provision of the information notice.

Save for the above, automated decisions are legitimate – according to the GDPR – only if:

- data subjects have been duly informed and have granted their consent;
- the decision is necessary for entering into, or for the performance of, a contract between data subjects and the controller; and
- the decision is authorised by applicable law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

Automated decisions shall not be based on 'sensitive' data, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place, and the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, or processing is necessary for reasons of substantial public interest, on the basis of EU or national law, which shall be proportionate to the aim pursued and respect the essence of the right to data protection.

Automated decisions are also subject to a DPIA.

In the case of a breach of personal data protection laws, data subjects may suffer damages and be entitled to compensation under Article 82 of the GDPR (mentioned also by Article 152 of the Privacy Code).

Damages shall be either material or non-material. As to non-material damages, no classification is required – according to Italian case law, any potential category of non-material damages (reputational, emotional, embarrassment, etc) is just a description, since non-material damages are and shall remain unitary and not subject to duplication due to the use of different names.

2.2 Sectoral Issues

'Sensitive' data is a definition previously used by the Privacy Code to address 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.

The GDPR renamed 'sensitive' data as 'special categories of personal data,' expressly adding genetic data and biometric data processed for the purpose of uniquely identifying a natural person. Although the GDPR Adaptation Decree replaced the definition of 'sensitive' data with 'special categories of personal data,' such data is still commonly referred to as 'sensitive' data.

Processing of 'sensitive' data is prohibited, except in the circumstances provided under Article 9 of the GDPR. Such circumstances are in addition to, and not in lieu of, the legal basis for processing.

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. Accordingly, the Privacy Code puts the Garante in charge of issuing, every two years, safeguarding measures for the processing of genetic data, biometric data and health data.

It has to be remembered that, under the Privacy Code, the prior authorisation of the Garante was needed to ensure lawful processing of 'sensitive' data. To ease controllers' tasks and duties, the Garante usually issued general authorisations (for example, for the processing of sensitive data in the employment context). Where the processing complied with the relevant general authorisation, controllers had no need for an ad hoc authorisation. The GDPR Adaptation Decree has put the Garante in charge of the duty to check existing general authorisations for the processing of 'sensitive' data and to amend or update these according to the GDPR.

Financial data, if it allows the identification of data subjects, is considered personal data.

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 Banca d'Italia (Bank of Italy). Further communications may also be due 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.

Guidelines were adopted in 2007 by the Garante for the processing of customers' data in the banking sector. 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, according to the GDPR Adaptation Decree, will remain in force until completion of the review process to be carried out by the Garante to ensure consistency with the GDPR.

Health data is 'sensitive' data and is therefore subject to the special safeguards provided for this category of data.

The Privacy Code allows the communication of health data to professional third parties, 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 data subjects' protection is properly ensured.

Guidelines have been adopted by the Garante to address particular cases. Pursuant to the GDPR Adaptation Decree, they are still applicable insofar as they are consistent with the GDPR.

Communications data are not considered to be 'sensitive' data; nevertheless, a high level of protection is granted under criminal law provisions, aimed at ensuring that collection of communications data is limited to what is necessary to prosecute offences.

'Sensitive' data revealing union membership has been addressed in a recent order issued by the Garante, clarifying that an employer cannot communicate information concerning its employees' union membership.

'Judicial' data, referred to as "data relating to criminal convictions and offences," is not 'sensitive' data; nevertheless, its processing is subject to tight constraints. Processing shall be carried out only under the control of an official authority or when authorised by the applicable law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of the official authority.

Text messaging can be used to send marketing communications.

The relevant legal basis for processing used to be data subjects' prior consent. Section 47 of the GDPR, stating that direct marketing purposes may be carried out under the legitimate interest of the controller, led many to question the exact scope of application of the legitimate interest and whether it can serve as a legal basis for telephone marketing. The Garante has not made its position clear and guidelines are eagerly awaited, since the legitimate interest as a legal basis for processing in lieu of consent would ease the data collection process of most controllers.

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 controller's own products or services without the data subject's consent. The awaited e-regulation will probably clarify the issue.

It should be noted that consent – if any – to receive marketing communications via automated calling or further systems without human intervention (fax, SMS, email, MMS, recorded calls) is deemed to include consent to receive marketing communications via traditional means (paper mail), but not vice versa.

Regarding phone numbers processed for marketing purposes, the Opt-Out Register (Presidential Decree 178/2010) should be mentioned. This collects, on a voluntary basis, the telephone numbers as contained in publicly available paper or electronic directories of data subjects who do not want their data processed for direct marketing or advertising purposes, or else for carrying out market surveys or interactive business communication.

According to Law 5/2018, the Opt-Out Register shall include also mobile numbers and controllers processing phone numbers for marketing purposes are required 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.

Further to the amendment under Presidential Decree 149/2018, the Opt-Out Register shall also include physical addresses: therefore, by enrolling in the Opt-Out Register, data subjects may also object to the receipt of marketing communications sent in paper form to their residential addresses published in publicly available paper or electronic directories.

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; if it is a third country, a prior notice shall be filed to the Garante (as well as to the Ministry of Labour, the National Labour Inspectorate and the Ministry of Economic Development) 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 ROC (Register of Communication Operators) managed by AGCOM. In addition, pursuant to Law 5/2018, providers of call centre services shall update their phone numbers using the prefixes indicated by AGCOM, the aim being to ensure that data subjects are able to easily identify calls dialled for statistical or marketing purposes.

It is highly unlikely that no personal data is collected through a website (most websites have a 'contact us' section); therefore a privacy policy easily accessible from the website is compulsory.

According to Legislative Decree 70/2003 (transposing Directive 2000/31/EC), a website must also clearly state the identification and contact data of its owner.

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

Tracking cookies, or profiling cookies, shall be installed provided that website users:

- 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
- have granted their consent.

Concerns have been raised as to the suitability of a consent granted implicitly by continuing to use the website, as such consent might not meet the requirement of express and unambiguous consent under the GDPR. These concerns have been shared by the French courts, which fined a website for not having collected an explicit consent. As a result, most websites began to ask for an express and explicit consent for the use of cookies.

Data subjects' consent is required not only for tracking cookies, but also for analytics provided by third parties, which are assimilated to profiling cookies 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.

As far as technical cookies are concerned, the provision of a cookie policy is sufficient.

Data subjects must be granted control over processing of their personal data. A 'do not track' option gives data subjects the ability to make choices about which processing operations to allow.

Behavioural advertising requires profiling. Art29WP's guidelines on automated individual decision-making and profiling should be taken into account, in which it clarifies that no legal basis for processing shall be excluded a priori and confirms that behavioural advertising does not necessarily have to be based just on consent. The Garante has not yet made its position clear; guidelines are eagerly awaited.

Where consent is relied upon, it has to be borne in mind that 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 consent.

So-called 'social spam' results in unlawful processing; this has been clarified by the Garante in a number of cases.

The general principle that controllers shall bear in mind is that an email address published on a social network cannot be processed for whatever purposes based on the sole fact that it is publicly accessible personal data.

As far as video and television are concerned, the Garante has focused on data protection issues concerning interactive television services, recommending that controllers:

- give data subjects clear, easy-to-understand and exhaustive information on all the features of the processing (through a preliminary 'short' notice giving access to a secondary 'long' notice if a data subject wishes for 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.

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 the providers themselves. An exception is Legislative Decree 70/2003, which focuses mainly on the responsibility of contents providers for users' content; Legislative Decree 206/2005 (Consumers' Code) should also be mentioned. General rules of law, such as the Privacy Code and criminal provisions, also apply. AGCOM and AGCM (Antitrust Authority) are both active for surveillance.

The Garante has addressed the topic on several occasions, recommending that providers implement adequate security measures but focusing mostly on increasing 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 effective deletion. No social network account is actually completely private.

The right to be forgotten consists of 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 short, it is the right not to be publicly reminded long after the relevant event.

The GDPR is clear on the right to be forgotten – it states that data subjects can request 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 controller to take any reasonable steps to inform other controllers that 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.

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, even before the GDPR. Reference shall be made, inter alia, to the 'Google Spain case' (C-131/12) and to Art29WP's guidelines on its interpretation.

The same principles are also commonly applied by the Garante when balancing an individual's right to be forgotten with the public interest to be duly informed. In a 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 subsequently been reinstated and the news was outdated. In contrast, the Garante has confirmed the lawfulness of search results that, although referring to the same legal case, provide further information of actual public interest in light of the role of the data subject, who is still holding high-level public office.

One open issue is the territorial extension of the deletion of the personal data. Indeed, the GDPR does not clarify whether the deletion shall be limited to the EU or extended to the whole world.

The Garante, in a decision issued on 21 December 2017, ordered Google to de-list all search results regarding a data subject, without territorial limits; a similar decision was also taken by CNIL, which fined Google for having limited the de-listing to the EU.

The order issued by CNIL was challenged by Google, and the French court asked the European Court of Justice for a preliminary ruling on whether the deletion shall cover the whole world or be limited to the EU. To date, only the opinion of the Advocate General has been issued, and (in contrast to the decision of the CNIL) it is in favour of limiting the de-listing to the EU.

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

On cyber-bullying, Law 71/2017 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. The aim is to prevent, rather than repress, acts of cyber-bullying through proper education.

As for disinformation, both the Garante and AGCOM are constantly fighting against fake news by increasing users' awareness and social media and social networks' commitment.

The right to data portability is governed under the GDPR, being new to Italy. It is defined as a data subject's right 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 with or without transmitting the 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 is carried out through automated means. Moreover, it will cover only the personal data of the requesting data subject (which does not concern other data subjects) that 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 controller on the basis of the data provided by a data subject are excluded.

This right is without prejudice to other rights granted to data subjects, who shall continue to use the controller's service even after a data portability operation (which does not automatically imply erasure of data).

These and further issues are addressed in Art29WP's guidelines.

There has been a case involving Facebook and WhatsApp, concerning the consent collected in 2016 by WhatsApp to the communication of personal data of Italian data subjects to Facebook for behavioural advertising purposes.

The consent was found to be unlawfully collected, since:

- the information notice was not comprehensive (ie, it did not highlight the amendments to its previous version, it was not easy to understand, and the purposes for processing were not duly explained); and
- the consent itself was not expressly, specifically and freely granted, having been collected through the opt-out mechanism and under the threat of disruption of a service that has become of general use (ie, a disproportion-

ate consequence compared to the relevant operational needs).

The Garante also stressed that the legitimate interest could not be invoked in that case, since the balancing test had not been performed and nothing had been provided to verify whether the processing was actually necessary to pursue the declared interest.

With effect from 4 October 2018, both Facebook and WhatsApp were prevented from further processing data that had been unlawfully collected.

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

As far as the offer of information society services is concerned, the Privacy Code sets the threshold at 14 years of age (under Article 8 of the GDPR).

Schools and educational institutions are bound by a duty of publicity and transparency. The Garante has issued guidelines to help in complying with both transparency and data protection.

The Privacy Code facilitates vocational orientation and training as well as employment in Italy and abroad, allowing high schools and other educational bodies to communicate or disseminate data on the evaluation and marks obtained by students, as well as to private entities and by electronic means, upon the data subjects' request, provided that such data is relevant for the mentioned purposes and that data subjects have been duly informed thereon.

2.3 Online Marketing

The possibility to base marketing on the legitimate interest instead of consent seems to have been introduced by Recital (47) of the GDPR (according to which the legitimate interest of the controller or of a third party might be a suitable basis for the processing of personal data for marketing purposes, thus excluding the need to collect data subjects' consent) but has not yet been addressed either in guidelines from the EDPB, nor in guidelines issued by the Garante.

When needed, 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.

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. 'Marketing' includes advertising materials, direct selling, surveys and commercial communications, since they 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 identify the means of delivery of marketing communications (either conventional marketing channels, systems without human intervention, or both). Data subjects shall be 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, without affecting the lawfulness of processing based on consent before its withdrawal.

The above issues are addressed in Garante's 'Guidelines on Marketing and against Spam,' which shall be deemed to still be in force insofar as they are consistent with the GDPR.

Art29WP's guidelines on automated individual decision-making and profiling shall be taken into account where they clarify that no legal basis for processing shall be excluded a priori and confirm that behavioural advertising does not necessarily have to be based solely on consent. The Garante has not taken a position on this yet; guidelines are eagerly awaited.

Where consent is required, it has to be borne in mind that this processing operation corresponds to a specific purpose and, therefore, it shall not be deemed included in the definition of 'marketing,' thus requiring a separate consent.

Location-based advertising is ruled in the same way as behavioural advertising – data subjects shall be informed of the collection of data concerning their geographical position and, when used as a legal basis for processing, a separate, specific and unambiguous consent shall be collected thereon.

Where it results in systematic monitoring of a publicly accessible area on a large scale, a DPIA will have to be performed.

2.4 Workplace Privacy

As to the processing of employees' personal data, the Garante has issued several guidelines that clarify employers' (controllers') duties and employees' (data subjects') rights under the applicable data protection law, provided that sectorial provisions such as the Workers' Statute remain unaffected.

The contents of email messages are subject to confidentiality safeguards under Constitutional principles and criminal law.

An employer is therefore, in principle, not entitled to read emails sent and/or received by employees on their business account.

To reconcile the need to ensure that work duties have been actually discharged and/or that work tools are used appropriately as regards employees' dignity and freedom, employees shall be clearly informed on whether, to what extent, how and for what purposes controls are carried out, with the privacy policy to be delivered when establishing the employment relationship. Internal guidelines shall be adopted and made known to employees (such as via an intranet, or by displaying them in the workplace, etc) to make clear that company devices (personal computers, mobile phones, business email addresses) must be used only for professional purposes, so that employees cannot reasonably contend that incoming and/or outgoing emails are to be kept confidential.

Article 4 of the Workers' Statute 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 or surveillance systems. Although equipment normally used within the execution of the employment relationship shall be deemed exempt from trade union approval, this exemption shall be interpreted restrictively; therefore, it cannot be used to avoid trade union approval for software used to monitor employees' email, since this kind of software (unlike the personal computer) is not necessary for the fulfilment of employees' obligations. The same principles concern surveillance systems, which shall also be subject to a DPIA.

Employees' consent shall not relieve the employer from its obligations under the Worker's Statute – as recently stressed by the Supreme Court, the consent of the employee might not be effective since employees are seldom in a position to give, refuse or revoke consent freely, given the dependency inherent in the employer/employee relationship. This was also highlighted by Art29WP, which stated that employees' consent is highly unlikely to be a legal basis for data processing at work unless employees can effectively refuse without adverse consequences.

The Garante also clarified that data collected via company devices such as mobile phones with the aim to control and limit costs incurred by the employer shall not be processed for disciplinary purposes and shall only be retained for six months.

Labour organisations and trade unions act as representatives for their respective members, to protect their rights and interests. Under the Workers' Statute, they shall be informed of, and are empowered to be consulted on and approve, the deployment – by the employer – of equipment intended to monitor employees.

Under Law 179/2017, companies that have adopted the internal corporate model of organisation and management (the 'Model') according to Legislative Decree 231/2001 against corporate crimes ('Law 231') 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 to the reporting, and penalties shall be imposed against whoever breaches measures to protect whistle-blowers.

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, but the Privacy Code limits the exercise of the rights granted to data subjects to ensure effectiveness of the protection of the privacy of the whistleblower.

The Garante has issued guidelines advising how to deal with business email accounts of former employees to reconcile the employer's need to access information necessary for business management with employees' confidentiality expectations. Measures include immediate de-activation of the relevant account and automatic messages to inform third parties of the new address to which business communications should be addressed. Employees shall be duly informed of the procedure adopted by the employer with internal guidelines.

In the case of unsolicited applications, the information notice shall be provided by the controller to the data subject at the time of the first contact after receipt of the curriculum vitae, and no consent is required.

2.5 Enforcement and Litigation

There are no legal standards for regulators to allege violations of data protection laws; assessment is made on a case-by-case basis.

Under the GDPR, infringements of data protection provisions are subject to administrative sanctions up to EUR20 million or, in the case of an undertaking, up to 4% of total worldwide annual turnover of the preceding financial year, whichever is higher. The Privacy Code does not set a minimum, nor define ranges.

Criminal penalties ruled under the Privacy Code shall be imposed by the judicial authority and consist of imprisonment from six months to six years, depending upon the seriousness of the infringement.

Facebook has been fined by the AGCM for unfair and aggressive commercial practices consisting of unlawful processing of personal data. Users were not sufficiently informed of the profiling and the communication of personal data to third parties; they were not allowed to grant their consent to the sharing of personal data with third parties; and they were not

aware of the fact that their data was processed to the profit of the social network (despite the claim of the free-of-charge creation of an account). The fine amounted to EUR10 million in the aggregate, in addition to a public declaration of the sanction suffered and its grounds.

There are no legal standards that authorise private litigation for alleged violations of data protection laws. Verification is on a case-by-case basis and actual circumstances are taken into account.

The administrative process for the examination of complaints filed to the Garante is ruled under a regulation to be adopted by the Garante itself.

Individuals can elect to be represented by not-for-profit organisations. Collective organisations representing specific categories of controllers or processors for general purposes may also draw attention to an infringement of the relevant data protection laws, or lodge a report to draw the Garante's attention to possible breaches.

There have been no major private litigation cases in the last 12 months; however, it is important to stress that in 2017 the Garante issued penalties amounting to EUR 3,776,694 in the aggregate.

From 25 May 2018 to 31 December 2018, 4,704 claims and warnings were filed to the Garante, as compared to 3,378 in the same period in 2017.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Legislative Decree 51/2018 repealed those provisions of the Privacy Code ruling personal data processing by police authorities.

The new set of rules introduced derogations and specifications to the 'general' provisions of the GDPR. Such rules are self-standing, and not limited to amendments or additions.

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

Privacy is protected by limits to law enforcement access to data, as well as by those provisions applicable to processing by public authorities and judicial authorities as provided under Legislative Decree 51/2018.

The processing of 'judicial' data, referred to as "data relating to criminal convictions and offences," is subject to tight constraints (see Article 10 of the GDPR).

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-bis of the Privacy Code).

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

Although Legislative Decree 51/2018 excludes from its scope the processing of personal data for national security purposes, the Privacy Code extends the applicability of some of the provisions of the above-mentioned Decree to such processing activities, namely definitions, general principles, automated decision-making (including profiling), privacy by design and privacy by default, processors, security measures, supervisory authority, compensation rights, administrative fines and criminal sanctions.

Law 124/2007 governs the Italian national security information system and state secrets.

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.

Privacy is protected by limits to law enforcement access to data, as well as by those provisions applicable to processing by public authorities and judicial authorities as provided under Legislative Decree 51/2018.

The processing of 'judicial' data, referred to as "data relating to criminal convictions and offences," is subject to tight constraints (Article 10 of the GDPR).

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 (Article 160-bis of the Privacy Code).

3.3 Invoking a Foreign Government

Foreign government access requests might be a legitimate basis on which to collect and transfer personal data if based on important reasons of public interest, which shall be recognised by EU or national law.

Legislative Decree 51/2018 also provides for specific derogations to the transfer of personal data. A foreign government access request is not expressly listed; nevertheless, based on the circumstances of each case, it might be traced back to one or more of the lawful bases expressly provided.

3.4 Key Privacy Issues, Conflicts and Public Debates

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

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 freely available among EU Member States because it is taken for granted that data subjects receive an adequate level of protection in all EU countries.

The transfer of personal data to third countries 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 by issuing an adequacy decision;
- under appropriate safeguards such as binding corporate rules and/or standard data protection clauses adopted by the European Commission; or
- when one of the derogations under Article 49 GDPR applies, such as the data subject's consent, the need to perform a contract or implement pre-contractual measures, or the establishment, exercise or defence of legal claims. These derogations are discussed in EDPB's guidelines.

Where none of the above is applicable, a transfer may occur only if it is not repetitive, it concerns only a limited number of data subjects, is necessary for the purposes of the controller's compelling legitimate interests and not overridden by the interests or rights and freedoms of the data subject, and under suitable safeguards. The Garante shall be informed beforehand.

Privacy Shield is an agreement between the EU and the US, providing for the specific commitments of public and private entities to ensure the effective protection of EU data subjects' personal data. After the second annual review of the Privacy Shield, the EDPB raised concerns over:

- the lack of concrete assurances that indiscriminate collection and access of personal data for national security purposes are excluded;
- the sufficiency of powers conferred to the newly appointed ombudsperson; and
- the strength of checks regarding compliance with the substance of the Privacy Shield's principles.

An adequacy decision concerning Japan has recently been adopted, creating a wider space for safe transfer of personal data, and binding Japanese companies to supplementary rules when processing personal data transferred from the EU.

4.3 Government Notifications and Approvals

No government notifications or approvals are required to transfer data internationally.

Special requirements might apply to categories of personal data of a more sensitive nature (such as 'judicial' data, or information covered by business and industrial secrecy).

4.4 Data Localisation Requirements

There is no general duty to maintain data in-country.

4.5 Sharing Technical Details

No software code, algorithms or similar technical detail are required to be communicated to the government. Nevertheless, the Garante (as well as any other relevant public authority) is entitled to ask controllers and processors for such information.

4.6 Limitations and Considerations

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.

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 based on sectorial laws (such as 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 relevant provisions on data protection. Concerns have been raised by the Garante in that Big Data is too innovative for the easy application of data protection rules.

On 30 May 2017, the Garante, the AGCM and the AGCOM undertook a public survey on Big Data, aimed at identifying risks and defining rules to protect personal data, consumers and the digital economy. The final outcome has yet to be disclosed.

The GDPR broadens protection 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 only legitimate 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 the data subjects and the controller; and
- the decision is authorised by applicable law.

The Garante has addressed profiling mainly from the perspective of marketing and advertising, highlighting the need for specific consent and issuing guidelines on online profiling to suggest a double-layered information notice. These guidelines and measures are still applicable as far as they are consistent with the GDPR, which might entail a different legal basis for processing to be used.

Art29WP's guidelines on automated individual decision-making and profiling are also relevant.

Artificial intelligence has garnered a great deal of attention recently.

In March 2018, Agid (Agency for Digital Italy) issued a white paper on artificial intelligence and its potential benefits in the public sector, and also set up a task force.

In January 2019, two groups of experts were appointed to work with the Ministry of Economic Development to develop an Italian strategy on artificial intelligence and blockchain to be discussed at a European level.

In February 2019, the legal enforceability of both smart contracts and distributed ledger technology time-stamping was recognised, thus equating a smart contract to a written contract.

Finally, the Committee of the Council of Europe's Convention 108 also issued guidelines.

The main issues concern system accountability and transparency of the choices made by algorithms through tracking. Article 22 of the GDPR, dealing with autonomous decision-making, has been criticised as limiting artificial intelligence in that it grants the right to obtain human intervention.

Risks related to the IoT have been assessed by Art29WP's opinions.

The Garante has drawn controllers' attention to the need to ensure effective data protection by design and by default and duly to inform data subjects.

Autonomous decision-making has to be deemed subject to the same rules provided for automated decision-making, as long as it entails personal data processing.

Facial recognition entails the processing of biometric data and is subject to the same rules (see below). Art29WP's opinions thereon should also be mentioned, highlighting – inter alia – that facial recognition might also involve 'sensitive' data processing.

Biometric data is classed as 'sensitive' data when used for the purpose of uniquely identifying a natural person.

The Garante has issued guidelines on biometric recognition and graphometric signatures. Any processing of biometric data that 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.

These guidelines shall be deemed to be still in force as long as they are consistent with the GDPR. On the one hand, it is certain that no prior authorisation shall be obtained (the prior consultation of the Garante might nevertheless be necessary, based on the outcome of the DPIA – when required); on the other, it is uncertain if the deadline to notify a breach will remain at 24 hours or whether the broader deadline of 72 hours provided under the GDPR will prevail.

Geolocation data is considered personal data.

In a recent decision on GPS installed on vehicles provided to employees, the Garante stressed the need to include the 'right to privacy' in the functionalities of the car itself, paying attention in particular to the data-minimisation principle as well as to those of privacy by design and by default.

Article 4 of the Workers' Statute shall also apply; therefore, unless 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 agreement with trade unions.

The use of drones raises a number of privacy issues, mainly related to a lack of transparency of processing operations due

to the difficulty in knowing what equipment is on board and by whom and for what purposes personal data is being collected. Drones' potential to invade the privacy of individuals is also acute, due to their ability to avoid obstacles and achieve unique viewpoints.

Criminal law provisions have to be taken into account when recording other people's conversations or private spaces (ie, a house or private garden).

Regulations issued by ENAC (National Civil Aviation Entity) and on CCTV systems are also relevant.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

The NIS Directive aims to improve cybersecurity, increasing the level of security of networks and information systems with specific regard to services vital to the EU, as well as improving cooperation at EU level. Italy has implemented the NIS Directive with Legislative Decree 65/2018 ('NIS Decree'), addressed to providers of essential services and key digital service-providers (such as search engines, cloud computing services and online marketplaces).

Digital service-providers shall comply with the Commission Implementing Regulation (EU) 2018/151, laying down rules for application of the NIS Directive as regards further specification for managing the risks and parameters for determining whether an incident has a substantial impact.

Other relevant laws include:

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC ('EIDAS Regulation');
- Directive 2013/40/EU on attacks against information systems, replacing Council Framework Decision 2005/222/JHA;
- the Criminal Code;
- Legislative Decree 259/2003 ('Electronic Communications Code'); and
- Legislative Decree 82/2005 ('Digital Administration Code' or 'CAD') and its implementing ministerial decrees.

ENISA is an advisory board for the EU on cybersecurity issues, actively promoting a high level of network and information security.

ENISA actively liaises with the Multi-Stakeholders Platform on ICT standardisation, an advisory expert group on all matters related to European ICT standardisation, as well as the CEN-CENELEC Focus Group on Cybersecurity (CSCG), which was created by European Standardisation Organisations (CEN, CENELEC and ETSI) to provide support for the analysis of technology developments and the issuance of recommendations for international standard-setting.

The OSCE (Organisation for Security and Co-operation in Europe) is also active in cybersecurity – its aim is to increase trust among Member States.

The Garante is in charge of receiving data breach notifications and checking the adequacy of the organisational and technical measures adopted to protect personal data, as well as to recommend actions and impose fines in the case of infringements.

The NIS Decree expressly requires the NIS Authorities (five ministries have been duly appointed in Italy) to consult and co-operate with the Garante.

Agid oversees the execution of the Italian digital agenda and compliance with the European digital agenda. Its tasks include the issuance of opinions, guidelines and technical rules, predominantly in the public sector.

Supervisory authorities, such as AGCOM, Banca d'Italia (the Central Bank of Italy) and IVASS (Institute for Private Insurances Supervision) are empowered to issue regulations and guidelines that might also concern cybersecurity (such as the Order of 17 December 2013 of Banca d'Italia, updated on 23 October 2018).

The CINI (Inter-university Consortium on Information Technology) is the main reference point for academic research on information technology. In partnership with CIS Sapienza (the Research Centre of Cyber Intelligence and Information Security of Sapienza Rome University), it regularly publishes reports on Italian cybersecurity, addressing essential cybersecurity controls.

The CLUSIT (Italian Association for Cyber Security) aims to increase awareness of cybersecurity among companies, public authorities and private citizens.

Assinform, the national association of information technology companies operating in Italy, is a private association representing companies of all sizes and specialisations and acts as a bridge between the IT sector and the main public Italian authorities.

6.2 Key Frameworks

Unless otherwise provided, recognised standards are not compulsory requirements, but rather tools to be used by controllers to identify the appropriate security measures to be implemented.

The UNI (Italian National Unification Entity) is a private not-for profit entity, recognised by both the Italian government and the EU and having been conferred legal status, that issues voluntary technical standards concerning all business sectors. UNI represents Italy at both CEN (European Committee for Standardization) and ISO (International Organization for Standardization), both of which are standardisation bodies.

Among many others, the ISO 27000 series appears to be the preferred standard to infer data protection security measures.

6.3 Legal Requirements

Written information security plans and incident response plans may, on a case-by-case basis, be appropriate security measures to notify data breaches and to detect a breach. They can also be used to notify breaches to the Garante, when necessary, within 72 hours after having become aware of the breach, and to adopt any due measures to mitigate the consequences.

According to the 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 component thereof."

This order provides for minimum provisions to be included in the appointment of a system administrator, and its consistency with the GDPR has been questioned. While waiting for an official decision from the Garante, many controllers are choosing to draft an appointment comprising compulsory elements of both a processor and a system administrator.

The board of directors (or the sole administrator) is the managing body of a company and is ultimately responsible for ensuring that appropriate measures are in place.

Internal risk assessments, vulnerability scanning, penetration tests and the like may be, on a case-by-case basis, appropriate security measures.

An insider-threat programme shall abide by the laws and principles concerning the control and monitoring of employees.

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. Their compliance shall be monitored.

When processing personal data, they shall be appointed as processors and all relevant provisions shall apply.

Training is a general duty of employers towards employees. Cybersecurity and data protection should be included in such training.

6.4 Key Multinational Relationships

Italy is a party to all major multinational relationships relating to being a member of the EU.

6.5 Key Affirmative Security Requirements

The GDPR provides for some examples of security measures that shall not be minimum compulsory requirements, including pseudonymisation and encryption. Adherence to approved codes of conduct and certification mechanisms helps demonstrate accountability.

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

The NIS Decree shall be relied upon when dealing with critical infrastructures. Operators shall assess appropriate measures based on their activities, taking into account guidelines and standards (if any) issued by relevant EU and national authorities (such as ENISA).

Digital service-providers can rely also on Commission Implementing Regulation (EU) 2018/151.

There is no legal security requirement to prevent denial of service attacks. Reference shall be made to general principles and rules, as well as to recognised standards.

6.6 Data Breach Reporting and Notification

Data-breach and security incidents' reporting is governed by both the GDPR and the NIS Decree.

Under the GDPR, a personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." In practical terms, a data breach is a type of security incident.

As to the NIS Decree, an incident means "any event having an actual adverse effect on the security of network and information systems," and security of network and information system means "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems."

All personal data may be the subject of a security incident or 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 the above.

No system is excluded from data breaches.

Two regulations must be mentioned – Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in vitro diagnostic medical devices. Both 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, they do not address security requirements in full detail. Reference shall thus be made to general data protection rules, especially those concerning 'sensitive' data, as well as to general standards (such as the ISO 27000 series, ISO 80001, ISO 14971, IEC 62304 and IEC 82304-1). Controllers and processors will have to assess the risks and implement adequate security measures to ensure protection, both by design and by default, according to the accountability principle.

ENISA guidelines should also be mentioned.

As with medical devices, Industrial Control Systems (such as SCADA) do not benefit from rules listing due to security requirements. General data protection principles, as well as general standards, shall help in the assessment.

ENISA has drafted a report listing most applicable standards.

No consolidated set of rules clarifies security requirements for the IoT.

Art29WP 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.

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 of the GDPR). The term for the notification is 72 hours after having become aware of the breach.

As to the NIS Decree, the duty to notify incidents without undue delay applies to providers of essential services and key digital service providers. The notification shall be made to the CSIRT and to the relevant NIS Authority. The CSIRT shall forward the notification to the Information Security Department in charge of the prevention of and preparation for crisis situations, as well as to the activation of alert procedures.

The NIS Decree entitles entities that do not fall under its scope to notify, on a voluntary basis, security incidents having a severe impact on the continuity of the services provided, following the same procedure as the compulsory notification.

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 of the GDPR), or if it is required by the Garante. The aim is to provide individuals with information on the measures to take to protect themselves.

As to security incidents, the relevant NIS authority, in agreement with the Information Security Department and the CSIRT, and subject to prior consultation with the service provider affected by the incident, might inform the public (or require the service provider to inform the public) of each incident with the aim of raising awareness and preventing future incidents, or managing an incident already occurred.

Both the GDPR and the NIS Decree do not provide for the duty to notify the data breach to companies or organisations that are not directly concerned by the breach itself.

The criteria to understand whether a data breach has to be notified is the likelihood of "risk to the rights and freedoms of natural persons" – therefore risk is a trigger for notification. Based on the seriousness of the risk, the breach might also have to be communicated to each data subject affected by the breach itself. Art29WP and ENISA have provided guidelines on the assessment of risk.

As to the NIS Decree, the main criteria to understand whether an incident has to be notified is its effect on the security of network and information systems.

6.7 Ability to Monitor Networks for Cybersecurity

Network monitoring shall be permitted according to applicable data protection rules and principles.

6.8 Cyberthreat Information Sharing Arrangements

The NIS Decree provides for the notification of security incidents to be forwarded to governmental authorities such as NIS authorities and CSIRT. These authorities might have to involve the relevant EU authorities, based on the severity of the incident.

The NIS Decree expressly entitles entities other than operators of essential services and digital service-providers to notify, on a voluntary basis, an incident having a significant impact on the continuity of the services that they provide.

The procedure to be followed is the same as that ruled for compulsory notifications, except for the fact that compul-

sory notifications are granted priority over voluntary notifications.

6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

In 2016, Uber suffered a severe data breach. During the investigation into the consequences of the breach for Italian citizens, the Garante ascertained that the information notice provided by Uber was not compliant with relevant data protection provisions and no consent had been collected to profile users for anti-fraud purposes. In addition, no notification for the geolocation data of Uber users had been made to the Garante, as required by the Privacy Code prior to the entry into force of the GDPR. An autonomous fining procedure was therefore started in December 2018 and is currently ongoing.

In May 2018, the Garante issued a fine of EUR160,000 to the main Italian telecom operator for a data breach that occurred in 2013. The breach, arising from a malfunctioning of services provided to clients, consisted of the disclosure of personal data to other clients due to a mistake in the matching of credentials with the data to be displayed.

In December 2018, the Garante ordered a major bank to notify data subjects of a data breach suffered a couple of months before and already communicated to the authority, granting a short timeframe to confirm such notification and the remedial actions taken.

After the entry into force of the GDPR, data breach notifications appear to have increased. From 25 May 2018 to 31 December 2018, 630 data breaches were notified to the Garante, whereas cyber-attacks increased by 500%.

LCA Studio Legale

Via della Moscova 18
20121 Milan
Italy

Tel: +39 027788751
Fax: +39 0276018478
Email: milano@lcalex.it
Web: www.lcalex.it