The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-32-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 15

ITALY

Daniele Vecchi and Melissa Marchese[1]

I OVERVIEW

The Italian Privacy Code, set out in Legislative Decree No. 196 of 30 June 2003, was approved on 27 June 2003 and published in the Italian Official Journal on 29 July 2003. It entered into force on 1 January 2004.

Although indirectly ascribable to the right to personal identity and dignity set out in Articles 2 and 3 of the Italian Constitution of 1947, and subsequently recognised by the Court of Cassation,[2] it was only in 1996, with the implementation in Italy of the European Data Protection Directive No. 95/46, that the 'right to the protection of personal data' was formally translated into legal provisions through Law No. 675 of 31 December 1996, the Act for the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data (Privacy Act 1996).

It is worth mentioning that the initial legal approach to the right to privacy and protection of personal data, in both the Privacy Act 1996 and the current Privacy Code of 2004, was one of all-embracing applicability: the privacy provisions applied 'to everyone', so that this term referred to both natural and legal persons, and thus in the broadest meaning of the European Data Protection Directive. Only in 2011, through Law No. 214, were the definitions of 'personal data' and 'data subject' changed to make them refer exclusively to natural persons. The protection of the privacy of legal persons, bodies and associations is maintained only for specific activities, such as marketing.

The Privacy Code, in common with the Privacy Act 1996, sets out detailed requirements and measures aiming at ensuring that personal data is processed in accordance with data subjects' rights and fundamental freedoms, particularly with regard to personal data protection and confidentiality. This is ensured by means of binding provisions and

1 Daniele Vecchi is a partner and Melissa Marchese is counsel at Gianni, Origoni, Grippo, Cappelli & Partners.

2 Decision No. 4487 of 1956 and Decision No. 990 of 1963.

'minimum' obligations in data security applicable both to manual and electronic processing operations involving personal data. Nevertheless, in diverse and specific areas – from national security and public interest, to the carrying out of investigations by defence counsel and the journalistic freedom of the press – the protection of data subjects' privacy and rights established by the Privacy Code may call for the application of the 'balancing of the interests'. This will often take into account the principles of proportionality, lawfulness and necessity to create exemptions from the aforementioned mandatory privacy requirements of the data subject to an overriding interest.

In addition to the general principles and rules set out by the Privacy Code, a number of provisions and guidelines provided by the Garante, the Italian data protection authority, as well as specific 'ethics codes' attached to the Privacy Code and issued to given sectors (such as, as mentioned, journalistic activities, but also data processing concerning credit reliability and commercial information, statistics and scientific purposes, etc.), touch on privacy issues and contain measures and obligations for the protection of personal data.

This chapter gives a brief overview of the current Italian legislative framework on privacy, and the relevant obligations and implications for organisations collecting and processing personal data. We also focus on stand-alone privacy issues arising from particular issues (such as marketing and profiling activities, international data transfers and data breaches), and set out the major enforcement actions and recent developments in Italy.

II THE YEAR IN REVIEW

It is not surprising that most of the activity carried out by the Garante during the past year concerned the conclusion of the legislation giving effect to the new General Data Protection Regulation and the Directive on the processing of personal data for the purposes of crime prevention and prosecution adopted by the European Parliament and the Council.

However, this has not been its only remit: in the last few months of 2015, the Garante took numerous and frequent decisions in response to data subjects' requests for de-indexation of personal data and information contained in the lists of results of Google's search engine under the 'right to be forgotten'. Furthermore, the Garante has issued several general provisions concerning unusual and 'sensitive' matters, especially in light of the spread of new technologies in emerging sectors, such as information systems in the health field.

Major enforcement actions were also carried out in the field of employment relationships and the use, by employers, of electronic systems that can monitor employees' working activities[3] without the implementation of appropriate privacy safeguards. In addition, the Garante has been active in relation to non-compliance by websites in the collection of users' personal data for the supply of online registration and services, and then processing the data for marketing and profiling purposes. Several proceedings led to the adoption of inhibitory and sanctioning orders.

Finally, the Garante has also issued individual decisions and sanctioning provisions against important national electronic communications providers following notifications of data breaches within their organisations.

3 In this respect, a reform has recently amended Italian Law No. 300 of 20 May 1970, the 'Workers' Statute'.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Under the Privacy Code – further to the aforementioned reform in 2011 with Law No. 214 and in line with the old privacy Directive No. 95/46 – 'personal data' is any information relating to identified or identifiable natural persons, even if it relates to them indirectly, by reference to any other information such as personal identification numbers.[4] It follows that none of the provisions of the Privacy Code applies to anonymous data, which means data that either in origin or after having been processed cannot be associated with any identified or identifiable data subject. On the contrary, when data permits a data subject to be – whether directly or indirectly – identified, the privacy obligations and requirements set out by the Privacy Code must be fulfilled. In addition, in the case of disclosure of 'sensitive data' (data allowing the disclosure of racial or ethnic origin, religious beliefs, political opinions, health and sex life) or 'judicial data' (personal data disclosing judicial measures taken in respect of a person and included in that person's criminal record[5]), further protection and additional measures (e.g., written consent from data subjects, authorisation by the Garante) must also be complied with.

Finally, the application of the Privacy Code is excluded for the processing of personal data carried out by natural persons for personal purposes only, provided that such data are not intended for systematic communication or dissemination.

The data controller

The data controller is the first point of reference for the obligations and liabilities provided by the Privacy Code. It is the individual, company, association or other entity that is factually in control of the processing of personal data and empowered to take the essential decisions on the purposes and mechanisms of that processing, including the security measures to be adopted. In relation to data processing operations performed by a company or a public or private body, the Garante has repeatedly clarified that it is the entity as a whole that acts as data controller, rather than the individual or department representing the entity (such as the legal representatives, chairperson, etc.). In fact, the data controller is only usually an individual in processing carried out by entrepreneurs or self-employed professionals.

The data processor

According to the Privacy Code, the data controller is entitled, on a discretionary basis, to appoint one or more data processors to carry out and supervise the processing of personal data carried out within the data controller's organisation and under the instructions given in writing by the latter. The data processor may be a natural or a legal person; however, it must have adequate knowledge and experience and be sufficiently reliable to ensure that the privacy obligations and measures are fully complied with. In fact, even though the data controller

4 Article 4, Letter b) of the Privacy Code.

5 Such as final criminal convictions, parole, residency or movement restrictions, and measures other than custodial detention. Being a defendant or the subject of criminal investigations also falls within the scope of the definition of judicial data.

delegates the processing of personal data and respective privacy duties to the data processor, the data controller remains under a duty to verify, including by means of periodic checks, the compliance of the activities carried out by the data processor with the instructions provided.

The persons in charge of the processing

While the appointment of a data processor is optional, it is compulsory under the Privacy Code to identify and appoint individuals that materially carry out the processing operations within the data controller's organisation, and on behalf of the same, as 'persons in charge of the processing', and to provide them with detailed written instructions referring to the scope of the operations allowed. This requirement is also fulfilled if the individual is entrusted with the task of directing a department, on a documentary basis, where the scope of the processing operations that may be performed by the staff working in that department has been specified in writing.

ii General obligations for data handlers

According to the Privacy Code, personal data cannot be collected and further processed unless the purposes of the collection and processing are pre-determined, explicit and legitimate; the data is proportionate, relevant and not excessive with respect to such purposes, as well as accurate and kept up to date; and it is retained for no longer than necessary for those purposes. Compliance with these fundamental conditions is essential for lawful data collection and processing; their violation could lead to the issuance – both by the Garante and by any court asked to deal with the matter – of orders of stop of processing, this practically resulting in a block of the data.

Before collecting personal data from a data subject, the data controller must provide complete and clear information as to the intended data processing operations. This must be through a simple but adequate notice detailing:

a the purposes and methods of the collection and processing;
b the mandatory or voluntary nature of providing the data;
c the entities involved in processing or receiving the data;
d the identity of the data controller and, where appointed, the data processor; and
e the data subject's privacy rights and how to enforce them.

However, where the data is not collected directly from data subjects, the obligation to provide the above information is postponed to the time when the data are recorded or, if the data are disclosed to third parties, no later than the moment of the first disclosure.

Furthermore, all processing of personal data is subject to obtaining prior, express consent from data subjects, except in the exempted circumstances expressly listed in the Privacy Code. These exempted circumstances include:

a when the processing relates to data collected under an obligation set out by laws, regulations or EU legislation;
b data retrieved from public records, lists and documents that are publicly accessible;
c when it is necessary for carrying out investigations by defence counsel or to establish or defend a legal claim; and
d when it is necessary for the purpose of performing an agreement to which the data subject is a party or to comply with specific requests by the data subject prior to entering into an agreement.

The Privacy Code requires the consent to be voluntary, specific and for a clearly identified processing operation. It should also be 'documented in writing' when non-sensitive personal data are concerned. When the data intended for collection and processing consist of sensitive data, the consent required for legitimate processing must be in written form (which, for electronic procedures, may be by means of an electronic signature).

Finally, in relation to both sensitive and judicial data, any processing or storage by data controllers must be preliminarily authorised by the Garante: to this extent, a number of general authorisations have been issued officially allowing the processing of these data by specific categories of data controllers (e.g., controllers operating in the fields of employment relationships, health, banks and insurance companies), so that the data controller is required to apply for an individual authorisation only if the specific data processing falls outside the area of the general authorisations.

Database registration requirements

Even though no general database registration requirement is established, the Privacy Code requires data controllers operating in some specific data processing fields to file a notification with the Garante prior to the beginning of the processing. The notification is an *ad hoc* form to be filled in electronically and signed digitally, and accompanied by a fixed contribution fee; it needs to be made only once in relation to the specific data processing, regardless of the number of transactions and duration of the same. A further notification must be filed – or the original modified – only in the case of changes in the original information contained in the first notice (e.g., additional categories of data subjects, participation of another data controller).

Specifically, the above notification must be filed for data collection and processing operations involving:

a genetic data, biometric data, or data disclosing the geographic location of individuals or objects by means of an electronic communications network;

b data disclosing health, sex life and psychological issues with the help of electronic means and for particular purposes (such as assisted reproduction and provision of healthcare services);

c data aimed at profiling data subjects and analysing their consumption patterns and choices, or at monitoring use of electronic communications services (except for processing operations that are technically essential to deliver those services);

d sensitive data stored in data banks for personnel selection purposes on behalf of third parties or used for opinion polls and sample-based surveys; and

e data stored in *ad hoc* data banks managed by electronic means in connection with data subjects' creditworthiness, assets and liabilities, appropriate performance of obligations, unlawful or fraudulent conduct (which could include internal whistleblowing schemes that, in Italy, are still not regulated by specific data protection provisions).

Furthermore, the recent guidance published by the Garante in relation to cookies sets out the obligation on websites to notify the Authority if they are using profiling cookies and third-party analytics.[6]

6 In relation to third party analytics cookies, this does not apply where the users' data is collected through anonymisation mechanisms such as disguising the IP address, and the third

Rights of data subjects

Under the Privacy Code, data subjects may access and obtain information concerning their personal data by making a request to the data controller, the data processor or the competent persons in charge of the processing. The data subjects' rights of access to their personal data are broad. They are entitled, for instance, to obtain confirmation of the existence and the source of their personal data, the criteria and purposes that have been used for the processing, the communication of the data, and the correction, integration or update of any inaccurate or incomplete data, as well as the erasure or blocking of the data processed in breach of the law (by way of example, without the data subject's consent). According to Garante decisions, a data controller's evaluation based on data subjects' data (for instance, the assessment of employees' productivity) are also to be regarded as personal data, and have to be made available to requesting data subjects.

A data subject may also require that a data controller stops processing personal data for direct marketing activities, for sending advertising materials or for market research purposes.

The above requests are not subject to any formalities or fees, save for certain cases where the existence of the personal data concerning the data subject is not confirmed, the personal data are contained on special media the reproduction of which is specifically requested, or if a considerable effort is required by the data controller on account of the complexity or amount of the requests for the data. However, the fee cannot be in excess of the costs actually incurred by the data controller in fulfilling the request and, in any event, must be less than the limit specified by the Garante.[7]

iii Technological innovation and privacy law

In recent years, both the Privacy Code and the provisions of the Garante have paid particular attention, through specific rules and guidance, to new technology that raises important data privacy issues, including the following:

Restrictions on cookies

The implementation in Italy of Directive 2009/136/EC brought about the introduction, through the Privacy Code, of the obligation to obtain informed consent from users or subscribers for the storage and use of information collected from their computer terminal, unless that storage or use is aimed exclusively at carrying out the transmission of a communication through an electronic communications network or providing an information society service explicitly requested by the user or subscriber.[8] In light of this, in both 2014 and 2015 the Garante issued specific provisions and guidelines for data controllers processing personal data through cookies. These set up rules and privacy measures for providing users or subscribers with information notices in accordance with simplified arrangements, as well as with user-friendly configurations to obtain their unambiguous consent.

party does not cross reference the collected information with other data already held by them (e.g., in relation to other online services provided).

7 Namely, €20, as set out in Decision of 23 December 2004.

8 In addition, consistent with Opinion 04/2012 on Cookie Consent Exemption by the EU Article 29 Working Party, this is the case for technical cookies.

Location tracking

As previously mentioned, processing operations involving the collection of geolocation data must first be notified to the Garante. Furthermore, in 2011, the Garante specifically addressed the issue of vehicle geolocation systems used by employers to meet organisational or production requirements and their interaction with personal data protection legislation. The Garante imposed certain privacy requirements, such as the prohibition on continuous monitoring of vehicle location, as well as the posting of stickers bearing the notice 'geo-located vehicle' inside vehicles as a simplified information notice pursuant to the transparency principle. In 2014, the Garante also authorised two telephone companies to use their employees' geolocation data collected through apps installed on their work smartphones[9] exclusively for the purposes of organisational and production needs.

Employee monitoring

With Legislative Decree No. 151 of 14 September 2015, the legislation that was previously in force, which prohibited any remote monitoring by the employer of the employee and required the carrying out of lawful checks on employee working activity to be agreed in advance with work councils, was changed. The new legislation allows the employer to 'perform checks on the instruments used by employees to carry out their professional tasks' and to use the relevant data 'for all the purposes connected to the employment relationship'. However, employees must always be informed in advance of the purposes and methods of this monitoring, as established by the Guidelines issued in 2007 by the Garante and that apply to the use of e-mails and the internet in the employment context. In this respect, the Garante has encouraged the adoption of 'privacy by design' monitoring solutions, and in June 2015 declared the monitoring of an employee's Skype conversations by an employer to be unlawful and in violation of privacy principles.

Facial recognition technology

Since facial features fall within the definition of biometric data, processing based on data subjects' facial recognition is also subject to the obligation of prior notification. Furthermore, in this regard, on 12 November 2014, the Garante issued a general provision – and provided exhaustive guidelines – concerning biometrics. The provision expressly authorised certain processing operations on biometric data, and also confirmed the requirement of the prior-checking request to the Garante[10] for the remaining biometric technology, among which was facial recognition systems. Subsequently, in June 2015, the Authority authorised the processing of biometric data by a facial recognition tool of passengers on holiday cruises.

Online behavioural advertising and profiling

In March 2015, following the issuance of a prescriptive order by the Garante against Google Inc concerning changes by the latter to its users' privacy policy and subsequent profiling

9 Provisions of 9 October 2014 and 11 September 2014.

10 Prior checking is an obligation expressly provided by Article 17 of the Privacy Code for data processing operations likely to present specific risks to data subjects' fundamental rights, freedoms and dignity on account of the nature of the data, the arrangements applying to the processing or the effects the latter may produce.

activities,[11] the Authority released guidelines for data controllers that, by offering publicly accessible online services, also analyse users' online behaviour and carry out profiling activities for targeted advertising. Included in these guidelines is the use of 'layered' information notices and banners disclosing the monitoring and that request the user's acceptance.

Electronic marketing

Both the Privacy Code and the Garante's Guidelines on marketing and against spam of 4 July 2013 require specific and informed consent from both data subjects and 'contracting parties' – which include legal persons, bodies and associations – for the sending of marketing materials, promotional communications, surveys and market research through electronic means (such as e-mail, fax, SMS, MMS). The opt-in consent must be entirely voluntary, which means that it cannot be the default setting (e.g., a pre-checked box). Nor can it be – factually or implicitly – a precondition to obtain the product or service being offered by the data controller.[12]

Internet of things (IoT)

In March 2015, the Garante started a public consultation on new technology falling within the category of IoT devices. The consultation was aimed at addressing the risks for personal data processing arising from the interconnection of different objects and systems such as personal computers, smartphones and other everyday things. The Garante collected proposals and remarks from relevant stakeholders in order to establish a suitable set of applicable privacy rules. In April 2016, the Authority – in coordination with the international network, GPEN – started 'privacy sweep' investigations on the IoT. The sweep is concentrating on domotic technologies to ascertain the degree of transparency in the collection and use of consumers' personal data, and the compliance with privacy rules by operators and companies, including multinational corporations, operating in the sector.

Cloud computing

Although still not specifically governed by the Privacy Code or provisions from the Garante, in the past few years the latter has provided guidance to both private and public organisations to highlight the major privacy issues and risks for personal data stored in cloud computing systems.[13]

11 The decision set out measures that Google Inc was required to take to bring the processing of personal data under Google's privacy policy into line with the Italian Data Protection Code of 10 July 2014.

12 However, the requirement for prior consent does not apply to e-mail marketing if the communications concern products and services similar to those already provided to the data subject ('soft-spam' exemption). For this exemption to apply, there must be a contractual relationship between the data controller and the data subject, and the recipient's e-mail address must have been collected in connection with a negotiation for the sale of products and services. In addition, the recipient must always have the right to oppose the processing for marketing activities.

13 By way of example, 'Cloud computing – protect your data without falling from a cloud' guidance of 24 May 2012.

iv Specific regulatory areas

Specific data protection rules apply to personal data processed in the fields of employment, health and video surveillance, as well as for the purposes of the assessment of data subjects' creditworthiness and commercial information.

In particular, the processing of personal and sensitive data in both private and public employment relationships, and the use and storage of health data and of images collected through video surveillance systems, are strictly regulated by the Garante by means of general provisions. These provisions require data controllers involved in these processing operations to implement precise security measures (such as, in relation to video surveillance systems, the granting of different levels of access to the images to each person in charge of the processing and operations) and the fulfilment of special privacy requirements (by way of example, the obligation to give notice of data breaches to the Garante in relation to health data shared among health professionals and data controllers through the 'electronic health file' and the 'electronic health dossier').

In contrast, the processing of personal data disclosing consumers' creditworthiness as recorded in information systems managed by private entities, or concerning entrepreneurs' reliability as offered by companies providing commercial information, are subject to binding criteria and privacy principles set out by the relevant codes of conduct attached to the Privacy Code.

IV INTERNATIONAL DATA TRANSFER

With respect to cross-border transfers of personal data, the Privacy Code contains detailed provisions governing transfers to extra-EU countries that do not have a level of data protection that is adequate by European standards. Specifically, data controllers intending to transfer personal data to other data controllers or data processors established in third countries must obtain prior and express consent from data subjects, which must be preceded by the delivery of a complete privacy information notice as to the methods and purposes of the transfer and subsequent processing. A list of exemptions from this consent is provided by Article 43 of the Privacy Code, including when the transfer is necessary:

a for the performance of obligations resulting from an agreement with the data subject; to take steps at the data subject's request prior to entering into an agreement; or for the conclusion or performance of an agreement made in the interest of the data subject;

b to judicially challenge, exercise or defend a right;

c to safeguard a third party's life or bodily integrity; and

d for responding to a request for information retrievable from public records.

Furthermore, in compliance with Article 26 of Directive 95/46/EC, the Privacy Code also allows a data controller to transfer personal data to extra-EU organisations by adopting the standard contractual clauses that are annexed to European Commission Decisions No. 2001/497/EC, 2004/915/EC and 2010/87/EU or, as an alternative for *infra*-group transfers, binding corporate rules (BCRs). With respect to Italian data protection provisions, agreements duly incorporating the standard contractual clauses, as well as any other necessary information concerning the transfer, must be submitted to the Garante only if the latter so

requests.[14] For BCRs to apply in Italy, a national application form – illustrating the categories of data, purposes and entities involved in the transfer and their respective relationships – must be filed, and the necessary authorisation by the Garante must be obtained.

V COMPANY POLICIES AND PRACTICES

In April 2012, Law No. 35, 'Urgent provisions in matters of simplification and development', repealed the part of Article 34 of the Privacy Code that imposed on data controllers the obligation of drafting and yearly updating their 'security policy document'. This document consisted of an internal policy summarising the actual personal data processing operations carried out by the data controller, the purposes and categories of personal data, and the organisational structure and functions for processing the data and, above all, set out the security measures taken to identify possible risks and damage to the personal data being processed. Notwithstanding the above-mentioned repeal, the mandatory obligations to implement and certify the minimum security measures provided by the Privacy Code and its Annex B, 'Technical specifications in matter of minimum security measures', have remained in place. Consequently, most organisations, as recommended standard practice, continue to adopt internal documents in line with the former security policy document, and to certify all the data processing operations performed and the relevant security measures adopted.

As a matter of best practice, organisations may also consider having in place further internal policies on, for example, data retention policies, whistleblowing procedures and policies for the management of requests for access to personal data from data subjects. However, internal regulations on the appropriate use of professional equipment available to employees (such as e-mail, internet), as well as on whether and how the employer monitors that use, are compulsory.

VI DISCOVERY AND DISCLOSURE

Pursuant to the Privacy Code, the processing of personal data carried out by national judicial offices is exempt from the application of certain privacy regulations when carried out for 'purposes of justice'. This means processing that is directly related to the judicial handling of matters and litigation, and will, therefore, include any disclosure or exhibition order, auditing activities carried out by judicial office holders, as well as in relation to the functioning of courts and the legal and economic status of members of the judiciary. In particular, some provisions of the Privacy Code related to data subjects' rights of access to personal data, the duty to provide information notice and request consent, notification to the Garante and cross-border transfers of personal data do not apply. However, only personal data that are actually necessary, relevant and proportionate to the relevant judicial activity will fall within the above exemptions.

Furthermore, data controllers that collect and process personal data either for carrying out investigations by defence counsel or to establish or defend a legal claim are exempted from

14 Article 157 of the Privacy Code and a general authorisation by the Garante for the transfer of personal data to other countries in compliance with standard contractual clauses of 10 October 2001.

the need to obtain the prior consent from data subjects, as well as the obligation to provide a full information notice in advance,[15] provided that the data are processed exclusively for these purposes and for no longer than is necessary. It should be highlighted that the 'defence exemption' from the need to obtain the data subject's consent[16] also applies to the transfer of relevant personal data to entities and organisations in third countries.

According to the Garante, this exemption applies not just when the relevant civil or criminal proceedings have already been instituted, but also in the phases prior to the beginning of the proceedings[17] (e.g., collection of evidence).

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Italian authority responsible for the enforcement of the Privacy Code is the Garante, an independent authority represented by a collegiate body of four members. The Garante was set up under former Privacy Law No. 675/1996 with the aim of protecting data subjects' fundamental rights and freedoms in connection with privacy and data protection. It is based in Rome.

The duties of the Garante are fully listed in Chapter II of the Privacy Code. They mainly consist of:

a supervising compliance with the provisions and requirements set out in the Code and applicable sector decisions and codes of conduct;

b receiving and handling reports, claims and complaints sent by data subjects or the associations representing them;

c issuing orders against data controllers or processors, also *ex officio*, to take the necessary steps, as well as comply with both mandatory and adequate measures, for the lawful processing of personal data or, in certain cases – such as operations likely to cause serious harm to data subjects – prohibiting unlawful or unfair data processing operations, in whole or in part, or blocking them; and

d issuing the annual general authorisations for the processing of sensitive and judicial data.

Secondly, the Garante is entrusted with the power of carrying out inquiries into, and inspections of, data controllers and data processors, both *ex officio* and following reports and complaints by data subjects or third parties. Pursuant to this power, the Garante can not only request them to provide information and produce documents, but also perform audits and access the premises where personal data are processed and relevant databanks are held.

15 This has been also expressly acknowledged by Italian case law on the matter, such as the following Decisions by the Court of Cassation: No. 3034 of 2011, No. 15076 of 2005, No. 15327 of 2009 and No. 8239 of 2003.

16 Since it is grounded on the fundamental right of defence pursuant to Article 24 of the Constitution.

17 Indeed, pursuant to the 'Code of Practice Applying to the Processing of Personal Data Performed with a View to Defence Investigations' issued by the Garante on 6 November 2008, the protection of the right to a defence must be safeguarded in all cases, including inspection and preliminary investigation activities.

These activities can be carried out by Garante staff as well as by the special privacy team of the Financial Police. The Garante is also involved, on a continuous basis, in the interplay between the parliament and government and other independent administrative authorities giving opinions, guidance and assistance on sector developments and legislation ratifying international agreements.

Finally, the Garante can impose administrative sanctions for the payment of pre-determined amounts, which can vary depending on the existence of aggravating or extenuating circumstances. Furthermore, under the conditions provided by the Privacy Code, the Garante may also forward the proceedings to the Italian public prosecutor's office for the application of criminal sanctions where there is, for instance, harm to a data subject and the consequent benefit to the offender.

ii Recent enforcement cases

As previously mentioned, in the past year about 50 claims were filed with the Garante for de-indexation from the Google search engine of information alleged to be devoid of public interest. The decision of the European Court of Justice in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* of 13 May 2014 recognised the data subject's right to ask Google – as data controller – for the de-indexation of the personal data appearing in the list of results of the search engine. Following Google's refusal, numerous Italian users filed claims with the Garante, which, in about a third of the cases, upheld the requests from the data subjects. The Garante ordered Google to remove the links to web pages reporting personal data that, according to the Garante, were lacking in public interest, often excessive and prejudicial to privacy or, in a few cases, referred to individuals unrelated to the judicial event in issue.

iii Private litigation

Data subjects and private plaintiffs may claim a violation of their privacy rights before the ordinary civil court as an alternative to filing a claim with the Garante.

In this respect, the Privacy Code provides certain rules for litigation relating to personal data processing. Specifically, a data controller is liable for any damage caused by the improper use or disclosure of processed data. Indeed, Italian provisions classify data processing as a 'dangerous' activity, which means that any person or entity that causes damage to third parties as a consequence of personal data processing must indemnify the relevant party for the damages incurred, pursuant to Article 2050 of the Italian Civil Code, unless the perpetrator can prove it has adopted all possible measures to avoid such damage. There is therefore a reversal of the burden of proof with respect to compensation for breach of privacy; the injured party does not need to prove the causal relationship between the data processing and the damage suffered – mere proof of the damage is sufficient – while the perpetrator will be forced to prove, for instance, that it has adhered to all the security measures and privacy requirements necessary to exclude its liability. In this connection, it must be highlighted that the Privacy Code does not refer to the data controller but to the actual person or entity that has caused the damage (it may be, for example, a data processor), although the data controller retains a sort of strict liability for failure to correctly choose and monitor the offender.[18]

18 *Culpa in eligendo* and *culpa in vigilando*.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Privacy Code applies to data controllers established in the Italian territory and processing personal data, meaning that foreign data controllers having an establishment – such as a branch – in Italy are also subject to Italian privacy provisions. Data controllers established in extra-EU countries that process personal data by means of equipment – whether electronic or otherwise – located in Italy will also fall within the scope of the Privacy Code, provided that such equipment is not used only for the purposes of transit through the Italian territory.

Furthermore, the Privacy Code provides that extra-EU data controllers that are subject to its application must appoint a 'representative in the state's territory', namely an Italian representative for the application of national data protection requirements and duties. This is a compulsory requirement and one of the major compliance issues that organisations based in third countries face with regard to the Italian data protection regime.

IX CYBERSECURITY AND DATA BREACHES

Personal data security is strictly regulated by the Privacy Code and its Annex B, 'Technical specifications concerning minimum security measures'. In line with these requirements, the data controller must implement mandatory and appropriate technical, logical and organisational measures to protect personal data from any destruction or loss, unauthorised access or other forms of unlawful processing or processing that is not in compliance with the original purposes of the data collection.

In relation to the minimum mandatory security measures where the processing is performed using electronic means these must include, by way of example:

a the assignment of computerised authentication codes and passwords to any persons in charge of the processing (user IDs), and defined procedures identifying the criteria for assigning and deactivating them;

b precise identification and written provisions on the methods for accessing personal data in the event of prolonged absence or impediment of persons in charge of the processing and consistent with the organisational and security needs of the data controller;

c annual review of the authorisation profiles and scope of the processing assigned to the persons in charge of the processing; and

d organisational and technical instructions for saving data (back-up copies) and for safekeeping and using removable media.

Furthermore, specific security measures are provided by the Garante for tasks entrusted to system administrators.

In relation to cybersecurity, apart from implementing the European Council's Convention on Cybercrime of 23 November 2001 – through the issuance of Law No. 48 of 18 March 2008 – in contrast to other European countries, Italy does not boast organic and

over-arching legislation in the matter of protection of communication systems and networks. However, due to a series of cybercrime incidents[19] and in light of the rise in terrorist threats,[20] cybersecurity has received increased attention in Italy in recent years.

With the approval of Law No. 133 of 7 August 2012, a reinforcement of the power of control by the Parliamentary Committee for the Security of the Republic and by the Department of Information for the National Cybersecurity (DIS) was established, including by means of preventive wiretappings. Subsequently, a Prime Ministerial Decree of 24 January 2013 addressing national protection against cybernetic threats imposed specific obligations on private and public operators that provide public electronic communications services or infrastructure of national significance, such as the notification of breaches of their IT systems to the national Cybersecurity Unit and mandatory access to their databases by the DIS.

Finally, from a data protection standpoint, important innovative measures have been introduced with reference to data breach notification requirements, both as mandatory and as recommended measures, for data controllers operating in certain sectors. In particular, current Italian data protection provisions provide for the notification of data breaches to the Garante and, in specific cases, to the data subjects involved, in relation to:

a electronic communication providers;
b banking and financial entities;
c data controllers processing biometric data;
d distinct health data controllers sharing electronic information and health data originated from individuals' clinic history by means of the electronic health file;
e health professionals operating within a data controller and sharing health information summarising the health history of an individual by means of the electronic health dossier; and
f public administrations.[21]

19 For instance, in 2015 the Italian company, Hacking Team, producing intelligence and investigations software, was hit by unknown hackers that copied and published online more than 400 gigabytes of sensitive information.

20 Particularly in relation to public exhibitions such as EXPO 2015.

21 Reference is made to the following provisions:
- *a* 'Provisions in the matter of flows of banking information and tracking of banking operations' of 12 May 2011;
- *b* 'Guidelines in the matter of implementation of the provisions on data breach notifications – Public consultation' of 26 July 2012;
- *c* 'Implementing measures with regard to the notification of personal data breaches' of 4 April 2013;
- *d* 'General Application Order Concerning Biometrics' of 12 November 2014;
- *e* 'Opinion on the draft of Decree of the President of the Council of Ministers in matter of Electronic Health File' of 22 May 2014;
- *f* 'Guidelines in matter of Electronic Health Dossier' of 4 June 2015; and
- *g* 'Security measures for the sharing of personal data between public administrations' of 2 July 2015.

Generally speaking, the notification obligation is only upon the controller, and the failure to notify data breaches can result in a fine and strict liability in tort.

X OUTLOOK

The Garante has still not expressed any official position in relation to the actual implementation of the newly approved EU General Data Protection Regulation, which is expected to entirely replace the Privacy Code. To date, the Garante has only provided some informal guidelines summarising the new requirements and obligations that will be enforceable from 25 May 2018. However, the new GDPR will introduce certain provisions of relevance to data controllers and organisations, such as a generalised obligation of data breach notification and data protection impact assessment, as well as the appointment of data protection officers, all of which are currently absent from Italian privacy provisions.

In the near future, we expect that the Garante will take a formal position, or at least provide some practical guidance, on how to coordinate the current Privacy Code with the additional EU data protection obligations, and above all on how to introduce the new EU provisions into the existing data processing structures of data controllers and other organisations.

Appendix 1

ABOUT THE AUTHORS

DANIELE VECCHI

Gianni, Origoni, Grippo, Cappelli & Partners

Daniele Vecchi is a partner in the Milan office of Gianni, Origoni, Grippo, Cappelli & Partners. He boasts more than 15 years of experience in the area of data protection, handling cross-border privacy issues involving multiple jurisdictions as well as related to different business sectors such as corporate, contracts, mergers and acquisitions, labour law, intellectual property, banking and securitisation laws.

He advises domestic and multinational corporations in commercial transactions with specific reference to IT and data protection issues, having developed considerable experience in providing assistance in relation to investigations carried out by local and foreign courts or authorities to require information or documents to assess conduct by managers or executives, the drafting and submission of binding corporate rules, the use of whistleblowing hotlines and cloud computing systems.

Daniele has delivered lectures at numerous conferences across Europe.

He speaks Italian and English.

MELISSA MARCHESE

Gianni, Origoni, Grippo, Cappelli & Partners

Melissa Marchese is counsel in the Milan office of Gianni, Origoni, Grippo, Cappelli & Partners. She is an experienced lawyer within the privacy, data protection and IT areas, providing legal advice to Italian and multinational companies in relation to ordinary and extraordinary data protection management, including the information technology and legal security aspects.

She has extensive experience in conducting data protection compliance programmes for top companies operating in all sectors, including banking, telecommunications, pharmaceutical and retail.

Melissa is also a consultant for some international law firms in the fields of information technology and data protection law.

She holds a teaching position at educational entities and in-house companies on data protection and IT-specific aspects.

She speaks Italian and English.

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS
Piazza Belgioioso 2
20121 Milan
Italy
Tel: +39 02 763741
Fax: +39 02 76009628
dvecchi@gop.it
mmarchese@gop.it
www.gop.it