The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 11

ITALY

Stefano Macchi di Cellere[1]

I OVERVIEW

While Italian legislation distinguishes between the concepts of privacy and data protection (and within these, further distinguishes an individual's right to personal identity, name, image and reputation), it can be maintained that both concepts find their roots in the 'open' principle established in 1947 by Article 2 of the Constitution, which states that the Republic affirms and protects inviolable human rights, whether these are manifested individually or in the social context in which the personality is expressed.

However, it was not until 1975 that the Court of Cassation authoritatively recognised the existence of 'an autonomous right to the "privacy" of an individual's own personal affairs', which the Court had previously denied since 1956.

The formalisation of a separate data protection right was instead established for the first time in 1996, with the enactment of Law No. 675, implementing EC Directive 95/46, and aimed at protecting persons (unusually, covering both individuals and legal entities) from the processing of personal data.

Privacy and data protection have different objects of protection, although sometimes their scope may overlap. Privacy rights are exercised in an exclusionary manner, by which the individual upholds the right to be let alone, not to disclose and to keep certain information private. Data protection, on the other hand, is exercised actively, by maintaining control over information.

Today, pending radical reform of the sector with the forthcoming EU Regulation on the Protection of Personal Data, most of the Italian provisions on data privacy and personal data protection have been collected and are contained in the Data Privacy Code (the Code),[2] enacted in 2003 and subsequently amended, most recently by Legislative

1 Stefano Macchi di Cellere is Of Counsel at Jones Day.

2 Legislative Decree No. 196 of 30 June 2003.

Decree No. 69 of 28 May 2012, which sets out the rules generally applicable to the protection of consumers' privacy in relation to electronic communications.

There are three key guiding principles behind the Code: simplification, harmonisation, and effectiveness.

The Code is divided into three parts. The first part sets out the general data protection principles that apply to all organisations. The second part provides additional measures that need to be undertaken by organisations in certain specific areas, such as the telecommunications, health care, human resources, or banking and finance sectors, and may be further expanded by the adoption of codes of practice for each specific industry sector. The third part of the Code relates to applicable sanctions and remedies.

Recently, the Code has been tested by developments deriving from the extensive use of the internet and the pervasive exchange of information fostered by social networks, raising questions on the appropriate response to the use of cookies, direct marketing, cloud computing, the balance between freedom of the press and the 'right to be forgotten', security breach notifications and cybersecurity in general.

These challenges have been addressed with the partial implementation of the EC Directives 2002/58 and 2009/136 on e-privacy, and sometimes clarified by recommendations or decisions of the Italian Data Protection Authority (the Authority), which is the independent public agency established by Legislative Decree No. 675/1996[3] and charged with protecting individuals' fundamental rights and freedoms in connection with the processing of personal data, and ensuring respect for their dignity.

The Authority is a collegiate body comprised of four members, who are elected by the Italian parliament for a seven-year term. The Authority has its seat in Rome and has a staff of about 125 people.

The tasks and duties of the Authority are set out in the Code under Title II and include supervising compliance with the provisions protecting private life; handling claims, reports and complaints lodged by citizens; banning or blocking processing operations that are liable to cause serious harm to individuals; checking into the processing operations performed by the police and the intelligence services; carrying out inspections, also to access databases directly; reporting to the judicial authorities on serious infringements; raising public awareness on privacy legislation; fostering the adoption of codes of practice for various industry sectors; granting general authorisations to enable the processing of certain categories of data; and participating in international activities, with particular regard to the work of joint supervisory authorities under the relevant international conventions.

The Authority submits its annual report to Parliament; directs Parliament and the government's attention to the need for future regulatory measures in the privacy, data protection and cybersecurity sector; and provides mandatory opinions for the administrative action taken by public administrative bodies.

3 Law No. 675 of 31 December 1996, abrogated with the enactment of the Code.

II THE YEAR IN REVIEW

One of the improvements introduced by the Code under the principle of simplification involved changing the previously burdensome notification process. Today the notification process is more transparent and understandable, and mandatory only when organisations process high-risk categories of data, such as genetic and biometric data, data processed for the purpose of analysing or profiling individuals, and credit-related information.[4]

According to the Authority,[5] the Code now aims to strengthen individuals' data protection rights, allowing them to exercise their rights and initiate proceedings more easily. In an effort to simplify the complaint process, the Authority has published a complaints form on its website. Moreover, businesses now have 15 days to comply with any request from the Authority, compared with the previous five-day window. The turnaround for dealing with complaints has increased to 60 days from 30 days, but the Authority affirms that this time window is more suitable for it to work effectively and for the parties to prepare their pleadings appropriately.

In March 2014 the Authority enacted the framework rules with the implementation of a Defaulting Debtors Database in the communications sector, which will allow telecoms industry operators and providers of electronic communications services to assess in real time the creditworthiness of prospective customers. It remains to be seen whether similar instruments will catch on in other industry sectors, or will face opposition from consumer associations.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The Code establishes that the processing of personal data must be respectful of the rights, the fundamental freedoms and the dignity of individuals. For this reason, the Code has implemented a detailed procedure to process personal data. As a general principle, data must be collected in a lawful and fair manner and must be used for purposes that are certain, explicit and lawful. Data must be correct, up to date and complete, and must comply with the purposes of the data processing, without being excessive; this means data must be kept in a form allowing the identification of the data subjects for a period not exceeding the time necessary for the purposes for which data was collected or subsequently processed. Personal data processed in violation of the provisions set forth in the Code cannot be used.

The processing of personal data carried out by natural persons exclusively for personal purposes is subject to the Code only if the data is intended for systematic communication or dissemination, although the provisions concerning liability and security set forth in the Code must nevertheless be applied to such person's computer or device database.

4 Section 37 of the Code.

5 See www.garanteprivacy.it.

Before the start of any processing, the data subject[6] must be informed (either orally or in writing) by means of a an *ad hoc* 'information notice' about, *inter alia*:

a the existence, purposes, and function of the data processing;
b the obligatory or voluntary nature of providing the requested data;
c entities to which data is disclosed;
d details of the data handlers;
e where the data subject's data is currently or will be stored;
f transfer of personal data abroad; and
g the rights of the data subjects set forth in the Code, which include the right:
- to obtain from the data handler confirmation of the existence of personal data;
- to obtain the availability of said personal data in an intelligible form;
- to be informed of the source of the personal data, the processing purposes and methods, the data processing logic, and the identification data of the data handler, and the entities to which personal data may be communicated; and
- to obtain erasure, anonymity, blocking of unlawfully processed data, and updating, rectification or integration of the data, and to object to the data processing on the basis of grounded reasons.

Whenever the personal data is not collected directly from the data subject, but from a third party, the above information notice (including the categories of processed data) shall be provided to the data subject at the time of recording such data or, in the event communication of data is anticipated, no later than the first communication of data.

Processing of personal data can be lawfully carried out only with the data subject's prior and 'express' (verbal or written) consent.[7]

Consent must be in writing when the processing relates to sensitive data.[8]

Consent is deemed to be effective if:

a it is voluntary, specific, and related to a clearly identified processing operation;
b it is documented in writing;[9] and
c the data handler has delivered to the data subject the information notice.

The data subject's consent should be required and given always before the collection of personal data is carried out. However, the data subject's consent is not required if the data processing, *inter alia*:

6 According to the Code, 'data subject' is the natural person to whom the personal data refers.

7 According to Italian scholars, 'express' consent means that the data subject consent can be given in verbal form, provided that it is explicit and manifest. In other words, in no circumstances can such consent simply be inferred from the behaviour of the data subject.

8 Data that allows the disclosure of racial or ethnic origin, religious, philosophical or other beliefs or political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade union character, as well data on the subject's health and sex life.

9 The additional requirement (that consent be documented in writing) means that the data controller must register in writing the consent received verbally.

a is necessary to comply with an obligation imposed by a law, regulations or EU legislation;

b is necessary to perform obligations arising from an agreement to which the data subject is a party, or to comply with specific requests made by the data subject prior to the entering into the agreement;

c concerns data taken from public registers, lists, deeds or documents that are publicly available, without prejudice to the limitations and modalities provided for by laws, regulations and EU legislation with regards to their disclosure and publicity;

d concerns data relating to economic activities that is processed in compliance with the legislation in force as applying to business and industrial secrecy; or

e is necessary for carrying out investigations by defence counsel or, in any event, enforcing or defending a right before a judicial authority, provided that data is processed exclusively for said purposes and for the period strictly necessary for the achievement of those purposes, in accordance with the legislation in force concerning business and industrial secrecy and with the exclusion, in any event, of the dissemination of that data.

ii General obligations for data handlers

The Code sets forth clear distinctions between various categories of data handlers, *inter alia*, the data controller, the data processor and the data processing agents.

'Data controller' is the natural person or the legal entity that determines the purposes and methods of the personal data processing as well as the means applied to the processing and security matters. The data controller is fully responsible in relation to the individuals whose personal data is processed and requires either a legal justification or the relevant individuals' explicit consent for the processing of the personal data.

The 'data processor', on the other hand, is the natural person or the legal entity that processes the personal data on the data controller's behalf.

It is worth noting that, while it is not possible to conduct data processing without a data controller, the appointment of the data processor is not mandatory under the Code. When a data processor is appointed, the duties assigned for the data processing shall be analytically documented in a specific document, such as a letter of appointment.

The Code also provides for the appointment of certain 'data processing agents', who shall be the individuals officially authorised by the data controller, or the data processor, to materially carry out any personal data processing operation. The appointment of at least one data processing agent is always mandatory under the Code. The duties assigned to the data processing agents in respect of the data processing must also be documented and detailed in a specific document or letter of appointment.

Under the Code, if it is deemed necessary for organisational or technical reasons, the data controller may appoint one or more data processors by subdividing the relevant duties.

If appointed, the data processor must be selected with consideration for their experience, skills, reliability, and ability to properly ensure full compliance with the applicable provisions in the matter of personal data processing, including safety measures.

The data processor carries out the data processing in accordance with the data controller's detailed instructions; these instructions could well be embedded into a contract, but not necessarily so.

The data controller, also through periodic assessments, must ensure that the data processor's activities are carried out in compliance with both the provisions set forth in the Code and the data controller's instructions.

The data processor ensures that the data processing is carried out in full compliance with the provisions set forth in the Code, and the Code's Technical Specifications concerning Minimum Security Measures,[10] and verifies periodically and at least on an annual basis, that the conditions related to the storing of the authorisation profiles associated with each data processing agent have been fulfilled.

As a result of efforts to reduce red tape, nowadays the data controller must only file a mandatory notification to the Authority if the data processing relates, *inter alia* to:

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

b data disclosing medical conditions or sexual preferences, where processed for the purposes of assisted reproduction; the provision of health-care services via electronic networks in connection with data banks or the supply of goods; epidemiological surveys; diagnosis of mental, infectious and epidemic diseases; organ and tissue transplants and monitoring of health-care expenditures;

c data disclosing sex life and the psychological sphere, where processed by not-for-profit associations, bodies or organisations – whether recognised or not – of a political, philosophical, religious or trade-union character;

d data processed electronically for the purpose of profiling the data subject or his or her personality, analysing consumers' patterns and choices, or monitoring the use of electronic communications services, except for such processing operations that are technically indispensable to deliver those services to users;

e sensitive data stored in data banks for personnel-selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys or other sample-based surveys; and

f data stored in *ad hoc* data banks managed electronically in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful or fraudulent conduct.

The Authority is entitled to identify additional types of processing that may present a specific risk to the rights and freedoms of the data subjects regarding the nature of the data, the manner of the data processing or the effects of such processing.

iii Technological innovation and privacy law

The Code has implemented the provisions contained in the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC. The use of automated calling systems without human intervention for the purposes of direct marketing, sending advertising

10 Annex B to the Code.

materials or carrying out of market surveys or interactive business communication, shall only be allowed with the data subject's consent (opt in).

The above-mentioned provisions shall also apply to electronic communications via e-mail, facsimile, text messages or any other electronic means.

Without prejudice to the above provisions, where a data controller uses for the the direct marketing of its own products or services, the electronic contact details supplied by a data subject in the context of the sale of a product or service, then the data controller is not required to request the data subject's consent, provided that the services are similar to those that have been the subject of the sale, and the data subject, after being adequately informed, does not object to that use either initially or in connection with subsequent communications.

The data subject shall be informed of the option to object to the data processing at any time, using simple means and without charge, both at the time of data collection and when sending any communications for marketing purposes (opt out).

As for data retention, communications service providers are permitted to retain traffic data for six months only to deal with disputes over billing and subscriber services. They are also required to retain traffic data for longer periods for the purposes of law enforcement activities alone; those retention periods are currently set at 24 months (telephone traffic data) and 12 months (electronic communications traffic data), irrespective of the offence at issue.[11]

With respect to cookies,[12] web beacons and similar devices, the Code provides that storing information, or accessing information that is already stored, in a user's terminal equipment shall only be permitted if the user has given his consent after being informed in accordance with the simplified arrangements determined by the Authority. However, certain cookies (technical cookies) can be used without the user's consent, provided that they are aimed exclusively at carrying out the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the user to provide the service.

For the purpose of expressing the above consent it is possible to implement 'user-friendly' configurations of software or devices.

iv Specific regulatory areas

The processing of data via the internet or in the employment context for purposes of direct marketing by private credit reference agencies or in connection with video surveillance activities, requires special attention.

In such areas, compliance with the provisions set forth in specific relevant codes of conduct is a prerequisite for the processing operations to be lawful.[13]

11 Section 132 of the Code.

12 According to the Authority, 'cookies' mean small text files that are sent to the user's terminal equipment by the visited website; they are stored in the user's terminal equipment to be then re-transmitted to the websites upon the user's subsequent visits to those websites.

13 Section 12(3) of the Code.

The adoption of a code of conduct takes place following action by the Authority and a specific procedure for publishing the final text in the Official Gazette.[14]

For example, on 1 March 2007, the Authority issued certain guidelines applicable to the use of e-mails and the internet in the employment setting.

In short, under these guidelines, employees have the right to be informed in advance and unambiguously about any data processing operations that may concern them in connection with possible checks. Employers are prevented from processing the employees' data by means of hardware and software systems allowing the 'distance monitoring' of employees. Distance monitoring systems include: (1) systematic scanning and recording of e-mail messages or the respective external data apart from what is technically necessary to provide e-mail services; (2) reproduction and systematic storage of the web pages visited by employees; (3) keystroke pattern analysis and recording devices; and (4) hidden monitoring or analysis of laptops assigned to individual employees.

IV INTERNATIONAL DATA TRANSFER

The Code does not contain a definition of 'data transfer'. As a general rule, the Code requires that the data subject must be adequately advised by the information notice of any transfer of personal data abroad, and thus give his or her express consent to the transfer of personal data to any country outside the EU. Such consent must be given in writing if the processing concerns sensitive data.

Besides a number of exemptions set forth by the Code, the transfer of personal data from Italy to countries outside the EU may be considered in any event as lawful, even if the data subject has not expressly consented to it, if the transfer is, *inter alia*:[15]

a necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request before entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject;

b carried out in response to a request for access to administrative records or for information contained in a publicly available register, list, record or document, in compliance with the provisions applying to this subject matter; or

14 Codes of conduct have been adopted and updated so far in various sectors. See, for example, the code of practice applying to the processing of personal data for defence investigations; the code of conduct and professional practice applying to consumer credit, reliability and timeliness of payments; the code of conduct and professional practice applying to the processing of personal data for statistical and scientific purposes; the code of conduct and professional practice regarding the processing of personal data for historical purposes; and the code of practice concerning the processing of personal data in the exercise of journalistic activities.

15 The transfer of processed personal data to a non-EU Member State may also be permitted if it is authorised by the Authority on the basis of specified adequate safeguards for the data subject's rights.

c necessary to carry out investigations by the defendant's lawyer or, in any event, to enforce or defend a right before a judicial authority.

Under the Code's new system, companies will only have to provide a mandatory notification in cases in which the transfer of data abroad could prejudice the data subjects' rights. The rules for authorising transfers to non-EU countries are set forth in Sections 43 and 44 of the Code. Data subjects are entitled to lodge claims in Italy for non-compliance with the provided contractual and corporate safeguards.

The Authority may also issue general authorisations for the cross-border flow of data. Where a data controller complies in full with the provisions of the relevant general authorisation, no *ad hoc* authorisation will be required for the data transfer. The Authority, however, reserves the right to investigate the processing arrangements and, where appropriate, block or ban the data transfer abroad.

V COMPANY POLICIES AND PRACTICES

The Authority recently issued certain guidelines specifically addressing the needs of businesses and reminding them of the fundamental rules of the Code as well as suggesting appropriate practical recommendations in their day-to-day conduct.

In brief, the guidelines provide corporate best practices at a number of levels of the company's activities; emphasise the importance and value of data, and the need to properly allocate responsibility within the organisation; and outline the requirements for transparent and fair data processing. The guidelines also detail useful information on the appropriate handling of CVs received during recruitment processes. Moreover, particular attention is given to the actual risks of data processing, the proper use of state-of-the art technology; surveillance and protection of data assets and the constant monitoring of all IT procedures. Finally, the guidelines advise businesses on compliance with data export rules and appropriate EU standards, and to apply a data-oriented approach to customer care.

VI DISCOVERY AND DISCLOSURE

Unlike certain common law countries, Italian law does not provide for an incisive 'discovery' system, but a disclosure request can be made with a court for it to grant an 'exhibition' order on some identified or identifiable piece of evidence or personal data held by the defendant or third parties.

In fact, the Code shall not apply if the processing of personal data is carried out for the 'purposes of justice' (deemed to be the case whenever the data processing is directly related to the judicial handling of matters and litigations), or if it produces direct effects on the functioning of courts as regards the legal and economic status of members of the judiciary, or if it is related to auditing activities carried out in respect of judicial offices.[16]

16 Section 47 of the Code.

Data identifying matters pending before judicial authorities at all levels and of all instances, can be made accessible only to interested parties, including by means of electronic communications networks, including the internet sites of the judicial authorities.[17]

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Data subjects may exercise their legitimate rights under the Code[18] either by filing a complaint before the ordinary courts or by contacting the Authority if they have been prevented from exercising the right to access, rectify, update or delete their personal data.

The Authority is also entrusted with powers of inspection,[19] which include requesting information and documents from organisations, although these requests are not legally binding. Nevertheless, in cases where an organisation fails to cooperate with the Authority and refuses to allow access to the data systems, the Authority may request a judicial order to enforce the right to carry out its inquiries.

When carrying out formal inspections, the Authority can demand copies of records and databases, which may be passed onto the judicial authorities. The reports of the outcome of any investigation are made public on the Authority's website.

ii Recent enforcement cases

An Italian court recently found that 'the possibility must be ruled out that an internet service provider, which offers active hosting, can carry out effective pre-emptive checks of the entire content uploaded by its users' with respect to the fulfilment of the Italian provisions regulating the processing of personal data. According to the court, such an obligation would impose a 'pre-emptive filter on all the data uploaded on the network', which would alter the network's functionality, and thus only the users who upload content to the internet must be fully responsible for compliance with data privacy laws.[20]

iii Private litigation

The Code provides that anyone who causes damages as a consequence of data processing shall compensate such damage in accordance with Article 2050 of the Italian Civil Code. Article 2050, which concerns 'liability in case of dangerous activities', affords a reversal of the burden of proof for any data controller or data processor in favour of the damaged

17 Section 51 of the Code.

18 Section 7 of the Code.

19 Section 158 of the Code.

20 Milan Court of Appeal, Case 4889/2010, where in 2013 the appellate court overturned the conviction of three Google executives on charges of unlawful data processing in violation of the Code for allowing video depicting the bullying of an autistic teenager to be uploaded to the Google Italia YouTube website (see www.law360.com/privacy/articles/426406/italian-court-s-google-decision-a-significant-precedent).

party. This means that, in such cases, the damaged party must (only) prove the damage and the action of the damaging party, whereas the damaging party must prove that there was no causation and that it adopted 'all the measures appropriate to avoid the damage'. In essence, full compliance with the Code must be proven in order to exclude liability and as such, compliance with the Code's safety measures is an essential and obligatory core function for the prevention of risks related to any data disruption, loss or unauthorised access.

In the case of a data breach caused or allowed by the data processor, the data subject has a claim against the data processor, but could also raise a claim against the data controller if the latter (pursuant to Article 2050) did not, for example: choose a qualified entity to act as data processor (for instance, an entity lacking requisite experience and skill); provide the data processor with appropriate instructions regarding the data processing; or sufficiently supervise the data processing carried out by the data processor.

The allocation of liability between the data controller and the data processor in the case of a breach of the latter is not clear cut. Italian scholars have pointed out that the data controller shall be in any event considered liable, while the data processor should be liable only if the latter has not strictly complied with the Code and the data controller's instructions.

There is no case law that clarifies the type and extent of the data processor's liability, and whether the data controller and the data processor should be deemed jointly or severally liable as a consequence of damages that occurred.

The data controller's liability, in particular, would arise from the fact that all final decisions as regards the data processing generally belong to it, and that it is also vested with a general duty to supervise the data processor's activity (and should ensure in advance that it can properly carry out such supervision on a continuous basis).

In light of the above, the data controller's liability cannot be excluded as a consequence of the fact that the data processor has been entrusted with the management of part or all of the aspects of the processing related to personal data.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Code applies to any processing carried out within the Italian territory.

It will also affect outside organisations that make use of equipment located within Italy, which could include any computer-based systems (or server, switch and router), since it applies to the processing of personal data, including data held abroad, where the processing is performed by any entity 'established' either in Italian territory or in a place that is under Italian sovereignty.[21]

For the purpose of determining when an entity shall be deemed to be 'established' in Italy, reference must be made to the 'effective and real exercise of activity through stable arrangements', it being understood that 'the legal form of such an establishment,

21 Section 5 of the Code.

whether simply by a branch or a subsidiary with a legal personality, is not the determining factor in this respect'.[22]

If an organisation outside the EU processes data on Italian territory, it must appoint a representative in Italy for the application of Italian rules (this will be necessary, *inter alia*, for notifying the Authority, if a notification is due and providing the data subjects with information notices).

IX CYBERSECURITY AND DATA BREACHES

Personal data must be kept and controlled in consideration of technological innovations, the nature of the data and the specific features of the processing, and in a way that minimises through suitable preventive security measures, the risk of: destruction or loss, whether by accident or not; unauthorised access to the data; or processing operations that are either unlawful or inconsistent with the purposes for which the data has been collected.

Processing by 'electronic means' is allowed only if the data controller, in accordance with the procedures set out in the technical specifications set forth in Annex B to the Code, has implemented certain minimum security measures.[23]

The data controller shall carry out certain security measures on a periodic basis that include, *inter alia*, the following:

a verifying that the prerequisites for retaining the relevant authorisation profiles still apply;

b regularly updating the scope of the processing operations that are entrusted to the data processing agents;

c regularly updating computer programs aimed at preventing vulnerability and removing electronic flaws; and

d regularly updating its antivirus systems.

The data controller shall also institute further measures to prevent unauthorised access to personal data by the system administrators by:

22 Whereas 19 of the European Directive No. 95/46/EC.

23 Computerised authentication; Adoption of authentication credentials management procedures; Use of an authorisation system; Regular update of the scope of the allowed Processing to the Data Processing Agents or of the maintenance of the electronic instruments; Protection of the electronic instruments and data against unlawful data processing operations, unauthorised access and specific software systems; Implementation of procedures for safekeeping, backup copies, and restoring data and system availability; Implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

a selecting experienced, capable and reliable individuals as system administrators, who appropriately guarantee full compliance with the data protection law in force;

b appointing the system administrator by means of an individual letter of appointment, which includes a detailed list of the duties to be performed; and

c recording the personal details of the system administrator in an internal document to be made available to the Authority in case of inspection.

The data controller's employees shall furthermore be provided with the details of the system administrator in cases where the latter processes, even indirectly, their personal data.

Following ratification of the Council of Europe's Cybercrime Convention, police authorities may under specific circumstances, order IT and internet service providers and operators to retain and protect internet traffic data – except for content data – for no longer than 90 days in order to carry out pretrial investigations or in connection with the detection and suppression of specific offences. The order issued by police authorities must be notified to and validated by the public prosecutor.

The National Anti-Crime Computer Centre for Critical Infrastructure Protection (CNAIPIC) is the public body responsible for the cybersecurity of infrastructure operating in particular sectors, such as health care, transport, telecommunications and energy. The CNAIPIC is a branch of the Italian police and its purpose is to intervene to prevent and fight cyberattacks, cybercrime and industrial espionage.

The protection of strategic infrastructure is carried out by the Italian police by creating an 'external wall' in an existing protection infrastructure, meaning an electronic protection system that monitors possible access anomalies and communicates them to the CNAIPIC.

In the case of a personal data breach, the provider of publicly available electronic communications services shall notify the breach to the Authority without undue delay. When the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual, the provider shall also notify the contracting party or the individual of the said breach without delay.

X OUTLOOK

The Authority has been active since 1997 and is recognised for playing a role in the social, economic, political and cultural life of the country's digital revolution. Special importance should be attached to popularly accepted provisions regarding health care, employment, banking, insurance, journalism, telecommunications, video surveillance, marketing and involving public administrative agencies.

Since its early years, the Authority has encouraged self-regulation and the adoption of a code of practice for journalists (1998); for the processing of personal data for historical research purposes (2001); for statistical purposes (2002); and for the purpose of credit checks (2004), while the use of genetic data for health care and research purposes was regulated via a general authorisation (2007).

The evolution of EU regulation on the protection of personal data is unlikely to diminish, but will rather enhance, the role and importance of the Authority as a fierce watchdog in safeguarding the principles of appropriate data protection and cybersecurity, and the defence of citizens' privacy in an increasingly digitalised world.

Appendix 1

ABOUT THE AUTHORS

STEFANO MACCHI DI CELLERE

Jones Day

Stefano Macchi di Cellere is head of the Italian TMT as well as the antitrust and competition law departments at Jones Day since 2001. A dual-qualified lawyer; both solicitor and *avvocato*, he practises international competition law, acting in cross-border merger and cartel cases before the EU antitrust authorities and assisting global enterprises on abuse of dominance claims and investigations. He advises on private damages, unfair competition and intellectual property litigation; he has also gained extensive experience in communications law, assisting corporations on radio and television broadcasting, information technology and internet communications, including complex privacy, data protection and cybersecurity issues.

Mr Macchi di Cellere is a regular author and speaker on antitrust, communications and technology law topics and a contributor to the World Bank's annual *Doing Business* reports. He is a member of the Italian Bar, the Law Society of England and Wales, the International Bar Association (antitrust and trade and communications law committees), the American Bar Association (section of antitrust law), the Inter-Pacific Bar Association (former council member and chair of the aerospace committee), the Alumni Association of the Academy of American and International Law (former deputy secretary general). Mr Macchi di Cellere co-founded the Jones Day Milan office in 2001 and he is the firm's *pro bono* coordinator for Italy.

JONES DAY
Via Turati 16–18
20121 Milan
Italy
Tel: +39 02 7645 4001
Fax: +39 02 7645 4400
smacchi@jonesday.com
www.jonesday.com