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 v
Alan Charles Raul

Chapter 1 EUROPEAN UNION OVERVIEW.....1
William Long, Géraldine Scali and Alan Charles Raul

Chapter 2 APEC OVERVIEW.....19
Catherine Valerio Barrad and Alan Charles Raul

Chapter 3 BELGIUM 31
Steven De Schrijver and Thomas Daenens

Chapter 4 BRAZIL.....43
André Zonaro Giacchetta and Ciro Torres Freitas

Chapter 5 CANADA.....54
Shaun Brown

Chapter 6 FRANCE.....70
Merav Griguer

Chapter 7 GERMANY.....83
Jens-Marwin Koch

Chapter 8 GREECE.....98
George Ballas and Theodore Konstantakopoulos

Chapter 9 HONG KONG.....113
Yuet Ming Tham and Joanne Mok

Chapter 10 HUNGARY.....127
Tamás Gödölle and Péter Koczor

Chapter 11 ITALY....142
Stefano Macchi di Cellere

Chapter 12 JAPAN....156
Takahiro Nonaka

Chapter 13 KOREA....170
Jin Hwan Kim, Brian Tae-Hyun Chung, Jennifer S Keh and In Hwan Lee

Chapter 14 MEXICO....180
César G Cruz-Ayala and Diego Acosta-Chin

Chapter 15 RUSSIA....194
Vyacheslav Khayryuzov

Chapter 16 SINGAPORE....204
Yuet Ming Tham, Ijin Tan and Teena Zhang

Chapter 17 SPAIN....219
Cecilia Álvarez Rigaudias and Reyes Bermejo Bosch

Chapter 18 SWEDEN....230
Jim Runsten and Charlotta Emtefall

Chapter 19 TURKEY....241
Gönenç Gürkaynak and İlay Yılmaz

Chapter 20 UNITED KINGDOM....253
William Long and Géraldine Scali

Chapter 21 UNITED STATES....268
Alan Charles Raul, Tasha D Manoranjan and Vivek Mohan

Appendix 1 ABOUT THE AUTHORS....295

Appendix 2 CONTRIBUTING LAW FIRMS' CONTACT DETAILS....309

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 17

SPAIN

Cecilia Álvarez Rigaudias and Reyes Bermejo Bosch[1]

I OVERVIEW

Data protection and privacy are distinct rights under Spanish law but both are deemed fundamental rights derived from the respect for the dignity of human beings. They are primarily based on the free choice of individuals to decide whether to share with others (public authorities included) information that relates to them (personal data) or that belongs to their private and family life, home and communications (privacy). Both fundamental rights are recognised in the Lisbon Treaty (the Charter of Fundamental Rights of the European Union) and the Spanish Constitution of 1978. Data protection rules address, among other things, security principles and concrete measures that are helpful to address some cybersecurity issues, in particular, because specific cybersecurity legislation (which not only covers personal data and private information but rather any information) is new and not sufficiently developed yet.

Spain has an omnibus data protection framework law along the lines of the EU approach and applies it both to the private and the public sectors. However, some personal data or some processing activities may require specific protection (not always supplementary to the general protection) such as certain financial, e-communications or health-related data or processing activities. There are several codes of conduct for data protection that have been approved in different sectors but, in general terms, they merely adjust the general obligations to the specific needs of the relevant sector or organisation.

The rights to data protection and privacy are not absolute and, where applicable, must be balanced with other fundamental rights or freedoms (e.g., freedom of information or expression) as well as other legitimate interests (e.g., intellectual property rights, public security and prosecution of crimes).

1 Cecilia Álvarez Rigaudias and Reyes Bermejo Bosch are lawyers at Uría Menéndez Abogados, SLP.

In the case of data protection, this balance must be assessed by the organisation and could be challenged before the Spanish Data Protection Authority (DPA), which is in charge of supervising the application of the regulations on data protection (see Section III.i, *infra*). Privacy infringements must be claimed before the (civil or criminal) courts.

The DPA was created in 1993 and has been particularly active in its role of educating organisations and the general public on the value of data protection and of imposing significant sanctions. These sanctions are published on its website, which is used by the media, among others, as an important source of data protection information.

II THE YEAR IN REVIEW

Spanish law in this area underwent a number of developments last year, which can be summarised as follows.

The new General Telecommunications Law 9/2014 (GTL) was approved, repealing the former telecommunication regulations and amending, among others, the E-Commerce Law 34/2002 (LISS), the e-Signature Law 59/2003 and the Gambling Law 13/2011.

Among the most relevant changes, a specific cybersecurity regime has been incorporated (through the GTL) into the LISS (see Section IX). In addition, the GTL corrected some technical defects of the cookies regime of the LISS so that the lack of consent, where required, could be sanctioned. The changes did not affect the core of the security breach notification regime introduced in 2012 in line with Directive 2009/136/EC: namely, that the providers of public communications networks or publicly available electronic communications services must notify any security breaches, when personal data are involved, to both the data subjects and the DPA. The DPA approved in March 2014 an online system for the notification of security breaches. The requirements of the notification itself are those established in EU Regulation 611/2013.

Since the notification of data breaches is not mandatory in general (except for the above-mentioned services providers), most of them remain unknown to the DPA and the public. One of those which was made public was the security breach suffered by BuyVip (which belongs to the Amazon group) in 2011, which involved the names, dates of birth, e-mail addresses, phone numbers and shipping addresses of its customers. Although BuyVip was not subject to a notification duty in Spain, it decided to inform all its users of the security breach and the notice went viral on the internet. The DPA then initiated an *ex officio* investigation, but there is no public information on the specific sanction imposed on BuyVip.

Directive 2011/83/EU on Consumer Rights has also been implemented in Spain; the most significant modifications introduced by the new regime affect e-commerce activities, where the mandatory requirements have become more stringent.

Regarding significant issues that have received broad media coverage in Spain, in addition to the *Google Spain* case before the ECJ (regarding the 'right to be forgotten'), the DPA has imposed the first sanctions for the use of cookies and Google has also been sanctioned in connection with its global privacy policy (see Section VII.ii, *infra*).

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The legal framework for the protection of personal data in Spain is regulated by: the Lisbon Treaty; Article 18(4) of the Spanish Constitution; and Law 15/1999 of 13 December on the Protection of Personal Data (the DP Law), as developed by Royal Decree 1720/2007 of 21 December (RD 1720/2007) (together, 'the DP Regulations'). Sector-specific regulations may also contain data protection provisions such as the LISS, the GTL, anti-money laundering legislation and the regulations on biomedical research.

Privacy rights are mainly regulated by Law 1/1982 of 5 May on civil protection of the rights to honour, personal and family privacy, and an individual's own image and by the Criminal Code approved by Law 10/1995 of 23 November.

Personal data and private data are not synonymous. Personal data is any kind of information (alphanumeric, graphic, photographic, acoustic, etc.) concerning an identified or identifiable natural person, irrespective of whether or not this information is private. However, data regarding ideology, trade union membership, religion, beliefs, racial origin, health or sex life as well as criminal and administrative offences is deemed more sensitive and requires specific protection.

Protecting personal data is achieved by allocating specific duties to both the 'controllers' (i.e., those who decide on the data processing purposes and means) and the 'processors' (i.e., those who process the data only on behalf of a controller to render a service).

The DPA is the entity in charge of supervising compliance with the data protection duties imposed by the DP Regulations (fair information, legitimate ground, security, notification, proportionality and quality, etc.).[2] The DPA has carried out *ex officio* audits of specific sectors (including online recruitment procedures, TV games and contests, hotels, department stores, distance banking, hospitals, schools, webcams and mobile apps). However, the DPA's activity in terms of individual compliance investigations has significantly increased over the past 10 years as well as the number of fines imposed. Indeed, failure to comply with the DP Regulations may result in the imposition of administrative fines ranging from €900 to €600,000 per infringement, depending on the gravity of the offence (and regardless of whether civil or criminal offences are also committed, if applicable). Neither harm nor injury is required (i.e., the infringement itself suffices for the offender to be deemed liable) but the lack of any harm or injury is considered an attenuating circumstance to grade the amount of the administrative fine. However, harm or injury will be required to claim damages arising from breaches of data protection rights before civil and criminal courts.

2 The data protection right is enforced by the DPA at a national level with limited exceptions. For example, Catalonia and the Basque Country are regions that have regional data protection authorities with competences limited to the processing of personal data by the regional public sector. Galicia has developed a regional decree but has not yet created a data protection authority.

ii General obligations for data handlers

Data controllers (irrespective of whether or not they handle the personal data) and data processors must comply with specific obligations set out in the DP Regulations.

Obligations of data controllers

a Any personal data file should be registered (as well as any modifications to it) with the DPA;

b data subjects from whom personal data is requested must be provided beforehand with information about the processing of their personal data;

c as a general rule, controllers must obtain the prior consent of the data subject to any processing activity – including (intra-group) transfers. Furthermore, explicit consent is required for certain processing activities involving 'sensitive' data (such as health-related data) or consisting of direct marketing;

d there are few exemptions to the need to obtain the data subject's prior consent, such as when the processing of the personal data is unavoidable to perform a contract that the data subject has executed with the data controller; or when the data controller engages a third-party services provider that in order to perform its services, needs to access or otherwise process personal data held by the data controller, in which case a written agreement with a minimum legally prescribed content (a processing agreement) must be executed;

e when the recipient is not located in the EU/EEA (or in a country whose regulations do not afford an equivalent or adequate level of protection identified by the EU Commission or the DPA), the prior authorisation of the DPA must be obtained, unless a legal exemption applies;

f controllers should adopt specific security measures; and

g data subjects have a right to access all data relating to them and to rectify and cancel data the processing of which does not comply with the data protection principles, in particular, when data is incomplete or inaccurate or excessive in relation to the legitimate purpose of its processing. Data subjects are also entitled to object to certain processing activities that do not require their consent or are made for direct marketing purposes.

Obligations of data processors

Data processors must execute the above-mentioned processing agreement with the relevant data controller; implement the above-mentioned security measures; process data only to provide the agreed services to the controller and in accordance with its instructions; keep the data confidential and not disclose it to third parties (subcontracting is not prohibited but is subject to specific restrictions), even for storage; and upon the termination of the services, return or destroy the data, at the controller's discretion.

iii Technological innovation and privacy law

Technology has created specific issues in the privacy field, including:

a Automated profiling and online behavioural advertising and tracking: explicit prior consent is required for any profiling (whether automated or not) and for

installing tracking cookies or similar devices in terminal equipment that are strictly necessary for ensuring a technical communication.

b Viral marketing: the DPA has considered many 'send-to-a-friend' systems illegal.

c Electronic marketing also requires express prior consent (with some exceptions).

d Big data projects and anonymous data: the DPA has narrowed its definition of anonymous data although it has not yet adopted an official position regarding the use of 'anonymous' data in big data projects.

e Cloud computing: in 2012 the Spanish DPA issued two cloud computing guidelines addressed to clients and service providers respectively.

f Employee monitoring: the Spanish Workers' Statute establishes that an employer is entitled to verify the fulfilment of an employee's work obligations. However, this right must be balanced with the privacy and data protection rights and right to secrecy of communications. This balance must be assessed in any investigation or audit that entails accessing devices used by the employees, either owned by the employer or by the employee under 'bring your own device' or similar policies.

g Facial recognition technology: the DPA has considered that facial recognition technologies may only be used if there are no other less intrusive means for collecting the same personal data and achieving the same (legitimate) purposes.

iv Specific regulatory areas

The DP Regulations apply to any personal data but they provide for a reinforced protection regarding data related to children (the verifiable consent of parents is required) and health-related data (express consent and specific security measures are required as a general rule). Specific rules also apply to the information processed by solvency and credit files and to the processing of data for video surveillance or access control purposes.

In addition, certain information is also protected by sector-specific regulations. This is the case for, *inter alia*, financial information that is subject to banking secrecy rules; the use (for purposes other than billing) and retention of traffic and location data; the sources of information and the intra-group disclosures to comply with anti-money-laundering and combating-the-financing-of-terrorism regulations and the restrictions to the transparency principle in relation to the data subjects; the use of genetic data or information contained in biological samples; information used for direct marketing purposes; the outsourcing of core financial services to third parties; and the use of video-surveillance cameras in certain sectors.

IV INTERNATIONAL DATA TRANSFER

Data transfers from Spain to (or access by) recipients located outside the EEA require the prior authorisation of the DPA, unless the recipient ensures an 'adequate' level of protection as recognised by the European Commission (or the DPA) or the transfer can be based on a statutory exemption.[3]

3 The DPA's prior authorisation is not required in the cases set out in Article 26 of Directive 95/46/EC.

Irrespective of the authorisation requirement, all international data transfers outside the EEA must be notified to the DPA for registration.

The authorisation of the DPA will be granted if the data exporter (controller or processor) provides adequate safeguards, such as by executing the European Commission's standard contractual clauses for data transfers or other clauses such as the standard contractual processor-to-processor clauses, approved by the DPA in 2012 in order to enable the subcontracting of non-EEA subcontractors by service providers established in Spain. In Spain, data transfer agreements must be previously authorised by the DPA, even if they are based on any of these clauses.

Spanish law also allows the DPA to grant authorisation based on binding corporate rules (BCRs) adopted within a group. Spain is a Mutual Recognition Procedure (MRP) country and, thus, the BCRs approved by the leading data protection authority of any MRP country must be recognised in Spain. The granting of the authorisation entails *per se* that the BCRs become legal obligations and, as such, may be enforced by the data subjects and the DPA. In any event, 'authorised BCRs' do not replace any obligation under the DP Regulations. To date the DPA has authorised 11 BCRs related to the financial, pharma and technology sectors.

V COMPANY POLICIES AND PRACTICES

Privacy and security policies

Organisations that process personal data are not required to have 'general' privacy policies but they are useful to comply with the information duties regarding the processing activities (see Section III.ii, *supra*). In addition, employees must be informed of the applicable security rules and organisations must create and keep up to date a security document and a record of incidents (see Section IX, *infra*).

Privacy officers

A chief privacy officer is not mandatory, but in practice this role is indispensable so that the controller or the processor can comply with the DP Regulations, in particular when the organisation is complex or the data processed is sensitive or private. In addition, one of the factors that may mitigate the liability in terms of breach is to have accountable data protection programmes, which necessarily entails the existence of the chief privacy officer. In any event, organisations must appoint a person responsible for the security measures for specific processing activities (in particular but without limitation, the processing of data related to the rendering of financial services or of sensitive data).

Work councils

Any employee representative in the organisation is entitled to issue a non-binding report before the implementation of new methods of control of the work. Although it is unclear what qualifies as a 'method of control' of the work, it is advisable to inform the works council of the implementation of new methods (e.g., whistle-blowing systems) and offer their members the possibility of issuing the above-mentioned non-binding report before its implementation.

VI DISCOVERY AND DISCLOSURE

Non-EU laws are not considered a legal basis for data processing, in particular, regarding transfers to foreign authorities and especially if they are public authorities.

e-Discovery and any enforcement requests based on these laws require a complex case-by-case analysis, from a data protection, labour and criminal law point of view (and other sector-specific regulations, such as bank secrecy rules).

From a data protection point of view, the main issues to be assessed include the need to obtain the DPA's authorisation, the lack of proportionality of the requests and whether information or consent is required. From a labour and criminal point of view, privacy (rather than data protection) must be guaranteed.

In this regard, the use of the international principles drawn up by the Sedona Conference has proven useful, in particular because Spain has filed reservations under Article 23 of the 1970 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters that essentially prohibit all pretrial document discovery.[4]

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA is the independent authority responsible for the enforcement of the DP Regulations[5] and the data protection provisions of the LISS and the GTL.

Among other powers and duties, the DPA has powers including the issuing of (non-binding) legal reports, recommendations, instructions and contributions to draft rules; powers of investigation; and powers of intervention, such as ordering the blocking, erasing or destruction of unlawful personal data, imposing a temporary or definitive ban on processing, warning or admonishing the controller or processor, or imposing administrative fines (fines are only imposed on private sector entities).

Disciplinary procedures start *ex officio*, but generally stem from a complaint submitted by any person (e.g., the data subject, consumer associations, competitors or former employees). These procedures must be settled within six months and no other party may intervene in the proceedings. If a data subject considers him or herself to have been harmed by the conduct, he or she may claim damages (if duly evidenced) before the civil courts. The alleged infringer is entitled to lodge an appeal against the resolution either before the DPA itself (within one month) and, if not successful, before the administrative courts (within two months); or directly before the administrative courts (within two months).

The DPA will decide the final administrative fine, taking into account the mitigating and aggravating factors described in the law. In very limited cases, the DPA may decide not to start any penalty proceedings but to warn the liable entity, setting

4 Article 23 specifically states that contracting states may declare, 'at the time of signature, ratification or accession,' that they will not execute letters of request issued to obtain pretrial discovery of documents.

5 See footnote 2.

a term within which the entity must adopt corrective measures and evidence their implementation.

The DPA is very active: in addition to *ex officio* inspections of specific sectors (always announced in advance), in 2013 (the most recent official statistics published by the DPA): almost 8,000 (1.3 per cent less than in 2012) investigations were carried out; over 800 fines (4.75 per cent less than in 2012) were imposed; and the fines amounted to approximately €22.34 million (6.1 per cent more than in 2012). Most of the sanctions imposed on the private sector were related to lack of consent and breach of the quality principle. The statistics show that the telecoms, energy and water supply, and commercialisation and financial sectors are the top three in terms of sanctions. The telecoms sector accrues by far the greatest number of fines. We provide some examples (with approximate figures) below:

a telecom operators: €40,000 (lack of consent, 2013), €50,000 (breach of the quality principle, 2013), €100,000 (incorrect disclosure of a debt to a creditworthiness file, 2012), €50,000 (lack of consent, 2012) €50,000 (unauthorised processing of the data of minors, 2012), €100,000 (breach of security measures, 2011) and €300,500 (unlawful assignment of credit rights, 2009);

b banks: €50,000 (incorrect disclosure of a debt to a creditworthiness file, 2012) and €80,000 (breach of secrecy, 2011);

c media operator: €50,000 (unsolicited e-spam, 2010); and

d department store: €60,000 (video surveillance, 2011).

ii Recent enforcement cases

The most significant issues that have received media attention in Spain in 2013–2014 are the following:

The DPA imposed the first-ever sanctions related to the use of cookies on two jewellery companies (€3,000 and €500 respectively) for not providing clear and comprehensive information about the cookies they used and, therefore, not obtaining the proper consent. Google was also sanctioned with a €25,000 fine for installing analytical and advertising cookies 'by default' in Blogger (the free blog service provided by Google). Although the editors of the blogs could administer the cookies to be installed in their blogs, their configuration failed to work properly. These cookies collected information on the editors and on the users of the blogs.

Google's privacy policy: In March 2012, Google replaced its existing privacy policies with a single all-encompassing policy covering the collection of personal data across all its services. The DPA imposed a €900,000 fine on Google for the following infringements:

a information duties and lack of valid consent: Google would collect the users' personal data without providing them clear and specific information on the categories of data collected and the purposes of the processing;

b data quality: Google fail to cancel the users' personal data when no longer needed according to the purposes of the processing for which they were collected; and

c user's data protection rights: Google's procedures would prevent users from exercising their right to access, rectification, cancellation and objection in an easy and clear way.

iii Private litigation

Data subjects may claim damages arising from the breach of their data protection rights before civil courts. Claims for civil damages usually involve pecuniary or moral damages, or both, linked to the violation of honour (such as the improper disclosure of private information) and privacy rights (such as the dissemination of private images). In general, indemnities granted to date have been exceptional and have not exceeded €3,000 (with the exception of a quite recent ruling that awarded €20,000).

There are no specific class actions for data protection matters. However, consumer class actions have been used by consumer organisations to request that specific data protection clauses be overturned on the basis that they breach the DP Regulations.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The application of the DP Regulations for foreign organisations is triggered by either the existence of a data processor or processing equipment in Spain or, according to the *Google Spain/Costeja* ECJ case (Case C-131/12), the existence of an establishment in Spain the activity of which is inextricably linked to that of the foreign organisation.

In addition, online tracking and marketing activities addressed to the Spanish market may trigger the application of the data protection provisions of the LISS as well as the consumer regulations (only if consumers resident in Spain are involved), irrespective of where the organisation is established.

The major compliance issues that foreign organisations face relate to transfers outside the EEA, the information and consent rules and the security measures.

IX CYBERSECURITY AND DATA BREACHES

The Spanish Criminal Code was amended in 2010 to implement the Convention on Cybercrime and the Council Framework Decision 2005/222/JHA on attacks against information systems. Specifically, this entailed the introduction of two new criminal offences: (1) the discovery and disclosure of secrets, namely, the unauthorised access to data or applications contained in an IT system, by any means and infringing implemented security measures; and (2) the intentional deletion, damage, deterioration, alteration or suppression of data, application and electronic documents of third parties and to render them unavailable, as well as the intentional serious hindering or interruption of the functioning of an information system. Other criminal offences that could be related to cybercrime were also modified (computer fraud, sexual offences, technological theft and offences against intellectual and industrial property). Finally, for the first time, legal entities can be held criminally liable for certain crimes, which include most of the above-mentioned offences.

Without prejudice to the above, there are no cybersecurity laws and requirements applicable to organisations 'generally' but rather a certain number of rules that address specific cybersecurity issues:

A recent modification of the LISS establishes specific obligations on cybersecurity incidents, which are applicable to information society services providers, domain names registries and registrars. These obligations are twofold: to collaborate with the relevant

computer emergency response teams for the response to cybersecurity incidents affecting the internet network (to this end, the relevant information – including IP addresses – must be disclosed to them, but 'respecting the secrecy of communications); and to follow specific recommendations on the management of cybersecurity incidents, which will be developed through codes of conduct (these have not yet been developed).

Operators of critical infrastructure [6] (entities responsible for investments in, or day-to-day operation of, a particular installation, network, system, physical or IT equipment designated as such by the National Centre for Critical Infrastructure Protection (CNPIC) under Law 8/2011) are subject to specific obligations such as providing technological assistance to the Ministry of Home Affairs, facilitating the inspections performed by the competent authorities and creating the specific protection plan and the operator's security plan, etc.

Furthermore, these operators must appoint a security liaison officer and a security officer. The security liaison officer requires a legal authorisation (issued by the Ministry of Home Affairs) and his or her appointment must be communicated to this ministry. The security officer does not need a legal authorisation but his or her appointment must nevertheless be communicated to the relevant government delegation or the competent regional authority.

Royal Decree 3/2010 establishes the security measures to be implemented by Spanish public authorities to ensure the security of the systems, data, communications and e-services addressed to the public and they could apply by analogy. These security measures are classified into three groups: (1) organisational framework, which is composed of the set of measures relating to the overall organisation of security; (2) operational framework, consisting of the measures to be taken to protect the operation of the system as a comprehensive set of components organised for one purpose; and (3) protection measures, focused on the protection of specific assets, according to their nature and the required quality according to the level of security of the affected areas. Spanish law does not directly address restrictions to cybersecurity measures.

Although cybersecurity requirements do not specifically refer to personal data (but rather to any kind of information), the security measures of RD 1720/2007 apply when personal data is involved, which distinguishes between three levels of security measures depending on the nature of the data.

Among other security measures, an incidents register must be in place. In addition, public and private organisations that process specific personal data must appoint a security officer to monitor compliance with the personal data security requirements. No specific legal rules apply to such appointment. The skills of this security officer and the resources and powers allocated to him or her within the organisation must be appropriate to ensure that the organisation complies with the legally prescribed security requirements.

6 The following infrastructures have been considered 'critical' by Law 8/2011 (which transposes Directive 2008/114/EC into Spanish law): administration, water, food, energy, space, chemical industry, nuclear industry, research facilities, health, financial and tax system, ICT and transport.

In addition to the above-mentioned laws, certain authorities with specific cybersecurity responsibilities have issued guidance, such as the National Cybersecurity Strategy issued by the Presidency in 2013; the strategy series on cybersecurity issued by the Ministry of Defence; and the Supervisory Control and Data Acquisition Guidelines issued by the CNPIC in collaboration with the National Cryptological Centre (CCN) in 2010.

The agencies and bodies with competences on cybersecurity are numerous: the CCN, which is part of the National Intelligence Centre, the CCN Computer Emergency Response Team, the CNPIC, the Cybersecurity Coordinator's Office (which is part of the CNPIC) and the National Institute of Communication Technologies.

X OUTLOOK

Data protection is constantly evolving. In the past it has been neglected by both private and public organisations or deemed an unreasonable barrier for the development of the economy. However, this trend has definitively changed in the past five years.

This change is mostly due to the sanctions imposed by the DPA, the role of data in the development of the digital economy (the 'new oil'), the active voice of users in the digital environment (developing new social interactions and not only acting as consumers) and the fact that the EU Commission and the EU Parliament have definitively embraced a strong 'privacy mission'. The recent decisions of the ECJ declaring the Data Retention Directive 2006/24/EC invalid and the application of the Spanish data protection law to Google Inc through a wide and economic construction of the concept of 'establishment' have also sent out a clear message on the importance of data protection rules in Europe.

It seems that the adoption in 2015 of the EU's proposed new General Data Protection Regulation is more feasible. In Spain, since the most recent draft of the new EU Regulation is actually fairly similar to the current DP Regulations, as construed by the ECJ and the Article 29 Working Party, the main impact of the EU Regulation would probably result from the new fines that would follow a criteria similar to those used in antitrust regulations (annual worldwide turnover percentage), the general security breach notification and the need to have a data protection officer and privacy and security professionals involved in the business of organisations.

Appendix 1

ABOUT THE AUTHORS

CECILIA ÁLVAREZ RIGAUDIAS

Uría Menéndez Abogados, SLP

Cecilia Álvarez Rigaudias heads the data protection practice of Spanish law firm Uría Menéndez and leads the LATAM data protection group. Cecilia focuses her practice on advising national and multinational companies on matters relating to data protection, information technology and e-commerce.

She is vice-president of the Spanish Association of Privacy Professionals and represents this association in the Confederation of European Data Protection Organisations. She is also a member of the Steering Committees of the International Privacy Law Forum and the Sedona Conference (W-6) as well as an arbitrator at the European Association of Arbitration) in the technology section.

She formed part of the Volunteer Group of Experts Privacy Working Group of the OECD, having contributed to the revision of the OECD guidelines governing the protection of privacy and transborder data flows of personal data.

She regularly speaks in national and international fora regarding personal data protection and technology, in addition to having written numerous articles on data protection related matters. She is ranked in prestigious legal directories such as *Chambers Europe*, *Best lawyers in Spain* and *Who's Who Legal: Internet, e-Commerce and Data Protection*.

REYES BERMEJO BOSCH

Uría Menéndez Abogados, SLP

Reyes Bermejo is a lawyer in the Madrid office of Uría Menéndez. She commenced her legal practice in 2006 and joined the firm in 2011.

She focuses her practice on data protection, e-commerce and IT. Reyes provides national and multinational companies with day-to-day advice on the abovementioned matters, such as privacy advice, consumer protection and e-commerce issues, dealings

with public authorities, including the drafting and negotiation of IT agreements, etc. In particular, she has extensive experience in the data protection design of commercial and M&A transactions, in the preparation of notices, clauses, contracts, protocols and training programmes, in authorisation proceedings for international transfers and administrative and judicial proceedings as well as in the preparation of website terms and conditions and cookie policies and in advising on direct marketing activities by electronic means.

Reyes is also a professor of data protection and e-commerce law at different master's programmes and seminars (Universidad de Valencia, Fundación de Estudios Bursátiles y Financieros and CEU Cardenal Herrera de Valencia).

She collaborates with the firm's data protection newsletter and legal magazine (*Actualidad Jurídica Uría Menéndez*) on aspects and updates relating to data protection regulatory issues and case law.

URÍA MENÉNDEZ ABOGADOS, SLP
Principe de Vergara, 187
Plaza de Rodrigo Uria
28002 Madrid
Spain
Tel: +34 915 860 131
Fax: +34 915 860 403
cecilia.alvarez@uria.com
reyes.bermejo@uria.com
www.uria.com/en/index.html