The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

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 2
(published in November 2015 – editor Alan Charles Raul)

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

The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor

Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, Felicity Bown, Joel Woods

ACCOUNT MANAGER
Jessica Parsons

PUBLISHING MANAGER
Lucy Brewer

MARKETING ASSISTANT
Rebecca Mogridge

EDITORIAL ASSISTANT
Sophie Arkell

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Gina Mete

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 978-1-909830-75-2

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE 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

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ADVOKATFIRMAET SIMONSEN VOGT WIIG AS

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K.

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JUN HE LAW OFFICES

LEE & KO

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

PEARL COHEN ZEDEK LATZER BARATZ

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 23

SPAIN

Leticia López-Lapuente 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 Leticia López-Lapuente 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 has not undergone significant changes in the past year. However, worth highlighting is the 2015 reform of the Spanish Criminal Code approved by Law 10/1995 of 23 November. Some changes (which came into force on 1 July) affect privacy and IT sectors.

Although no significant issues have received broad media coverage in Spain, the DPA's activity has again increased and, as consequence of *Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González* case C-131/12 (*Google Spain*), followed last year before the Court of Justice of the European Union (CJEU) (regarding the 'right to be forgotten'), the DPA has initiated certain proceedings and has imposed sanctions also based on the new concept of 'establishment' following the *Google Spain* case's doctrine and principles (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 E-Commerce Law 34/2002 (LISS), the General Telecommunications Law 9/2014 (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 Spanish Criminal Code.

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.

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 a 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, to perform its services,

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 competence 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.

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 or 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, open data (reuse of public sector information) and anonymous data: the DPA is working on adopting an official position regarding the use of 'anonymous' data and open data in big data projects. In particular, the DPA intends to publish guidelines on the protection of personal data related to the reuse of public sector information. These guidelines will be submitted to an online public consultation.

e Cloud computing: in 2012 the Spanish DPA issued two cloud computing guidelines addressed to clients and service providers respectively. In 2015 the DPA has also carried out an *ex officio* investigation of cloud computing services in the education sector.

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]

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 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

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

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 16 BCRs related to the financial, insurance, consulting, pharma and technology sectors.

V COMPANY POLICIES AND PRACTICES

i 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*).

ii 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).

iii 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 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 2014 (the most recent official statistics published by the DPA): 8,068 (2.69 per cent more than in 2013) investigations were carried out; over 800 (827) procedures (0.61 per cent more than in 2013) were carried out declaring the existence of infractions; and the fines amounted to approximately €17 million (23.89 per cent less than in 2013). Most of the sanctions imposed on the private sector were for lack of consent and breach of the quality principle. The statistics show that the

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.

telecoms, energy and water supply, 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), €50,000 (breach of the quality principle) and €50,000 (breach of secrecy);

b financial entities: €50,000 (incorrect disclosure of a debt to a creditworthiness file), €50,000 (breach of the quality principle) and €50,000 (breach of secrecy);

c media operators and energy suppliers: €50,000 (lack of consent); and

d retail: €60,000 (spam).

ii Recent enforcement cases

The most significant issues in Spain in 2014–2015 are the following:

The DPA has carried out certain number of disciplinary proceedings related to the use of cookies (almost 30). In most cases it just gave a warning to the liable entity (i.e., no economic fines were imposed). The DPA has also imposed the first ever sanction based on the new concept of establishment created by the CJEU in *Google Spain*: 'It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46/EC is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary that is intended to promote and sell advertising space offered by that engine and that orientates its activity towards the inhabitants of that Member State.' In particular, the DPA imposed a €15,000 fine on an Irish company that acquired a credit portfolio from a Spanish bank. The DPA considered that the Irish company was processing data as part of the activities of an establishment in Spain based on the following criteria: first, the transaction was carried out in Madrid, where the relevant public deed was executed and the purchase agreement ratified. In addition, once the transaction was formalised, the person representing the Irish company stated that Madrid was its domicile 'for these purposes'. Second, the Irish company disclosed Spanish credit blacklist information on payment defaults, providing a Spanish contact address. Third, the Irish company used its data processor's premises in Barcelona, where the DPA's inspection of the Irish company took place (and where there was a representative of the Irish company) and the initiation of the disciplinary proceedings was notified. In addition, the Irish company regularly operates in this establishment in Barcelona (although not on a continuous basis).

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* CJEU case, 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). In addition, the Spanish Criminal Code was again amended in March 2015. Specifically, in line with European regulations on computer-related offences, the following new criminal offences are regulated: (1) intercepting data from information systems for the discovery and disclosure of secrets; and (2) creating computer programs or equipment for the purposes of discovering and disclosing secrets or committing damage to IT systems. Finally, legal entities can be held criminally liable for 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.

In 2012 the security breach notification regime was introduced in Spain through the GTL in line with Directive 2009/136/EC: 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 to notify 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 service providers), most of them remain unknown to the DPA and the public. One of those made public was the security breach suffered by BuyVip (which belongs to the Amazon group) in 2011, which involved the names, dates of birth, email 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 the sanction imposed on BuyVip, if any, was not made public.

The LISS was amended last year to establish specific obligations on cybersecurity incidents applicable to information society service providers, domain name 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.

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.

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 an 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.

In addition to the above-mentioned laws, certain authorities with specific cybersecurity responsibilities have issued guidance, such as the guidelines published by the Spanish National Institute of Cybersecurity (INCIBE) in 2015 regarding, among others, (1) how companies should manage information leaks, (2) cybersecurity for e-commerce, (3) security-related risk management for companies and (4) protocols and network security in industrial control systems infrastructures; 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 competence in relation to 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); the Secretary of State for Telecommunications and Information Society; and INCIBE (previously known as the National Institute of Communication Technologies), which is the public-sector company in charge of developing cybersecurity.

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'. Decisions of the CJEU (such as the declaration of the Data Retention Directive 2006/24/EC invalid or 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.

The adoption in 2016 of the EU's proposed new General Data Protection Regulation now seems more feasible. As the most recent draft of the new EU Regulation

is actually fairly similar to the current DP Regulations in Spain, as construed by the CJEU and the Article 29 Working Party, the main impact of the EU Regulation would probably be in relation to the new fines (which would follow criteria similar to those used in antitrust regulations – on the basis of a percentage of annual worldwide turnover); the general security breach notification; and the implementation (either voluntary or mandatory) of a data protection officer and privacy and security professionals involved in the business of organisations.

Appendix 1

ABOUT THE AUTHORS

LETICIA LÓPEZ-LAPUENTE

Uría Menéndez Abogados, SLP

Leticia López-Lapuente is a lawyer in the Madrid office of Uría Menéndez. She heads the firm's data protection and IT practice, and leads the LATAM data protection group.

Leticia focuses her practice on data protection, and commercial and corporate law, especially in the internet, software, e-commerce and technology sectors. She also advises on privacy law issues. Leticia provides clients operating in these sectors with day-to-day advice on regulatory, corporate and commercial matters, including the drafting and negotiation of contracts, M&A, privacy advice, consumer protection and e-commerce issues, corporate housekeeping, public procurement and RFP procedures, dealings with public authorities, etc. She has been involved in major transactions and assisted businesses and investors in these sectors.

She regularly speaks in national and international fora on personal data protection and technology, in addition to having written numerous articles on data protection-related matters.

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 such matters as privacy, 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, 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 on a number of master's programmes and seminars (the University of Valencia, the Financial and Stock Market Studies Foundation and CEU Cardinal Herrera University, Valencia).

She contributes to the firm's newsletter and legal magazine (*Actualidad Jurídica Uría Menéndez*) on all aspects of data protection, with particular attention to regulatory issues and updates to case law.

URÍA MENÉNDEZ ABOGADOS, SLP
Príncipe de Vergara, 187
Plaza de Rodrigo Uria
28002 Madrid
Spain
Tel: +34 915 860 131
Fax: +34 915 860 403
leticia.lopez-lapuente@uria.com
reyes.bermejo@uria.com
www.uria.com/en