

THE PRIVACY, DATA
PROTECTION AND
CYBERSECURITY
LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA
PROTECTION AND
CYBERSECURITY
LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER

Clare Bolton

HEAD OF BUSINESS DEVELOPMENT

Nick Barette

TEAM LEADERS

Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS

Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD

Kieran Hansen

EDITORIAL COORDINATOR

Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR

Adam Myers

PRODUCTION EDITOR

Anne Borthwick

SUBEDITOR

Jonathan Allen

CHIEF EXECUTIVE OFFICER

Nick Brailey

Published in the United Kingdom

by Law Business Research Ltd, London

Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

© 2021 Law Business Research Ltd

www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at September 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above.

Enquiries concerning editorial content should be directed
to the Publisher – clare.bolton@lbresearch.com

ISBN 978-1-83862-810-9

Printed in Great Britain by

Encompass Print Solutions, Derbyshire

Tel: 0844 2480 112

ACKNOWLEDGEMENTS

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

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS & PARTNERS

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAUIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 1	GLOBAL OVERVIEW.....	1
	<i>Alan Charles Raul</i>	
Chapter 2	EU OVERVIEW.....	6
	<i>William R M Long, Francesca Blythe, Denise Kara and Alan Charles Raul</i>	
Chapter 3	APEC OVERVIEW.....	43
	<i>Ellyce R Cooper, Alan Charles Raul and Sheri Porath Rockwell</i>	
Chapter 4	ARGENTINA.....	59
	<i>Adrián Furman and Francisco Zappa</i>	
Chapter 5	AUSTRALIA.....	70
	<i>Gavin Smith and Emily Cravigan</i>	
Chapter 6	BELGIUM.....	85
	<i>Steven De Schrijver and Olivier Van Fraeyenhoven</i>	
Chapter 7	BRAZIL.....	101
	<i>Ricardo Barretto Ferreira, Lorena Pretti Serraglio, Camilla Lopes Chicaroni and Nariman Ferdinian Gonzales</i>	
Chapter 8	CHINA.....	117
	<i>Hongquan (Samuel) Yang</i>	
Chapter 9	DENMARK.....	143
	<i>Tommy Angermair, Camilla Sand Fink and Caroline Sylvester</i>	
Chapter 10	ESTONIA.....	161
	<i>Risto Hübner</i>	
Chapter 11	GERMANY.....	173
	<i>Olga Stepanova and Patricia Jechel</i>	

Contents

Chapter 12	HONG KONG	182
	<i>Yuet Ming Tham</i>	
Chapter 13	HUNGARY.....	200
	<i>Tamás Gödölle and Márk Pécsvárady</i>	
Chapter 14	INDIA	213
	<i>Aditi Subramaniam and Sanuj Das</i>	
Chapter 15	INDONESIA.....	227
	<i>Danny Kobrata and Rahma Atika</i>	
Chapter 16	JAPAN	241
	<i>Tomoki Ishiara</i>	
Chapter 17	MALAYSIA	264
	<i>Shanthi Kandiah</i>	
Chapter 18	MEXICO	281
	<i>César G Cruz Ayala and Marcela Flores González</i>	
Chapter 19	NETHERLANDS.....	297
	<i>Herald Jongen, Nienke Bernard and Emre Yildirim</i>	
Chapter 20	PORTUGAL	310
	<i>Jacinto Moniz de Bettencourt and Beatriz Assunção Ribeiro</i>	
Chapter 21	RUSSIA	322
	<i>Vyacheslav Khayryuzov</i>	
Chapter 22	SINGAPORE.....	332
	<i>Yuet Ming Tham</i>	
Chapter 23	SPAIN.....	351
	<i>Leticia López-Lapuente and Reyes Bermejo Bosch</i>	
Chapter 24	SWITZERLAND	366
	<i>Jürg Schneider, Monique Sturny and Hugh Reeves</i>	
Chapter 25	TAIWAN.....	389
	<i>Jaclyn Tsai, Elizabeth Pai and Jaime Cheng</i>	

Contents

Chapter 26	TURKEY.....	402
	<i>Susen Aklan, Kaan Can Akdere and Melis Mert</i>	
Chapter 27	UNITED KINGDOM.....	419
	<i>William R M Long, Francesca Blythe and Denise Kara</i>	
Chapter 28	UNITED STATES.....	449
	<i>Alan Charles Raul and Snezhana Stadnik Tapia</i>	
Appendix 1	ABOUT THE AUTHORS.....	487
Appendix 2	CONTRIBUTORS' CONTACT DETAILS.....	505

SPAIN

*Leticia López-Lapuente and Reyes Bermejo Bosch*¹

I OVERVIEW

Cybersecurity and data protection are becoming essential values for society and, consequently, both areas have undergone significant legal development in recent years. In particular, a new law on cybersecurity and a new national data protection law were passed in the second half of 2018. Both laws are based on and mirror the corresponding EU Security of Network and Information Systems Directive (the NIS Directive) and the General Data Protection Regulation (GDPR). Nevertheless, data protection and privacy rules are more consolidated in the EU and Spain than cybersecurity regulations, which are currently being developed.

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, *inter alia*, 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 not sufficiently developed yet.

With regard to data protection, the main rules are the GDPR and Basic Law 3/2018 of 5 December on data protection and digital-rights guarantees (the Spanish Data Protection Law). With the approval of this law, former Spanish data protection laws and regulations were repealed.

In addition to the foregoing legal regime, there are sector-specific regulations that also include data protection provisions, since certain categories of personal data and certain processing activities may require specific protection such as the processing of personal data within the financial, e-communications or health-related sectors. There are several codes of conduct for data protection for various sectors. Some of these codes are still being reviewed pursuant to the GDPR and the Spanish Data Protection Law.

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). In the case of data protection, this balance must be primarily assessed by the organisation and individuals, and public entities and other organisations may

¹ Leticia López-Lapuente and Reyes Bermejo Bosch are lawyers at Uría Menéndez Abogados, SLP.

challenge the assessment 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). 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 imposing significant sanctions. The new DPA statutes have been approved in 2021 (through Royal Decree 389/2021 of 1 June). According to the most accurate information available on the DPA's website, in 2020 alone, the DPA received 10,324 claims from individuals, organisations and authorities (including authorities of other EU jurisdictions) and issued and published 172 sanctioning resolutions within the private sector. These sanctions are published on the DPA's website, which is used by the media (and others) as an important source of data protection information.

II THE YEAR IN REVIEW

Spanish law in this area has not changed significantly in the past year. The Spanish government is greatly involved in the 'Digital Spain 2025', a plan that contains 47 measures to drive digital transformation in Spain. However, covid-19 has held back their development this year.

Regarding the implementation of the NIS Directive, the Spanish government approved a law (by approving a Royal Decree-Law), which a new Royal Decree has recently developed (see Section IX). A draft rule on security in 5G technology was introduced in December 2020.

Moreover, as part of the 'Digital Spain 2025', the Digital Rights Charter, which reinforces and extend citizens' digital rights, has been recently approved. This Charter is not regulatory in nature, but rather proposes a framework of reference for future legislative projects.

Finally, at the time of writing, the DPA has in the past months issued a number of sanctioning resolutions through which it has imposed very high fines (between €5 million and €8 million) on Spanish banking and telecoms companies in connection with the transparency principle, subcontracting obligations and international data transfers.

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; the GDPR and the Spanish Data Protection Law.

Sector-specific regulations may also contain data protection provisions, such as the E-Commerce Law 34/2002 (LSSI), the General Telecommunications Law 9/2014 (GTL) (which will be replaced by a new law pending approval), anti-money laundering legislation, financial regulation or the regulations on clinical records or biomedical research. However, they generally refer to the former Spanish data protection regulations and, now that the GDPR and Spanish Data Protection Law are in force, will either be subject to review or should at least be reinterpreted according to the new rules.

Privacy rights are mainly regulated by the Spanish Constitution, 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 are 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 minors, political opinions, trade-union membership, religion or philosophical beliefs, racial or ethnic origin, genetic data, biometric data, health, criminal offences, sex life or sexual orientation are deemed more sensitive and require specific protection. This protection is established in the GDPR in the regulation on the ‘special categories of personal data’ or in specific and more restrictive rules for the processing of data of minors or data related to criminal offences. In addition to this additional protection granted in the GDPR, the Spanish Data Protection states that the processing of data related to administrative offences also requires additional measures.

Protecting personal data is achieved by allocating specific duties to both ‘controllers’ (i.e., those who decide on the data processing purposes and means) and ‘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 by both controllers and processors with the data protection duties imposed by the GDPR (fair information, legitimate ground, security, proportionality and quality, accountability, etc.)² and by the Spanish Data Protection Law (direct-marketing processing activities, credit bureaus, whistle-blowing schemes, video-surveillance, etc.). The DPA has in the past carried out and *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). More recently, in 2020, it has carried out a specific analysis of social healthcare, 5G technologies and anti-covid technologies. However, the DPA’s activity in terms of individual compliance investigations has significantly increased over the past 10 years, as has the number of fines imposed. Indeed, failure to comply with the GDPR and the Spanish Data Protection Law may result in the imposition of administrative fines depending on the severity of the offence (and regardless of whether civil or criminal offences are also committed, if applicable). The DPA has in the past months imposed its highest ever fines. Section VII.i below explains how the Spanish Data Protection Law has developed the general sanctioning regime set out in the GDPR. Neither harm nor injury is required for an administrative sanction to be imposed (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 for data subjects to claim damages arising from breaches of data protection rights before civil and criminal courts.

ii General obligations for data handlers

The main obligations of data controllers and data processors are those set out in the GDPR and in the Spanish Data Protection Law, but sector-specific Spanish regulations may also provide specific rules on the processing of personal data in a specific sector or activity (e.g., data included in clinical records).

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.

Obligations of data controllers

Any processing activity should be internally monitored, registered and documented:

- a* data controllers must assess risks before implementing data processing operations and must ensure from the design of any processing operations that data protection principles and rules are met (i.e. privacy by design and privacy by default);
- b* data subjects from whom personal data are requested must be provided beforehand with information about the processing of their personal data (the DPA published specific guidelines to comply with the GDPR rules on information duties; however, the DPA has established a new standard on terms of transparency through recent sanctioning resolutions as further explained in Section VII.ii);
- c* the processing of personal data must be based on a legitimate ground, among others, have the prior and explicit consent of the data subject, be based on the existence of a contractual relationship that makes the processing unavoidable, the existence of a legal obligation imposed on the controller or a legitimate interest;
- d* when the recipient is not located in the EU or EEA (or in a country whose regulations afford an equivalent or adequate level of protection identified by the European Commission or the DPA), appropriate guarantees must be adopted, unless a legal exemption applies;
- e* controllers should adopt appropriate security measures and notify the DPA and, in some cases, the affected data subjects, of any data breaches, as explained in Section IX; and
- f* as explained in Section III.iii, data subjects have specific rights concerning their personal data.

Obligations of data processors

Data processors must:

- a* execute a processing agreement with the relevant data controller;
- b* implement the above-mentioned security measures;
- c* process data only to provide the agreed services to the controller and in accordance with its instructions;
- d* keep the data confidential and not disclose it to third parties (subcontracting is not prohibited but is subject to specific restrictions);
- e* assist the controller by identifying any instructions that could infringe data protection rules and, if so agreed, assist in managing data protection requests from individuals;
- f* notify without delay any data breaches suffered that affect the controller's personal data;
- g* allow controllers to audit their processing; and
- h* upon termination of the services, return or destroy the data, at the controller's discretion.

iii Data subject rights

Data subjects have a right to access all data relating to them, to rectify their data and have their data erased if the processing does not comply with the data protection principles, in particular, when data are incomplete, 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, as well as to request the restriction of processing and the portability of their data.

In addition, the Spanish Data Protection Law establishes the obligation of the data controller to block the data during a reasonable term following rectification or erasure of the data, in order to prevent its processing but still have it available to judges and courts, the Public Prosecution Service or the competent public authorities (including the data protection authorities) in relation to potential liabilities derived from the processing and only during the applicable limitation period. Once the blocking period has ended, the data controller must delete the data.

As regards data subjects' right to obtain compensation for damage from data controllers or processors, the GDPR has reinforced the rights including the right of consumer organisations to bring class actions. The Spanish Data Protection Law adds no significant changes to the general regime provided in the GDPR.

Finally, the Spanish Data Protection Law incorporates into the Spanish legal system a list of new rights of citizens in relation to new technologies, known as 'digital rights'. These digital rights, which are not data protection rights as such but independent digital rights, can be divided into three categories:

- a* general rights aimed at all citizens, such as the right to the digital testament, to a digital education or to the digital security;
- b* specific rights addressed to providers of information society services and social networks, some of which seem to be a reaction to recent and significant public cases, such as the right to rectification or update of information over the internet or the right to be forgotten; and
- c* specific rights closely related to the use of technologies within the employment relationships, such as the right to privacy in the use of digital devices, of video surveillance and geo-localisation in the workplace.

These rights present some limitations on processing for these purposes, and employers' obligations to inform employees about access to the information stored on digital devices supplied by the employer to the employees, and for the use of video-surveillance systems and geo-localisation for the purposes of controlling employees. In addition, the novel 'digital disconnection right' is included, which aims to guarantee workers' and civil servants' break time, leave and holidays.

iv Specific regulatory areas

The data protection regulations apply to any personal data, but they provide for reinforced protection of data related to children (e.g., the verifiable consent of the minor's parents is required for children under 14) and to certain categories of especially protected data, such as health-related data (e.g., they may require the performance of a privacy impact assessment). The Spanish Data Protection Law incorporates – and comprehensively regulates – data processing activities that are not expressly regulated in the GDPR. This is the case, for example, of data processing activities for video-surveillance purposes, whistle-blowing channels and solvency and credit files. Some of these specific data processing activities were regulated in the former Spanish data protection regulations (e.g., solvency and credit files) or were the subject matter of specific guidelines by the DPA, in which case, in general, the Spanish Data Protection Law continues in the same vein regarding those guidelines or previous national regulations.

In addition, certain information is also protected by sector-specific regulations. This is the case for, *inter alia*:

- a* financial information that is subject to banking secrecy rules (Law 10/2014 of 26 June 2014 on the regulation, supervision and solvency of credit institutions);
- b* the use (for purposes other than billing) and retention of traffic and location data (GTL);
- c* the sources of information and intra-group disclosures to comply with regulations concerning anti-money laundering and combating the financing of terrorism, and restrictions on the transparency principle in relation to data subjects (Law 10/2010 of 28 April on the prevention of money laundering and financing of terrorism);
- d* the use of genetic data or information contained in biological samples (Law 14/2007 of 3 July on biomedical research);
- e* information used for direct-marketing purposes (LSSI);
- f* the outsourcing of core financial services to third parties (Royal Decree 84/2015 of 13 February developing Law 10/2014, and Bank of Spain Circular 2/2016 on the supervision and solvency of credit institutions, which adapts the Spanish legal regime to EU Directive 2013/36/EU and EU Regulation 575/2012); and
- g* the use of video-surveillance cameras in public places (Law 4/1997 of 4 August governing the use of video recording in public places by state security forces).

Since the above regulations generally refer to the data protection regulations, they need to be reinterpreted according to the GDPR and the Spanish Data Protection Law.

v Technological innovation

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

- a* electronic-privacy issues, including for ISPs, online platforms, and search engines;
- b* online tracking and behavioural advertising: as a general rule, explicit prior consent is required. The DPA does not generally consider that online behavioural advertising or profiling activities can be based on the existence of a legitimate interest. In addition, the DPA considers that profiling activities must be considered as separate processing activities from any others, such as advertising ones, and, as such, a specific and separate legal ground must legitimate these activities (e.g., a separate consent). The DPA has also developed (through recent sanctioning resolutions) the transparency requirements to be complied with in the context of profiling activities;
- c* location tracking: the Spanish Data Protection Law and the DPA consider that the use of this technology in work environments may be reasonable and proportionate provided that certain requirements and proportionality test are met (mainly, that specific information has been previously provided to data subjects on the potential monitoring of IT resources). In 2020, the DPA published documents analysing the processing of location data (some of them in the context of covid-19);
- d* use of cookies: as a general rule, explicit prior consent is required for installing cookies or similar devices on terminal equipment. In November 2019, the DPA published a 'Guide on the use of cookies'. However, only a few months later (in July 2020) the DPA felt it necessary to update its Guide, to mirror the Guidelines that the European Data Protection Board issued in May 2020 on the topic of consent. The updated Guide considers that the mere fact of continuing to view a screen, or scrolling or navigating through a website, will under no circumstances be considered a clear affirmative action.

- In addition, the Guide adopts a restrictive position on cookie walls. In 2020, the DPA received 1,602 claims and issued 73 sanctioning resolutions regarding internet services (certain of which included the use of cookies);
- e biometrics: traditionally, the processing of biometric data has not been considered 'sensitive' and, therefore, the implementation of the GDPR in Spain implies a change in the concept of biometrics, which are now considered especially protected data. The DPA has recently issued some reports and guidelines regarding biometric authentication and identification in different sectors (e.g., anti-money laundering);
 - f big data analytics: in April 2017, the DPA published guidelines on how to implement big data projects according to GDPR rules;
 - g anonymisation, de-identification and pseudonymisation: the DPA has adopted an official position regarding the use of 'anonymous' data and open data in big data projects. In particular, the DPA has published guidelines on the protection of personal data related to the reuse of public-sector information, anonymisation techniques and 'K-anonymity as a privacy measure' and it has published guidelines on the 'hash' as an pseudonymisation technique;
 - h internet of things and artificial intelligence: the DPA has recently published some reports and guidelines on GDPR adequacy to artificial intelligence (e.g. regarding the requirements applicable to audits of processing that include AI);
 - i data portability: the DPA has published a legal report on, among other issues, the data portability right. The DPA stated that the portability right includes not only data subjects' current data, but also their former data (either provided by them or inferred from the contractual relationship); however, the information obtained from the application of profiling techniques (e.g., algorithms) would not be subject to portability. Although the DPA's legal reports are not binding, they are highly useful since they reflect the DPA's doctrinal tendency;
 - j right of erasure or right to be forgotten: the right to be forgotten in relation to search engines is actively pursued both by Spanish data subjects and the DPA. Notably, *Google Spain*,³ in which the CJEU's ruling recognised the right to be forgotten, was initiated in Spain and the Spanish DPA had a significant role in the case. There are several DPA resolutions issued every year recognising the right of Spanish individuals to be forgotten and also setting out certain exceptions to the applicability of the right (see the ruling issued by the National Court on 22 November 2019 mentioned in Section II). Also, the Spanish Constitutional Court, in its ruling dated 4 June 2018, confirmed this approach and has recognised the right to be forgotten as a new fundamental right, different but related to data protection rights, and this was ultimately confirmed by the Spanish Data Protection Law, which has included the right to be forgotten as one of its new digital rights; in addition, the DPA includes in its website a specific section of 'right to be forgotten' in which data subjects may obtain specific information regarding the scope of this right as well as templates to carry out its exercise; and
 - k data-ownership issues: to date, there is no Spanish legislation that specifically regulates the question of ownership of data. Notwithstanding this, several regulations exist that may have an impact on data ownership including, among others, data protection legislation, copyright law (which regulates rights over databases) or even unfair competition rules.

3 Case C131/12.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

According to the data protection rules prior to the GDPR, data transfers from Spain to (or access by) recipients located outside the EEA required the prior authorisation of the DPA, unless the transfer could be based on a statutory exemption.⁴ However, this local regime was repealed by the GDPR and general rules in the GDPR applicable to international transfers of personal data apply directly in Spain. Also, the Spanish Data Protection Law does not include changes to the GDPR's general regime. Thus, international transfers of personal data cannot be carried out unless they are made to white-listed countries, if specific safeguards are adopted (such as BCRs or EU Model Clauses) or if they are based one of the derogations of Article 49 of the GDPR.

In addition, as a consequence of the *Schrems II* case before the European Court of Justice (ECJ) in July 2020 and the invalidity of the Privacy Shield scheme for transfers of personal data between Spain and the US, the DPA has encouraged Spanish controllers to adopt alternative means to ground any existing transfer to the US (e.g., the execution of Standard Contractual Clauses). Such means may include new sets of Standard Contractual Clauses approved by the European Commission in June 2021 and following recommendations 1/2020 of the EDPB.

Turning to data localisation, there are no specific restrictions in Spain; however, along with the GDPR (which imposes certain restrictions and requirements on disclosing data to non-EU entities), there are specific Spanish laws imposing requirements that could be understood as 'restrictive measures', including, among others, tax regulations (Royal Decree 1619/2012 of 30 November on invoicing obligations), gambling regulations (Royal Decree 1613/2011) and specific public administration regulations (Law 9/1968 of 5 April on secrecy pertaining to official issues, Law 38/2003 of 17 November on subsidies and Law 19/2013 of 9 December on transparency and access to public information).

V COMPANY POLICIES AND PRACTICES

i Privacy and security policies

Organisations that process personal data must comply with the accountability principle and, thus, are required to have both 'general' and 'specific' privacy policies, protocols and procedures. In addition, such policies are useful for (1) complying with the information duties regarding processing activities (see Section III.ii) and (2) complying with the duty to have all employees aware of the applicable security rules since organisations must implement appropriate technical and organisational measures to ensure a level of security that is commensurate with the risk (see Section IX).

To that end, organisations in Spain are adopting corporate privacy policies and cybersecurity prevention and reaction plans as part of their internal compliance programmes. Those policies not only comply with the above-mentioned duties but also evidence that principles such as privacy-by-design are duly implemented within the organisations. Approval at board and management level of these policies and strategies is also required, which thus reinforces the involvement of top management on data protection and cybersecurity matters. The DPA has approved specific guidelines regarding compliance with the privacy by default principle.

⁴ The DPA's prior authorisation is not required in the cases set out in Article 26 of EU Directive 95/46/EC.

In addition, as a consequence of the covid-19 pandemic, companies in Spain have had to implement tele-working strategies. The DPA has issued specific recommendations on how to protect personal data in tele-working situations.

ii Data protection officers

Before May 2018, a data protection officer was not mandatory, but in practice this role was deemed crucial for the controller or the processor to comply with the DP Regulations, in particular when the organisation is complex or if the data processed are sensitive or private.

From May 2018, several Spanish data controllers and processors are required to appoint a data protection officer according to Article 37 of the GDPR. The Spanish Data Protection Law expands and provides additional details on the cases in which the appointment of a data protection officer will be mandatory including, among others: financial entities, insurance and reinsurance companies, educational institutions, and private-security companies.

Under the former Spanish data protection regulations, the appointment of a security officer specifically in charge of implementation of security measures was required under certain circumstances, but from 25 May 2018, the appointment of this role is no longer mandatory.

The DPA has imposed its first sanctions (in both private and public sectors) for lack of compliance with the obligation of appointing a data protection officer.

iii Privacy impact assessments

Privacy impact assessments have been mandatory for certain data processing as from May 2018. For this reason, the DPA has published guidelines on how to carry out privacy impact assessments. However, the DPA has been encouraging the adoption of privacy impact assessments in certain cases (e.g., big data projects) since 2014 (when it published its first guidelines on the matter). Finally, it must be noted that Spain published the list of cases in which a privacy impact assessment must be carried out (e.g., when the processing involves data subjects in special conditions of vulnerability or when special categories of data are processed and the processing is not merely incidental or accessory). To provide support in this complex field, the DPA designed an electronic tool (publicly available on its website) to carry out privacy impact assessments. The DPA has recently approved new guidelines on privacy impact assessments and risk analysis.

iv Data mapping

As part of the mandatory risk analysis, organisations should carry out data-mapping activities regarding the collection, use, transfer and storage of personal data. The DPA offers various electronic tools to help organisations in this regard; however, these tools are intended for either small companies or companies that carry out simple processing activities.

v Work councils

Employee representatives – works councils and employee delegates – are entitled to issue a non-binding report before new methods of control of work are put into place or if existing methods are modified. Since what qualifies as a ‘method of control’ of work is sometimes debatable and unclear, it is generally advisable to inform the employee representatives of the implementation or modification of control methods (e.g., whistle-blowing systems or IT acceptable-use policies) and offer them the possibility of issuing the non-binding report.

VI DISCOVERY AND DISCLOSURE

Non-EU laws are not considered, as such, a legal basis for data processing, in particular regarding transfers to foreign authorities and especially if they are public authorities. This approach is consistent with Article 6.3 of the GDPR.

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 Spanish DPA's position is the one adopted by all EU DPAs in the Guidelines on Article 49 of Regulation 2016/679 adopted by the Article 29 Working Party (currently, the European Data Protection Board (EDPB)). According to this joint position, data transfers for the purpose of formal pretrial discovery procedures in civil litigation or administrative procedures may fall under derogation of Article 49 of the GDPR. According to the DPAs, this rule of the GDPR can also cover actions by the data controller to institute procedures in a third country, such as commencing litigation or seeking approval for a merger. Notwithstanding this, the derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA is the independent authority responsible for the enforcement of the GDPR and DP Regulations⁵ and the data protection provisions of the LSSI and the GTL.

Among other powers and duties, the DPA has powers that include 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). It is worth noting that the Spanish Data Protection Law has further developed the general and rather vague sanctioning regime set out in the GDPR, by providing, on the one hand, three categories of infringements (minor, serious and very serious) which depend on the type and seriousness of the breach – rather than the mere two fine ranges set out in the GDPR – and, on the other hand, a detailed administrative sanctioning and investigation system and procedures.

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).

The DPA is very active: in addition to *ex officio* inspections of specific sectors (always announced in advance), in 2020 (the most recent official statistics published by the DPA): 10,324 complaints from individuals were solved and the fines imposed amounted to approximately €8 million.

ii Recent enforcement cases

The following are the most significant enforcement issues to have arisen in Spain in 2020.

⁵ See footnote 2.

The DPA has carried out numerous disciplinary proceedings related to video-surveillance (94), internet services (73) and direct marketing by electronic means (17). The DPA has also issued several reports assessing the interpretation of both the GDPR and the New Spanish Data Protection Law and has published new automated tools to allow start-ups to comply with GDPR obligations and to facilitate data controllers to comply with their notification duties (in connection with data breaches) vis-a-vis the data subjects.

In addition, the number of proceedings carried out and sanctions imposed by the DPA against non-Spanish and non-EU controllers has also increased. The DPA has indicated that it has participated in 451 cases of cross-border cooperation and in 17 cases as leading authority.

On the other hand, it is worth noting is that the DPA imposed its highest-ever economic fines between December 2020 and March 2021. It issued three sanctioning resolutions fining Spanish banking and telecoms companies €5 million, €6 million and €8 million fines, respectively. Both data controllers and data processors should take good note of these resolutions since they provide useful recommendations to comply with the transparency and accountability principles in the context of subcontracting and analyse the contractual measures that should be implemented for international transfers of data.

iii Private litigation

Data subjects may claim damages arising from the breach of their data protection rights before the 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 limited exceptions such as one awarding €20,000). Notwithstanding this, recognition under the GDPR of the possibility to initiate class actions related to data protection matters has created a new framework and there is news in the market around the recent initiation by the Spanish consumers association of class actions against one of the largest social media platforms for alleged data protection infringements.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The application of the DP Regulations for foreign organisations was triggered by either the existence of a data processor or processing equipment in Spain or, according to Google Spain, the existence of an establishment in Spain, the activity of which is inextricably linked to that of the foreign organisation. Following 25 May 2018, after the GDPR rules became applicable, the extraterritorial applicability of EU data protection legal framework is reinforced as a result of the GDPR's territorial scope rules under Article 3.2 of the GDPR.

According to them, offering goods and services to EU citizens and online tracking addressed to the EU or Spanish market may trigger the application of the data protection provisions not only of the GDPR but also of the LSSI, as well as the consumer regulations (only if consumers resident in Spain are involved), irrespective of where the organisation is established.

There are some rules in Spain that require specific types of data (e.g., anti-money laundering, health data, specific financial records held by credit institutions or public archives, classified data relevant to national security) to be stored and processed within Spanish territory (unless an exception applies).

IX CYBERSECURITY AND DATA BREACHES

The approval in July 2016 of the NIS Directive was the most significant cybersecurity milestone in recent years. It marks the first instance of EU-wide rules on cybersecurity. Spain was late in implementing the NIS Directive, but in September 2018 a law was finally passed. In particular, the NIS Directive was implemented into Spanish law through Royal Decree-Law 12/2018 of 7 September, on the security of networks and information systems; since Royal Decree-Law 12/2018 provides general and unspecific rules, Royal-Decree 43/2021 has recently been approved to develop specific aspects of Royal Decree-Law 12/2018.

Royal Decree-Law 12/2018 and Royal-Decree 43/2021 are consistent with the NIS Directive and, in general, do not introduce particularities. Royal Decree-Law 12/2018 and Royal-Decree 43/2021 only apply to operators of essential services⁶ located in Spain and digital service providers registered in Spain (provided that Spain constitutes its main establishment in the EU). As to notifying security breaches, Royal-Decree 43/2021 has introduced a National Platform for Notifying and Tracking Cyber Incidents and a specific Annex on how cyber incidents are to be reported and handled.

However, in addition to cybersecurity duties arising from the NIS rules, security and cybersecurity duties can be found in other Spanish rules. This means that the legal regime is rather disseminated and complex. We provide a summary below.

For instance, the GDPR also establishes specific security duties for data controllers and processors when processing personal data, as well as notification duties in the event of data breaches. For this reason, the DPA is highly active in relation to cybersecurity matters. In the context of the covid-19 pandemic, the DPA has been publishing posts on its website regarding security breaches, including:

- a* top five technical measures to be taken into account;
- b* security breaches notified within the state of emergency; and
- c* phishing campaigns related to covid-19.

Moreover, the DPA has just published new security breaches guidelines that include a new notification form that broadens the level of detail of the information to be provided to the DPA (when such notification is mandatory).

As to criminal law, the Spanish Criminal Code was amended in 2010 to implement the Convention on Cybercrime and Council Framework Decision 2005/222/JHA on attacks against information systems. Specifically, this entailed the introduction of two new criminal offences:

- a* 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
- b* the intentional deletion, damage, deterioration, alteration or suppression of data, applications and electronic documents of third parties rendering 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

⁶ They are mainly operators of critical infrastructure. More information below.

property). The Criminal Code was amended again in March 2015. Specifically, aligned 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 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. Also, the LSSI was amended in 2014 to establish specific obligations on cybersecurity incidents applicable to information society services providers, domain name registries and registrars. These obligations are twofold:

- a* to collaborate with the relevant computer emergency response teams to respond 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
- b* to follow specific recommendations on the management of cybersecurity incidents, which will be developed through codes of conduct (these have not yet been developed).

In addition to the obligations set out in Royal Decree-Law 12/2018 and Royal-Decree 43/2021, operators of critical infrastructure⁷ (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 inspections performed by the competent authorities, and creating the specific protection plan and the operator’s security plan. 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 43/2021 has included the mandatory appointment of an information-security officer by operators of essential services. Royal-Decree 43/2021 provides a list of functions and responsibilities as well as a list of requisites to be complied with by the information security officer. The provisions included in Royal-Decree 43/2021 should prevail over the current framework under Law 8/2011; however, no derogative provisions have been included.

Furthermore, Spanish Royal Decree 3/2010 establishes the security measures to be implemented by Spanish public authorities (the ‘National Security Scheme’) 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: the

⁷ The following infrastructure areas have been considered critical by Law 8/2011 (which transposes Directive 2008/114/EC into Spanish law): administration, water, food, energy, space, the chemical industry, the nuclear industry, research facilities, health, the financial and tax system, ICT and transport.

organisational framework, which is composed of the set of measures relating to the overall organisation of security; the 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 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. A draft of the new National Security Scheme has been published pending its approval by the government.

In addition to the above-mentioned laws, certain authorities with specific cybersecurity responsibilities have issued guidance, such as:

- a* the most recent guidelines published by the Spanish National Institute of Cybersecurity (INCIBE) regarding, inter alia:
 - cyber-threats against business environments (2021);
 - ransomware (2021);
 - glossary of cybersecurity terms (2021);
 - teleworking cybersecurity (2020);
 - security in the installation and use of IoT devices (2020);
 - smart toys cybersecurity (2020);
 - wi-fi network security (2019);
 - backup files (2018);
 - increased competitiveness by complying with the GDPR (2018); and
 - cloud computing (2017);
- b* the publication by INCIBE in 2016 of a consolidated code of cybersecurity rules in Spain (amended in July 2021);
- c* the National Cybersecurity Strategy issued by the presidency in April 2019;
- d* the strategy series on cybersecurity issued by the Ministry of Defence.

The agencies and bodies with competence in cybersecurity are numerous and include:

- a* the CCN, which is part of the National Intelligence Centre;
- b* the CCN Computer Emergency Response Team;
- c* the CNPIC;
- d* the Cybersecurity Coordinator's Office (which is part of the CNPIC);
- e* the Secretary of State for Digitalization and Artificial Intelligence;
- f* the Secretary of State for Telecommunications and Digital Infrastructures; and
- g* INCIBE (previously known as the National Institute of Communication Technologies), which is the public-sector company in charge of developing cybersecurity.

Finally, also related to cybersecurity and security legal duties, Spanish legislation includes disseminated rules on data retention or deletion rules. Most of these rules are sector-specific (e.g., AML rules establish retention duties of 10 years for certain information). However, the scope of some of these rules is more general and applies to the vast majority of companies in Spain, such as Article 30 of Spanish Commercial Code, which obliges companies to retain documentation with an impact on accounting for at least six years. More recently, the New Spanish Data Protection Law set out general retention rules, such as the one-month retention rule applicable to video surveillance.

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 to 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 ‘data-driven economy’), the active voice of users in the digital environment (developing new social interactions and not only acting as consumers) and the fact that the European Commission and the European Parliament have definitively embraced a strong ‘privacy mission’. Decisions of the CJEU (such as in the *Schrems I and II v. Facebook* or in the *Google v. Costeja* cases) have also sent out a clear message on the importance of data protection rules in Europe.

The adoption in 2016 of the GDPR constituted a significant milestone in the construction of a new data protection environment. In Spain, the approval of the Spanish Data Protection Law in 2018 represents a challenge for Spanish companies, which must deal not only with the GDPR provisions but also with the new set of particularities included by the Spanish Data Protection Law that affect specific processing activities such as those involving solvency files, direct-marketing activities and video surveillance. Although the GDPR provides for data protection principles that are similar to those of the repealed Directive 95/46/EC and former Spanish data protection regulations, as construed by the CJEU and the EDPB, it also provides for new rules and standards. Spanish organisations are particularly concerned about the fines (the applicable criteria for which would be similar to those used in antitrust regulations – a percentage of annual worldwide turnover), the accountability principle, the general security breach notification and the mandatory implementation of a data protection officer. Additional requirements regarding information and consent duties set out in the GDPR will also be a challenge for Spanish data controllers.

Also, we expect the regulation of the cybersecurity legal regime to change in Spain in the coming months, particularly if the Spanish public authorities implement the draft rule on 5G security and the new National Security Scheme.

ABOUT THE AUTHORS

LETICIA LÓPEZ-LAPUENTE

Uría Menéndez Abogados, SLP

Leticia López-Lapuente joined Uría Menéndez in 2004. She was named partner in 2019. She heads the firm's data protection and e-commerce area and also leads the LatAm data protection group. Leticia focuses her practice on data protection, 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, and dealings with public authorities. She has been involved in major transactions and assisted businesses and investors in these sectors.

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.

REYES BERMEJO BOSCH

Uría Menéndez Abogados, SLP

Reyes Bermejo is a lawyer based in both the Madrid and Valencia offices of Uría Menéndez. She became a lawyer 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 in the above-mentioned areas, on matters such as privacy, consumer protection and e-commerce, and dealings with public authorities, including the drafting and negotiation of IT agreements. 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 preparing 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 various master's degree programmes and seminars.

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

URÍA MENÉNDEZ ABOGADOS, SLP

c/Príncipe de Vergara, 187

Plaza de Rodrigo Uría

28002 Madrid

Spain

Tel: +34 915 860 131

Fax: +34 915 860 403

leticia.lopez-lapiente@uria.com

reyes.bermejo@uria.com

www.uria.com

an LBR business

ISBN 978-1-83862-810-9