IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

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

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 17

SPAIN

Leticia López-Lapuente and Ignacio Esteban Avendaño[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, which has recently been replaced and updated by the passing of the NIS 2 Directive in December 2022, yet to be transposed in Spain) 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 and pending of approval (such as the Cyber Resilience Act or the Cyber Solidarity Act).

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 the Spanish Data Protection law, former Spanish data protection laws and regulations were repealed. On the other hand, Spain has implemented Directive 2016/680 through Basic Law 7/2021 of 26 May on the processing of personal data for the purposes of the prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties.

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

1 Leticia López-Lapuente is a partner and Ignacio Esteban Avendaño is a senior associate at Uría Menéndez Abogados, SLP.

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 have been recently reviewed and approved 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 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 DPA statutes were approved in 2021 (through Royal Decree 389/2021 of 1 June). According to the most accurate information available on the DPA's website, in 2022 alone, the DPA received 15,128 claims from individuals, organisations and authorities (including authorities of other EU jurisdictions) and imposed 378 economic fines totalling €20,775,361. 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

At the EU level, creating the Digital Single Market is one of the most ambitious European projects. In this regard, some European regulations (which apply directly in Member States) have been approved since last year (such as the Data Governance Act and the Digital Services and Market Services Acts). Spanish law in this area has not changed significantly in the past year. The Spanish government is greatly involved in the 'Digital Spain 2026', a plan that contains 42 measures to drive digital transformation in Spain. However, covid-19 and the war in Ukraine have held back their development.

Regarding the implementation of the NIS Directive (see Section IX), the Spanish government is currently reviewing the national cybersecurity laws. On the other hand, a law on security in 5G technology was approved in March 2022.

Finally, at the time of writing, the DPA has in the past months issued a number of sanctioning resolutions through which it has imposed fines in the millions of euros on Spanish banking, telecoms and energy companies in connection with the transparency, legitimacy and accountability principles, among others. Moreover, the DPA has also fined Google LLC (based in the US) €10 million in connection with the right to erasure and the content takedown proceedings that Google makes available to users in its different products. With regard to sanction proceedings, it is worth noting that in December 2022 the Spanish National Court annulled a sanctioning decision imposed on a bank with fines amounting to €5 million on the basis of procedural defects. In particular, the Spanish National Court upheld the bank's argument that the rules of procedure had not been complied with by the DPA because there was a mismatch between the complaints that motivated the proceedings and the infringements in the sanctioning decision, as the DPA had not examined the complaints in question but used them to open a general investigation into the bank's data protection policies.

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 11/2022 (GTL) (which has been recently approved) and Law 2/2023 on the protection of persons who report violations of the law and the fight against corruption (which has also been recently approved), 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. A Digital Rights Charter was also approved in 2021, which reinforces and extends citizens' digital rights. This Charter is not actually a regulation, but rather proposes a reference framework for future legislative projects.

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 *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 2021, it has carried out a specific analysis of remote monitoring of clinical trials and data protection risks arising from covid certificates. However, the DPA's activity in terms of individual compliance investigations has

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.

significantly increased over the past 10 years, as has the number of fines imposed. 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 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 or images captured by CCTV cameras).

Main 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 is establishing new standards on terms of transparency through 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.

Main 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 pertaining 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, 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 destroy 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 geolocation 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 geolocation 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 concerning 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, for 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);

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); and

h whistle-blowing channels' information (Law 2/2023 on the protection of persons who report violations of the law and the fight against corruption).

Because 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 considered that the mere fact of continuing to view a screen, or scrolling or navigating through a website, shall under no circumstances be considered a clear affirmative action. In addition, the Guide adopted a restrictive position on cookie walls. Recently, in July 2023, the DPA updated again the Guide in order to incorporate the Guidelines that the European Data Protection Board issued in February 2023 about deceptive design patterns in social media platform interfaces. The update imposes new requirements such as the actions of accepting or rejecting cookies having to be presented in a prominent place and format, and both at the same level, without it being more complicated to reject them than to accept them. The new criteria is effective as from January 2023. In 2022, the DPA received 2,221 claims and there were 89 sanctioning proceedings 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 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 a 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 because 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 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 (however, the Data Governance Act – recently approved in the EU – applies in Spain). 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.

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 binding corporate rules 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 (CJEU) in July 2020 and the invalidity of the Privacy Shield scheme for transfers of personal data between Spain and the US, the DPA encouraged Spanish controllers to adopt alternative means to ground any existing transfer to the US (e.g., the execution of Standard Contractual Clauses), such as new sets of Standard Contractual Clauses approved by the European Commission in June 2021 and following recommendations 1/2020 and 5/2021 of the European Data Protection Board (EDPB).

However, the European Commission recently adopted on 10 July 2023 its adequacy decision for the EU–US Data Privacy Framework, taking into account the concerns raised

3 Case C131/12.

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

by the European Court of Justice in the *Schrems II* case, and recent changes in US legislation (particularly, in the field of national security). Therefore, international data transfers to the US may now rely on the EU–US Data Privacy framework provided such transfers are made to companies who have adhered to this new framework.

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 as 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.

In addition, as a consequence of the covid-19 pandemic, companies in Spain have had to implement teleworking strategies. The DPA has issued specific recommendations on how to protect personal data in teleworking 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. In any case, note that voluntarily appointing a data protection officer where not mandatory is considered an attenuating circumstance to grade the amount of administrative fines pursuant to the Spanish Data Protection Law.

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 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, 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 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. Because 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

Spain has implemented – through Basic Law 7/2021 of 26 May – Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Under Basic Law 7/2021, any Spanish national or citizen and any legal entity with a registered office in Spain must cooperate with the requesting police authority, public prosecutor or criminal court and provide the information requested as long as the following data protection requirements – if applicable – are met: (1) the request is limited and specific (proportionality principle) and (2) data subjects are informed unless a legal exception applies (transparency principle). Therefore, provided the disclosure falls under Basic Law 7/2021, its applicable legal basis will be Article 6.1.c of the GDPR.

From an international standpoint, 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 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 Regulations[5] 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 (nonbinding) legal reports, recommendations, instructions and contributions to draft rules; powers of investigation (now even by videoconference); 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). 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 2022 (the most recent official statistics published by the DPA): 15,128 complaints from individuals were solved and the fines imposed amounted to approximately €21 million.

ii Recent enforcement cases

The following are the most significant enforcement issues to have arisen in Spain in 2022.

The DPA has carried out numerous disciplinary proceedings related to video surveillance (164), internet services (89) and direct marketing by electronic means (29). The DPA has also issued several reports assessing the interpretation of both the GDPR and the Spanish

5 See footnote 2.

Data Protection Law and has updated automated tools to allow startups to comply with GDPR obligations and to facilitate data controllers to comply with their notification duties (in connection with data breaches) with regard to the data subjects.

In addition, the number of proceedings carried out and sanctions imposed by the DPA against non-Spanish and non-EU controllers is very high. The DPA has indicated that it has participated in 201 cases of cross-border cooperation and in 15 cases as leading authority.

On the other hand, Google LLC's €10 million fine is the highest the DPA has ever imposed to date. Both data controllers and data processors should take good note of the DPA's resolutions because they provide useful recommendations to comply with the data protection principles.

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, now replaced and updated by the NIS 2 Directive passed in December 2022. 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 transposed 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 was 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 services 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. Note that depending on the sector in which companies operate, companies are subject to different competent authorities under Royal Decree-Law 12/2018 and Royal-Decree 43/2021.

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 published an updated version of its security breaches guidelines that include a notification form that broadens the level of detail of the information to be provided to the DPA (when such notification is mandatory). Some sections of the notification form have also been updated in 2021. Additionally, the DPA published guidelines on security and privacy on the internet.

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 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, as detailed below.

In 2012, the security breach notification regime was introduced in Spain through the former General Telecommunications Law (Law 9/2014) (current, Law 11/2022) 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 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 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 their appointment must be communicated to this Ministry. The security officer does not need a legal authorisation, but their 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 43/2021should prevail over the current framework under Law 8/2011; however, no derogative provisions have been included.

Furthermore, Spanish Royal Decree 311/2022 (recently approved) establishes an updated version of the security measures to be implemented by Spanish public authorities (the new '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 organisational framework, which is composed of the set of measures concerning the overall organisation of security; the operational framework, consisting of the measures to be taken to protect the operation of the system

6 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.

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.

Finally, Royal Decree-Law 7/2022 of 29 March, on the requirements to ensure security of 5G networks and electronic communications has recently been approved. Royal Decree-Law 7/2022 follows Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks and Communication from the Commission COM (2020) 50 final of 29 January 2020 regarding Secure 5G deployment in the EU (Implementing the EU toolbox).

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:
- defence of endpoints in industrial control systems (2023)
- cybersecurity guide. Cybersecurity for everyone (2022)
- cybersecurity in tourism and leisure activities (2021);
- 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 2022);

c the National Cybersecurity Plan issued by the presidency in March 2022;

d the National Cybersecurity Strategy issued by the presidency in April 2019; and

e 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 Centro Criptográfico Nacional (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 Digitalisation 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., anti-money laundering 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 Spanish Data Protection Law set out general retention rules, such as the one-month retention rule applicable to video surveillance.

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

In relation to the development of information technologies (including software) and to the extent such software processes personal data, the principle of 'data protection by design'[7] mandates that appropriate technical and organisational measures are adopted (such as data monitoring or pseudonymisation) when developing, designing, selecting or using applications, services or products whose functions entail the processing of personal data. Safeguards to ensure data protection principles and obligations can be fulfilled (e.g., transparency, data minimisation, storage limitation, data localisation and cybersecurity) need therefore to be integrated in the design of the software. Similarly, the principle of 'data protection by default'[8] establishes that technical and organisational measures must be adopted so as to ensure only the necessary data is processed, which is a practical implementation of the data minimisation principle. In this sense, data protection obligations are extended to the pre-production phase when developing information technologies that will involve the processing of personal data. In this regard, we note that the Spanish DPA has issued specific Guidelines on the principles of data protection by design (2019) and by default (2020) that are not only addressed to data controllers or processors but also to developers and providers that seek to offer products and services that facilitate the data protection compliance of data controllers and processors.

Additionally we note that depending on the context in which the software is intended to be used (e.g., financial, health, whistle-blowing, public sector) or the concerned data subjects (e.g., minors) more specific rules, as stated in the foregoing sections, should also be taken into account when developing information technologies.

On a final note, we highlight that as part of the Spanish government's interest in fostering innovation, it has recently approved Law 7/2020 for the digital transformation of the financial system. This law creates a regulatory sandbox in the financial sector for the secure development of technology projects.

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

As part of the digital governance strategy at the EU level, the European Commission is issuing a series of rules aimed at regulating information technology platforms such as the Data Governance Act (May 2022), the Digital Markets Act (September 2022) and the Digital Services Act (October 2022) – complemented in Spain by Law 15/2007 on the Defence of Competition and the LSSI. In Spain, the Spanish National Markets and Competition Commission is the authority in charge of enforcing competition rules and is the national competent authority relevant to cooperation and coordination activities in competition matters with the European Commission.

7 Article 25.1 GDPR.

8 Article 25.2 GDPR.

In this area, Spain has not issued regulations, policies or enforcement actions that significantly diverge from those at the EU level. Among latest enforcement actions of the Spanish National Markets and Competition Commission, we highlight that several companies, among them Amazon and Apple, were fined with a total of €194.15 million for agreeing upon and implementing certain restrictions of competition in Amazon's online marketplace that affect third-party resellers of Apple products and products competing with Apple. Only a number of resellers appointed by Apple could sell Apple-branded products on Amazon's website in Spain, and Apple competing brands were restricted in purchasing advertising space on Amazon's website in Spain to advertise their products (e.g., Amazon could not, without Apple's consent, conduct marketing and advertising campaigns that targeted customers who purchased Apple products on Amazon's website in Spain and encourage those consumers to switch to a competitor's product).

XII 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 a result of 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 as the Digital Single Market has been developed through the approval of major regulations such as the Data Governance Act and the Digital Services and Market Services Acts and sector specific rules that are pending to be approved such as the European Health Data Space.

ISBN 978-1-80449-214-7