Spain

Carlos Pérez Sanz

Ecija Abogados

Pia Lestrade Dahms

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Currently, the principal data protection legislation is the Spanish Data Protection Act 15/1999 (the "**LOPD**"). Royal Decree 1720/2007 (the "**RLOPD**") is ancillary to the LOPD and sets out security measures for personal data and further regulation. However, this regulation is set to be modified.

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repeals Directive 95/46/EC (the "**Data Protection Directive**") and leads to increased (though not total) harmonisation of data protection law across the EU Member States. In Spain, a draft bill (the "**Draft LOPD Bill**") is currently before the Spanish Parliament (please note: these answers were written before the Draft LOPD Bill was adopted; consequently, they might not reflect the final adopted text). This bill is intended to repeal the current LOPD and any provisions of equal or inferior category that contradict, oppose or are incompatible with the GDPR and the Draft LOPD Bill. Further, in its current version, the Draft LOPD Bill is intended to enter into force from 25 May 2018.

1.2 Is there any other general legislation that impacts data protection?

Organic Law 1/1982 on civil protection of the rights to honour, personal and family privacy and an individual's own image.

Gross privacy non-disclosure violations might be prosecuted under criminal charges in accordance to Art. 197 of the Criminal Code.

Law 34/2002 on information society services and ecommerce (the "**LSSI**"). This law covers the e-marketing communications regime, internet service provider (ISP) liability and anti-spam regulation.

1.3 Is there any sector-specific legislation that impacts data protection?

A large number of sector-specific legislation is available. A few examples are listed below:

(a) Art. 96 of the Spanish Consumer Rights Act *Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias*, in connection with Art. 29 of *Ley 3/1991 de 10 de enero, de competencia desleal*, as modified by Law 29/2009. According to this regulation, marketing phone calls must be clearly identified as such, and fully disclose the identity of the calling company. In every communication, recipients shall be offered the opportunity to oppose to further calling. Human operators are allowed for telemarketing only. Recorded telemarketing campaigns need the prior recipient to opt-in.

(b) Art. 41 of the Spanish Telecoms Act *Ley 9/2014, de mayo, General de Telecomunicaciones* sets forth privacy standards for telecommunications, including compulsory notifications to the Data Protection Authority (the "**DPA**") and to data subjects in the case of breaches or violations of security. Art. 48 further provides that customers' geolocation information (latitude data) should always be processed anonymously. Nominal customer geolocation is only allowed when strictly necessary and indispensable for the provision of value-added services expressly requested by the customer. In such a case, the customer should be informed about the extent, purpose and duration of this processing.

(c) Insurance legislation such as *Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados* and *Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados* contain data protection provisions specific to the insurance industry.

(d) Legislation specific to healthcare service provision sheds light on rights to access health records and mandatory conservation timeframes of such information. The most important piece of legislation is *Ley 41/2002, de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*.

(e) Art. 17 of *Ley 59/2003 de firma electrónica* covers data privacy issues related to electronic signature.

(f) *Real Decreto 1553/2005, de 23 diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica* covers electronic identity card usage.

(g) Art. 6.2b of Ley 11/2007 *de Acceso electrónico de los ciudadanos a los servicios públicos* provided the citizens' right to get in touch with the public administration by electronic means. It has now been derogated by Ley 39/2015, *de 1 octubre, del Procedimiento administrativo común de las administraciones públicas*. The public administration must ensure security measures when handling a citizen's data with regards to such communication.

(h) The Spanish Data Retention Act *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*. This act governs carrier companies' obligations to retain traffic and personal data related to such traffic.

(i) Art. 20.3 of *Real Decreto Legislativo 2/2015, de 23 de octubre, del Estatuto de los Trabajadores*. This article sets out that control measures on employees are permitted.

1.4 What authority(ies) are responsible for data protection?

The main data protection authority is the *Agencia Española de Protección de Datos* (the "**AEPD**" or "**Spanish DPA**"). However, there are also regional data protection authorities in Catalonia and the Basque Country with powers essentially over public entities within their respective territory.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**" means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**" are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data").*

  There are no other key definitions to be aware of.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of data subjects who are in the EU in relation to: (i) the offering of goods or services (whether or not in return for payment) to data subjects who are in the EU; or (ii) the monitoring of the behaviour of data subjects who are in the EU (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of data subjects who are in the EU (to the extent such behaviour takes place in the EU).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**

Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

■ **Data minimisation**

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

■ **Accuracy**

Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

■ **Retention**

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

■ **Data security**

Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

■ **Accountability**

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to data/copies of data**

A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

■ **Right to rectification of errors**

Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

■ **Right to deletion/right to be forgotten**

Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

■ **Right to object to processing**

Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

■ **Right to restrict processing**

Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

■ **Right to data portability**

Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

■ **Right to withdraw consent**

A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

■ **Right to object to marketing**

Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

■ **Right to complain to the relevant data protection authority(ies)**

Data subjects have the right to lodge complaints concerning the processing of their personal data with the competent data protection authority in Spain, if the data subjects live in Spain or the alleged infringement occurred in Spain.

■ **Right to basic information**

Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under the LOPD/RLOPD, businesses must register with/notify the Spanish DPA before creating files containing personal data. They must also notify any modifications or cancellations of such files to the Spanish DPA (see the LOPD/RLOPD).

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

It must be specific. The specific forms are available on the Spanish DPA's website and cannot be submitted unless the required information is filled out.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations/notifications are made per legal entity and type of processing.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

All of the above must register with the relevant data protection authorities.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The mandatory fields are the following:

- Information of the declarant.
- Information of the data controller (name, industry, CIF/NIF number and address).
- Valid address for exercising rights of access, opposition, rectification and erasure (if different).
- Information on relevant data processors (if any).
- File name.
- Purpose of processing.
- Source/origin of data.
- Categories of data under processing.
- Security level (basic, medium or high).
- Processing methods (automated, manual or mixed).
- Transfer of data to third parties (data surrender or disclosure).
- International transfers (for transfers outside of the European Economic Area).

6.6 What are the sanctions for failure to register/notify where required?

Failing to notify files, or doing so in an inaccurate way, constitutes a minor infringement on the grounds of Art. 44.2.c of the LOPD (and will incur a fine of EUR 900 to EUR 40,000). Failure to notify files after being expressly mandated to do so by the DPA constitutes a serious infringement punishable by a fine of between EUR 40,001 and EUR 300,000.

6.7 What is the fee per registration/notification (if applicable)?

There is no fee.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

There is no set renewal obligation for registrations/notifications. However, any modifications to the categories listed under question 6.5 must be notified. Further, a notification must also be submitted when a data processing stops taking place (is discontinued) or when data processing is transferred to a new data controller.

6.9 Is any prior approval required from the data protection regulator?

There is no prior approval required for these registrations/notifications. However, please note that prior approval may be required for international transfers.

6.10 Can the registration/notification be completed online?

Yes. They can be completed at the following address: https://sedeagpd.gob.es/sede-electronica-web/. However, please note that the procedure might not be able to be carried out entirely online.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes. However, not all information is made available to the public. For example, registration codes and security levels are not available publicly.

6.12 How long does a typical registration/notification process take?

One (1) month.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

The Draft LOPD Bill provides an extensive list of when the appointment of a Data Protection Officer is mandatory:

- Professional associations which are regulated by Law 2/1974.
- Educational institutions which are regulated by Law 2/2006.

- Entities which exploit networks and provides electronic communications services when they process large-scale regular and systematic personal data.
- Society information service providers when they create large-scale profiles of users of the service.
- Entities covered by Law 10/2014 (credit entities).
- Financial establishments which are regulated by Law 5/2015.
- Insurance entities which are regulated by Law 20/2015.
- Investment services companies which are regulated by Royal Decree 4/2015.
- Electric energy distributors and suppliers as well as natural gas distributors and suppliers.
- Entities who are in charge of general files for assessing financial solvency and creditworthiness or general files for managing and preventing fraud, including controllers which are regulated by Law 10/2010.
- Entities engaged in advertising activities and commercial research, including commercial and market research, when they carry out processing activities based on preferences of data subjects or when they carry out processing activities which involve profiling of the data subjects.
- Health centres which are legally required to keep medical records of patients in accordance with Law 41/2002.
- Entities whose purposes include the issuance of commercial reports which could mention natural persons.
- Gaming operators whose activity is carried out electronically, telematically and interactively in accordance with Law 3/2011.
- Those who carry out activities which are regulated by Law 5/2014 (private security).

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

Failure to comply with the requirement to designate a Data Protection Officer (when mandatory to do so) is considered a serious infringement under the Draft LOPD Bill.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing his or her tasks and should report directly to the highest management level of the controller or processor.

The Draft LOPD Bill specifies that the appointed Data Protection Officer cannot be dismissed or penalised for performing his tasks except in cases of intent or gross negligence.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer. More specifically, the Draft LOPD Bill indicates that controllers and processors shall notify designations and dismissals of Data Protection Officers within ten (10) days. This applies when the designation of a Data Protection Officer is mandatory as well as when the entity chooses to appoint one voluntarily.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the WP29 recommends that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

The Spanish DPA has published Guidelines for the Preparation of Contracts between controllers and processors available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/EN_directricescontratos.pdf (English version).

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Unsolicited Email, SMS, and Other Electronic Means

General opt-in rule: Unsolicited emailing requires previous opting in from the data subject.

Exceptional opt-out rule: Customers can be sent unsolicited emails, provided such unsolicited emailing is advertising similar goods and services to those previously purchased by such customers.

Single click unsubscribe: Such an option at the end of every post is mandatory.

The Robinson List: Must be checked before sending electronic communications.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Regular Post

Unsolicited marketing communications can only be sent in written paper format by regular post to individuals whose contact details are displayed in telephone directories or are obtained from other public sources.

Phone Call

The Spanish Consumer Rights Act *Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias* bans "robot" telemarketing phone calls. Unsolicited telemarketing calls must be performed by human agents, and shall always show the phone number of the calling party. People in the Robinson List should never be contacted.

Art. 29 of the Spanish Unfair Competition Act *Ley 3/1991, de 10 de enero, de Competencia Desleal* considers it an aggressive practice to carry out persistent unsolicited phone calls, emails or any other electronic means, unless this is deemed necessary and justifiable in order to seek fulfilment of legal obligations.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they do.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, they are.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Due regard shall be paid to the legal basis of the processing and the duty of information (Art. 13 of the GDPR and Art. 14 of the GDPR). Further, the purchaser must be able to demonstrate that it complies with the GDPR and, specifically, that the use of a purchased marketing list complies with any of the legitimate basis of processing as established by Art. 6 of the GDPR. The general rules on sending marketing communications apply.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Sending marketing communications in breach of the LSSI shall be fined up to EUR 150,000. However, if doing so involved an infringement of the LOPD at the same time, then an additional fine of up to EUR 300,000 shall be imposed.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The LSSI implements Art. 5 of the ePrivacy Directive. Pursuant to Art. 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request. The Spanish DPA has published a Guide on Cookies available in Spanish.

10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

See the previous answer.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes. It is noteworthy to mention that a fine was imposed in 2017 for using the Mailchimp Service in breach of Art. 22.2 of the LSSI.

For other sanction resolutions, please visit the Spanish DPA's website: http://www.agpd.es/portalwebAGPD/canaldocumentacion/cookies/index-ides-idphp.php.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Failure to provide proper cookie information might attract fines of up to EUR 30,000. If this action is repeated within three years after the first final decision of the Spanish DPA, this might attract fines from EUR 30,000 to EUR 150,000.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the "**EEA**") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or BCRs.

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of Binding Corporate Rules ("**BCRs**"). The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses on in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.

The Article 29 Working Party (the "**WP29**") has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. The WP29 recommends that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, the WP29 considers that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

Traditionally, Spain prohibited anonymous reporting (see the Spanish DPA's legal report 2007-0128). However, the Draft LOPD Bill opens the door to anonymous reporting.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

According to the LOPD, prior notification is needed as for any other type of personal data processing. Further, controllers must place a sign which is sufficiently visible, and documents which comply with the duty to inform must be made available to data subjects.

Under the GDPR, a data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

The Draft LOPD Bill follows essentially what has been outlined under the current LOPD.

13.2 Are there limits on the purposes for which CCTV data may be used?

A guide on video surveillance is set to be published by the Spanish DPA once the GDPR and the new LOPD become applicable.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Monitoring must be lawful, transparent, proportionate and legitimate and there should not be other less intrusive means to reach equivalent goals. Prominent video surveillance signs are always a must.

In 2017, the WP29 updated its opinion on data processing at work (Opinion 2/2017).

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent of employees is not needed, since notice is required since control measures on employees are permitted by law (Art. 20.3 of *Estatuto de los trabajadores*), provided that such control measures comply with the above-mentioned principles. The Draft LOPD Bill adds that failure to provide the required information will not deprive the images of their probative value where the images have captured the flagrant commission of a criminal act. However, this is without prejudice to the liabilities that may arise from such failure.

The issue of notice in the context of covert video surveillance of employees has been the subject of a recent case of the ECHR (*López Ribalda v. Spain*).

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The Company's Workers' Committee (*comités de empresa*) must be informed of the existence of CCTV, according to Art. 64.2 of *Estatuto de los trabajadores*.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisation measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of EUR 20 million or 4% of worldwide turnover.

Further, failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk as is required by Art. 32.1 of the GDPR is considered a serious infringement under the Draft LOPD Bill.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigative Powers	The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment.	N/A
Corrective Powers	The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).	N/A
Authorisation and Advisory Powers	The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.	N/A
Imposition of administrative fines for infringements of specified GDPR provisions	The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year.	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Non-compliance with a data protection authority	The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year, whichever is higher.	N/A

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The Spanish DPA makes all its decisions available to the public. Therefore, there are countless enforcement examples available on the Spanish DPA's website.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes. Just recently the Spanish DPA imposed fines on Facebook, Inc. and Whatsapp, Inc. (see Resolution R/00259/2018). The preliminary questions revolved around the applicable law. The Spanish DPA concluded that:

- Facebook Spain, S.L. was an establishment of Facebook Inc.: Spanish Law is applicable when the data are processed in the context of activities conducted at the controller's establishment, provided such establishment is located on Spanish soil (see Art. 2.1.a) of the current LOPD).
- Facebook, Inc. processed data with hardware located on Spanish soil which was not employed for transit only: Spanish Law is applicable when the controller is not established in the European Union and processes the data with hardware located on Spanish soil, unless such hardware is employed for transit only (see Art. 2.1.c) of the current LOPD).
- Whatsapp, Inc. did not have an establishment in Spain nor in any other country of the EEA when it published its update of the Terms of Service and Privacy Policy. Nevertheless, it was using hardware located on Spanish soil which was not employed for transit only (see Art. 2.1.c) of the current LOPD).

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses will typically analyse the request on a case-by-case basis and take into account data protection, labour, criminal, and other relevant laws. They will check, among others, if the request is correctly made, if it complies with the legal formalities between the countries, the scope of the request, the legal basis for the disclosure, and any international data transfer issues.

17.2 What guidance has/have the data protection authority(ies) issued?

No clear guidance is in place besides international conventions ratified by Spanish regulatory bodies, such as the USA FTC Memorandum of Understanding and equivalent documents. However, the WP29's Working Document 1/2009 on pre-trial discovery for cross-border civil litigation might provide some guidance. Further, the Spanish DPA analysed the issue in 2011 and published a legal report which is available on its website.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Sanction procedure resolutions of the Spanish DPA have dealt mostly with the following:

- Art. 4.3 of the LOPD – Quality of data.
- Art. 6.1 of the LOPD – Data subject consent.
- Art. 21 of the LOPD – Prohibition of commercial communications sent by electronic means without previous data subject consent.

Also noteworthy is that the Spanish DPA has imposed fines on Facebook, Whatsapp, and Google in the last 12 months.

18.2 What "hot topics" are currently a focus for the data protection regulator?

The GDPR and the Draft LOPD Bill are the two main "hot topics".

Carlos Pérez Sanz
Ecija Abogados
Av. Diagonal, 458
8th floor
08006 Barcelona
Spain

Tel: +34 933 808 255
Email: cperez@ecija.com
URL: ecija.com

Partner and Head of Information Technology at ECIJA

With a professional background of more than 20 years in advising leading Spanish and International companies on matters related to information technology, telecommunications, intellectual property, privacy law and compliance regulations, Carlos Pérez Sanz developed most of his career in Landwell – PwC Tax & Legal Services, which he joined in 1998. In PwC, he has been a partner and the Head of the Information Technology Department of the firm in Spain. Carlos Pérez Sanz holds an LL.B. from Universidad de Barcelona, an M.B.A. from ESADE in Barcelona, and is an associated professor at the same university for its Intellectual Property and Information Society Master's programme. In addition, he holds the International CISA Certification as a qualified information technology systems' auditor by ISACA (Information Systems Audit and Control Association).

Carlos Pérez Sanz has played an active role during his professional career in the elaboration process of numerous regulations related to new technology law; in particular, related to the Spanish Data Protection Act, Intellectual Property Act and Information Society Act.

He has been selected as one of the best lawyers in information technology and data protection law in Spain by the prestigious international rankings *The Legal 500* and *Best Lawyers International*.

Pia Lestrade Dahms
Ecija Abogados
Av. Diagonal, 458
8th floor
08006 Barcelona
Spain

Tel: +34 933 808 255
Email: plestrade@ecijalegal.com
URL: ecija.com

Information Technology at ECIJA

Pia Lestrade Dahms is a member of the Florida Bar in the United States. She holds a B.A. in Political Science from the University of Connecticut, a J.D. from St Thomas University, and a Master's in Intellectual Property and Information Society from ESADE. She has volunteered at technology-related conferences organised by the French Member of Parliament who represented French citizens living in North America. Further, she also volunteered at the first edition of the Startup Europe Awards by providing analysis on the French startup landscape. She is a member of the International Association of Privacy Professionals and speaks English, French, Spanish and Catalan.

ECIJA

ECIJA is among the Top 10 best law firms in the Spanish market (*Chambers Europe* and *The Legal 500 2017*) which received the 2017 Expansión Awards for most innovative law firm, and best information technology, intellectual property, and data protection law firm. It also received that same year the Forbes Awards for law firm of the year for the aforementioned fields from Forbes.

Established in 1997 with a focus on TMT and IP, the firm has grown since then to become a full-service firm with presence in all areas of law and in every sector. ECIJA comprises a team of first-class lawyers with outstanding experience and is broadly international in scope. It is lauded for service, quality and client satisfaction.

While ECIJA is a full-service firm and provides a range of legal services, we offer distinctive specialisation in some areas linked to the most developed sectors of industry: ECIJA is the Spanish reference in technology, media, and telecommunications law.

The firm has offices in Madrid, Barcelona, Valencia, Lisboa, Miami, and Santiago de Chile, and collaborates in any other worldwide jurisdictions as the sole Spanish member of MERITAS, the largest worldwide lawyers' network, with more than 7,000 lawyers in over 70 countries around the world.

For further information, please visit www.ecija.com.