ICLG

The International Comparative Legal Guide to:

Data Protection 2016

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
April 2016

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Spain

Carlos Pérez Sanz

ECIJA ABOGADOS

Lorena Gallego-Nicasio Peláez

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The main legislation specific to data protection is the Spanish Data Protection Act 15/1999 (hereinafter, *Ley Orgánica de Protección de Datos, 15/1999* or LOPD).

Royal Decree 1720/2007 (hereinafter, RLOPD) is ancillary to the LOPD and sets out security measures for personal data and further regulation.

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

Organic Law 1/1982 deals with civil torts arising from violation of honour rights.

Gross privacy non-disclosure violations might be prosecuted under criminal charges, following Art. 197 of the Criminal Code.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (hereinafter, LSSI) covers the e-marketing communications regime, the internet service provider (ISP) liability and anti-spam regulation. For further information regarding marketing restrictions, please refer to section 7.

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

A large number of sector specific legislation is available. These are a few examples:

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 (hereinafter, 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* contains data protection provisions specific to the insurance industry.

d) Legislation specific to healthcare service provision sheds light on rights to access to 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 electronica* covers data privacy issues related to electronic signature.

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

g) Art. 6.2.b of *Ley 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos* provides citizens' right to get in touch with the public administration by electronic means. The public administration must ensure security measures when handling a citizen's data in that connection.

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 is the relevant data protection regulatory authority(ies)?

Agencia Española de Protección de Datos (AEPD) monitors privacy violations carried out by individuals, companies and the government. Thus, the AEPD is in charge of prosecuting and enforcing sanctions arising from the LOPD and the LSSI. Catalonia

and the Basque country have appointed regional data protection authorities surveilling government legal entities within the territory of such autonomous communities.

2 Definitions

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

- **"Personal Data"**

  LOPD Art. 3.a: Any information concerning identified or identifiable natural persons.

  RLOPD Art. 5.1.f: Any alphanumeric, graphic, photographic, acoustic or any other type of information pertaining to identified or identifiable natural persons.

- **"Sensitive Personal Data"**

  Data concerning ideology, trade union membership, religion, beliefs, ethnic origin, health status and sex life. Please consult LOPD Art. 7 for further details.

- **"Processing"**

  RLOPD Art. 5.1.t: Any operation or technical process, whether automated or not, that allows the collection, recording, storage, creation, amendment, consultation, use, rectification, erasure, blocking or deletion, as well as the disclosure of data arising from communications, consultations, interconnections and transfers.

- **"Data Controller"**

  RLOPD Art. 5.1.q: A natural person or legal entity, public or private, or administrative body, that alone or jointly with others decides on the purpose, content and use of the processing, although he does not effectively do it.

- **"Data Processor"**

  RLOPD Art. 5.1.i: The natural person or legal entity, public or private, or administrative body that, alone or jointly with others, processes personal data on behalf of the data controller, due to the existence of legal relations binding them and delimiting the scope of his action for the provision of a service. Entities without legal personality acting as separate parties in the operation may also be data processors.

- **"Data Subject"**

  RLOPD Art. 5.1.a: The natural person to whom the data undergoing processing pertains.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Pseudonymous Data"**

    There is no such definition in Spain.
  - **"Direct Personal Data"**

    There is no such definition in Spain.
  - **"Indirect Personal Data"**

    There is no such definition in Spain. Instead, there is only "Identifiable Personal Data".

3 Key Principles

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

- **Transparency**

  Autodeterminación informativa involves:
  - Information right: The data subject must be informed about the identity of the controller, purpose of collecting and valid address for exercising the rights of access, opposition, rectification and erasure.
  - Consent: Data subjects' consent is needed for processing data and for transmission to third-party controllers.
  - Exercise of rights: The data subject might at all times be able to exercise its rights of access, opposition, rectification and erasure.
- **Lawful basis for processing**

  LOPD Art. 4: Personal data may be collected for processing, and undergo such processing, only if they are adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained.

  RLOPD Art. 8.1: Personal data must be processed fairly and lawfully. The collection of data by fraudulent, unfair or illicit means is hereby prohibited. Personal data may only be collected for specified, explicit and legitimate purposes of the data controller.
- **Purpose limitation**

  LOPD Art. 4: Personal data may be collected for processing, and undergo such processing, only if they are adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained.

  RLOPD Art. 8.1: Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected.
- **Data minimisation**

  Data controllers shall only process the necessary inputs in order to serve legitimate goals and purposes. Controllers should at all times consider less intrusive processing alternatives, and collect only indispensable data. Obsolete data should be erased as soon as possible unless specific laws mandate otherwise. (Please refer to LOPD Art. 4 for further details.)

  RLOPD Art. 8.4: Personal data may only be processed if they are adequate, relevant and not excessive in relation to the specific, explicit and legitimate purposes for which they were obtained.
- **Proportionality**

  This is basically the same as data minimisation. The controller should at all times consider less intrusive processing alternatives, and collect only indispensable data. (Please refer to LOPD Art. 4 for further details.)

  RLOPD Art. 8.4: Personal data may only be processed if they are adequate, relevant and not excessive in relation to the specific, explicit and legitimate purposes for which they were obtained.
- **Retention**

  RLOPD Art. 5.1.b – Erasure: Procedure through which the data controller stops using data. Erasure shall imply data being blocked, comprising their identification and **retention** in order to prevent processing with the exception of being at the disposal of public administrations, judges and courts for the purpose of determining any liability arising from processing, and only for the duration of such liability. On the expiry of such a term, the data shall be deleted.
- *Other key principles – please specify*
  - **Security**

    Controllers and processors must abide by the security measures set forth in Royal Decree 1720/2007. There are three degrees of protection: basic; medium; and high level security measures (see question 13.1).

LOPD Art. 9 – Data security:

1. The controller or, where applicable, the processor, shall adopt the technical and organisational measures necessary to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access, having regard to the state of the article, the nature of the data stored and the risks to which they are exposed by virtue of human action or the physical or natural environment.
2. No personal data shall be recorded in files which do not meet the conditions laid down by rules regarding their integrity and security, as well as the rules governing the processing centres, premises, equipment, systems and programmes.
3. Rules shall be laid down governing the requirements and conditions to be met by the files and the persons involved in the data processing referred to in LOPD Art. 7.

- **Publicity**

  Data controllers must notify files before the Spanish Data Protection Authority. Registry is open for public consultation.

  LOPD Art. 14 – Right to consult the General Data Protection Register: Anyone may consult the General Data Protection Register to learn about the existence of personal data, their purpose and the identity of the controller. The General Data Protection Register shall be open to the public consultation free of charge.

- **Secrecy**

  LOPD Art. 10 – Duty of secrecy: The controller and any persons involved in any stage of processing personal data shall be subject to professional secrecy as regards such data and to the duty to keep them. These obligations shall continue even after the end of the relations with the owner of the file or, where applicable, the person responsible for it.

- **Data with special protection**

  LOPD Art. 7.1: In accordance with the provisions of Art. 16 (2) of the Spanish Constitution, nobody may be obliged to state his ideology, religion or beliefs. If, in relation to such data, the consent referred to in the following paragraph is sought, the data subject shall be warned of his right to refuse such consent. Personal data which reveal the ideology, trade union membership, religion and beliefs may be processed only with the explicit and written consent of the data subject.

- **Transfer and access to data by third parties**

  As a general rule, access to data by third parties requires the data subject's consent (see LOPD Art. 11). Access to data by data processors is subject to specific requirements (see LOPD Arts. 11 and 12).

4 Individual Rights

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

- **Access to data**

  LOPD Art. 15: The data subject shall have the right to request and obtain, free of charge, information on his personal data subjected to processing, on the origin of such data and on their communication or intended communication. The information may be obtained by simply displaying the data for consultation or by indicating the data subjected to processing in writing, or in a copy, fax or photocopy, whether certified a true copy or not, in legible and intelligible form, and without using keys or codes which require the use of specific devices.

- **Correction and deletion**

  LOPD Art. 16: The controller shall be obliged to implement the right of rectification or cancellation of the data subject within a period of 10 days. Rectification or cancellation shall apply to data whose processing is not in accordance with the provisions of this Law and, in particular, when such data are incorrect or incomplete. Cancellation shall lead to the data being blocked and maintained solely at the disposal of the public administrations, judges and courts, for the purpose of determining any liability arising from the processing, and for the duration of such liability. On expiry of such liability, they shall be deleted.

- **Objection to processing**

  RLOPD Art. 34: The right to object is the right of the data subject. This right ensures that the processing of his personal data cannot be carried out, or cannot cease, in the following situations:

  a) When his consent to the processing is not necessary, as a result of a legitimate and grounded reason, referring to his specific personal situation which justifies it, unless otherwise provided by law.

  b) When the purpose of the relevant files is to carry out advertising and commercial research activities, under the terms provided in Art. 51 hereof, whatever the company responsible for its creation.

  c) When the purpose of the processing is to make a decision regarding the data subject and is solely based on the automated processing of his personal data, under the terms provided in RLOPD Art. 36.

- **Objection to marketing**

  Please refer to section 7.

- **Complaint to relevant data protection authority(ies)**

  In the case of unsuccessful attempts to exercise the rights of access, rectification, opposition or erasure, data subjects can seek enforcement before the regulatory authority.

- *Other key rights – please specify*

  - **Information and consent rights**

    The data subject must be informed about the identity of the controller, purpose of collection and valid address for exercising the rights of access, opposition, rectification and erasure. Such a principle also includes the obligation to obtain consent for the processing of data and for the transfer of data to third parties (although there are exceptions to such an obligation of consent). Finally, this principle also includes the rights granted to any data subject to access, correct, supress and oppose to the treatment of personal data, which are further explained below. For further details, please refer to LOPD Arts. 5–7.

  - **Profile impugnation (*derecho de impugnación de valoraciones*)**

    LOPD Art. 15.3 and RLOPD Art. 36 provide that data subjects are entitled to challenge wrong or inaccurate profiling (data mining) adversely affecting them.

  - **Right to be indemnified**

    In cases where a controller commits a breach of data protection legislation causing damage to a data subject, the latter can seek indemnification on the grounds of LOPD Art. 19.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

The general obligation is that files must be registered before the DPA prior to processing. In addition, there are specific notification obligations related to international data transfers (some of them are subject to authorisation from the DPA).

5.2 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 processing category.

5.3 Who must register with/notify the relevant data protection authority(ies)? (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.

5.4 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:

- data controller name, address and contact details;
- file name;
- purpose of processing;
- categories of data under processing;
- source/origin of data;
- security level (basic, medium, and high);
- processing methods;
- transfer of data to third parties;
- relevant data processors;
- international transfers; and
- valid address for exercising rights of access, opposition, rectification and erasure.

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

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

5.6 What is the fee per registration (if applicable)?

There is no fee.

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

Any changes of categories listed in question 5.4 must be notified. It must also be notified when data processing stops taking place (is discontinued) or when data processing is transferred to a new data controller.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

Prior approval is only necessary for certain international transfers (this is covered under section 8).

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

For data processing registrations, the maximum term established by the law is one month. This means that if, within such a one-month term, the DPA has not otherwise replied, the registration request is deemed to be granted. For international transfers, the maximum period for issuing and notifying the decision shall be three months, starting from the date of entry in the Spanish Data Protection Agency of the request. If within this three-month period a decision has not been issued and notified, the international transfer of data shall be deemed to be authorised.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a Data Protection Officer is optional, but there is an obligation to appoint a Data Security Officer when a data controller is handling processings which are subject to medium and high level security. Such a Data Security Officer is only responsible for ensuring compliance with compulsory security measures but has no responsibility for compliance with any other obligations arising from the law.

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

This is not applicable in Spain, but failure to appoint a Data Security Officer when compulsory is considered a major infringement punishable by a fine of between EUR 40,001 and EUR 300,000.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

A voluntarily appointed Data Protection Officer could ensure compliance with all obligations arising from the law, not only with compulsory security measures.

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

There are no specific requirements for a Data Protection Officer nor for a Data Security Officer.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

This is not applicable in Spain.

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

Neither an appointment of a Data Protection Officer, nor an appointment of a Data Security Officer, must be notified.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

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 "Robinson lists" 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.

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 sign-off at the end of every post is mandatory.

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

Yes, they are.

7.3 Are companies required to screen against any "do not contact" list or registry?

Yes. The so-called "Robinson list" (see question 7.1) is an opt-out list where people who do not wish to receive marketing communications are registered.

7.4 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.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

Implied consent (not explicit opt-in consent) is accepted for all kinds of cookies. Please refer to question 7.6.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

For all types of cookies, a prominent scroll or banner should be placed when entering a website. Implied cookie consent is thus obtained as the user remains on the website and keeps exploring it. From this point onwards, further layered and prominent cookie information must be provided, in order that the user is enabled to read a detailed cookie policy fully if the user wishes to do so, before granting implied consent (i.e. before continuing his/her navigation through the website). The DPA in Spain has set up clear criteria so that no cookie is installed at a user terminal before a user has granted implied consent. For further details, please refer to the AEPD *Guía de cookies*.

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

Yes. There has recently been the first fine (R/02990/2013). For other sanction resolutions, please visit Spanish Data Protection website (http://www.agpd.es/portalwebAGPD/index-ides-idphp.php).

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

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

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

Transfer of data to outside the European Economic Area, and to those countries which have not been declared as offering equivalent protection or are included under the Safe Harbour agreement, must undergo prior approval from the DPA. Notwithstanding the foregoing, transfers to such countries are expressly allowed by the law in the following extraordinary circumstances:

a) The international transfer of personal data is the result of applying treaties or agreements to which Spain is a party.

b) The transfer serves the purposes of offering or requesting international judicial aid.

c) The transfer is necessary for medical prevention or diagnosis, the provision of health aid or medical treatment, or the management of health services.

d) Where the transfer of data is related to money transfers in accordance with the relevant legislation.

e) The data subject has given his unambiguous consent to the proposed transfer.

f) The transfer is necessary for the performance of a contract between the data subject and the controller or the adoption of precontractual measures taken at the data subject's request.

g) The transfer is necessary for the conclusion or performance of a contract concluded, or to be concluded, in the interest of the data subject, between the controller and a third party.

h) The transfer is necessary or legally required to safeguard a public interest. A transfer requested by a tax or customs authority for the performance of its task shall be considered as meeting this condition.

i) The transfer is necessary for the recognition, exercise or defence of a right in legal proceedings.

j) The transfer takes place at the request of a person with a legitimate interest, from a public register, and the request complies with the purpose of the register.

k) The transfer takes place to a Member State of the European Union or to a country which the Commission of the European Communities, in the exercise of its powers, has declared to ensure an adequate level of protection.

Summarising: Transfers within the EEA, equivalent-protection countries are not restricted, and there is only an obligation to notify such transfers to the DPA. Transfers of data to third countries which fall within any of the categories of authorised transfers described above (letters a) to k) of the previous paragraph) are authorised by law and only subject to notification to the DPA. All other international transfers to third countries are subject to prior authorisation.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

- EU Model clauses (controller-to-controller, and controller-to-processor clauses).
- Ordinary data processor clauses are used for international transfers within the EEA, or equivalent protection countries.

There are no Spanish multinational companies that have approved the BCR although some of them have initiated the process for creating them.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Please see the answers to questions 8.1 and 5.9. For further details and timeframes, refer to RLOPD Arts. 137–140.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

Only substantial breach of laws or severe violations of codes of conduct are eligible. Minor violations are not eligible for whistle-blowing. There are no pieces of legislation specific to whistle-blower hotlines. Case law such as the Spanish DPA legal report 2007-0128 mandates performing case-by-case balancing-tests so as to evaluate the legitimacy of topics eligible for the whistle-blowing hotline. The Spanish DPA legal report 2007-0128 refers to a company where vague and unspecific violations of statutory provisions, laws or internal regulations or codes of practice were targeted for whistle-blowing, and this was deemed too broad and blurred as a definition. Therefore, further clarification is needed.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous reporting is strictly prohibited. See the Spanish DPA legal report 2007-0128.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

No, this is not the case in Spain.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

No, this is not the case in Spain.

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

The obligation is to inform all members of a company (especially all employees) about the existence and use of a whistle-blowing system, and that their data might be processed.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Prior notification is needed, as for any other type of personal data processing.

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

Monitoring must be lawful, transparent, proportionate and legitimate and any more intrusive means to reach equivalent goals should not exist. Prominent video vigilance signals are always a must.

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

Notice is always required. Consent of employees is not needed, 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 (transparency, proportionality, legitimacy, and not being intrusive where possible).

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

Employees boards at companies (*comités de empresa*) must be informed of the existence of CCTV, according to Art. 64.2 of *Estatuto de los trabajadores*.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No. Nevertheless, please bear in mind that CCTV, in addition to the above-mentioned articles on labour legislation, must always comply with *Instrucción 1/2006* of the AEPD.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There is no specific regulation for data processing in the cloud; however, the latter must comply with applicable rules for international data transfers and common obligations established for data processors.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

If a data processor (cloud provider) processes data within the EEA, equivalent protection jurisdictions or Safe Harbour framework, then general contractual conditions for data processors as established in LOPD Art. 12 and RLOPD Arts. 20–22 would suffice. If a data processor processes data in third countries, all obligations described in previous questions of this questionnaire for international transfer of data and access to data by the data processors shall apply (mainly use of model EU clauses for controller-processor or approval of the BCR).

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific obligations on big data. It is therefore permitted, provided that it complies with all obligations in data protection legislation, especially obligations related to purpose limitation, information, consent, transfer to third parties, international data transfers, contractual obligations to data processors and security measures.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Royal Decree 1720/2007 provides three security levels:

AUTOMATISED PROCESSING SECURITY MEASURES

Nivel alto **(high level)** (this level deals with health records, sexual life, ideology, and work union membership information):

- Communication encryption.
- Support encryption.
- Full access logging.
- Strict physical access control: premises where computers used for data treatment are located must be subject to strict physical boundaries and control checks.
- Basic and medium security measures.

Nivel medio **(medium level)** (this level applies to administrative infractions and personality profiling):

- Data Security Officer appointment.
- Biennial audit.
- Basic security measures.

Nivel básico **(basic level)** (this level applies to remaining kinds of personal data):

- Security Document and fully updated policies and procedures.
- Incident record management.
- Identification and authentication: minimum yearly mandatory password change; encrypted password storage; and mandatory password change upon first login.
- Asset access control: least privileged tenet.
- Support management systems.
- Weekly backup.
- Security training to personnel.

NON-AUTOMATISED PROCESSING SECURITY MEASURES

***Nivel alto* (high level)** (this level deals with health records, sexual life, ideology, and work union membership information):

- Strict control of physical access to rooms.
- Basic and medium security measures.
- Access registry.

***Nivel medio* (medium level)** (this level applies to administrative infractions and personality profiling):

- Data Security Officer appointment.
- Biennial audit.
- Basic security measures.

***Nivel básico* (basic level)** (this level applies to remaining kinds of personal data):

- Key-locked cupboards.
- Security Document and fully updated policies and procedures.
- Filing criteria.
- Security training for personnel.

13.2 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) expects voluntary breach reporting.

There is no such legal requirement in Spain.

13.3 Is there a legal requirement to report data breaches to individuals? 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) expects voluntary breach reporting.

There is no such legal requirement in the Spanish Data Protection legislation. However, there does exist such a requirement in Art. 34.4 of the Spanish Telecoms Act *Ley 9/2014, de mayo, General de Telecomunicaciones*, which establishes the obligation to report or notify data breaches to the Spanish Data Protection Authority; and, if such a breach violates the right of privacy of individuals, it should also be notified to those individuals.

13.4 What are the maximum penalties for security breaches?

The maximum penalty for security breaches is up to EUR 300,001.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Agencia Española de Protección de Datos.	Administrative fines: EUR 900 to EUR 600,000.	Not allowed to impose criminal sanctions.
Agència Catalana de Protecció de Dades (rules over public administration, regional government, town councils and other administrations within the region of Catalonia, companies owned by all such administrations and the providers of thereof).	Administrative fines: EUR 900 to EUR 600,000.	Not allowed to impose criminal sanctions.
Datuak Babesteko Euskal Bulegoa/ Agencia Vasca de Protección de Datos (rules over public administration, regional government, town councils and other administrations within the region of the Basque country, companies owned by all such administrations and the providers of thereof).	Administrative fines: EUR 900 to EUR 600,000.	Not allowed to impose criminal sanctions.
Criminal courts (if infringement qualifies to criminal offence).	-	Prison sentence lasting from one to four years. Fines from EUR 720 to EUR 288,000 if infringer is an individual. Fines from EUR 10,800 to EUR 3.6m if infringer is a company or institution. Criminal fines to be imposed in addition to administrative fines.

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

The AEPD makes all its decisions available to the public. Therefore, there are countless enforcement examples available on the AEPD website.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

These requests abide by the same rules that govern international data transfers. Therefore, if an international data transfer is serving international judicial aid to foreign law enforcement agencies (LOPD Art. 34.b), or the international transfer is necessary or legally required to safeguard a public interest (LOPD Art. 34.h), then it is allowed.

15.2 What guidance has 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.

It is also worth bearing in mind:

- the EU-U.S. PNR agreement; and
- Global Privacy Enforcement Network e-discovery requests.

16 Trends and Developments

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

The most infringed articles in connection with Organic Law 1/1982 and Law of Information Society Services and E-Commerce (LSSI) are:

- LOPD Art. 4.3 – Quality of data: personal data shall be accurate and updated in such a way as to give a true picture of the current situations of the data subject – PS-00440-2014.
- LOPD Art. 6.1 – Related to obtaining data subject consent for the processing of data: processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law – PS-00467-2014.
- LOPD Art. 11.1 – Communication of data: personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of the transfer and transferee with the prior consent of the data subject – PS-00319-2014.
- LSSI 21 – Prohibition of commercial communications sent by electronic means without previous data subject consent: PS-00498-2014.
- LSSI 22.2 – Use of cookies without previous users' consent: PS-00231-2014.

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

The following "hot topics" are currently a focus for the data protection regulator:

- Cookies.
- Big Data.
- Internet of Things (IoT).
- New European Platform Regarding Online Dispute Resolution.

Carlos Pérez Sanz
ECIJA ABOGADOS
Av. Diagonal, 458, planta 8ª
08006 Barcelona
Spain

Tel: +34 933 808 255
Email: cperez@ecijalegal.com
URL: www.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*.

Lorena Gallego-Nicasio Peláez
ECIJA ABOGADOS
Av. Diagonal, 458, planta 8ª
08006 Barcelona
Spain

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

Attorney of Information Technology at ECIJA.

Lorena Gallego-Nicasio Peláez advises national and international clients on new technologies law, with a particular focus on data protection, intellectual property and commercial contracts. She is a member of ICAB (Barcelona Bar Association) and she holds an LL.M. in Practice Law from Universidad de Barcelona. She also holds an LL.B. from Universidad de Barcelona. Additionally, she has attended specialised conferences in intellectual property at prestigious institutions such as ICAB or WIPO and United Nations simulations. Lorena speaks Spanish, Catalan and English.

ECIJA

ECIJA is a "Top 10" law firm in the Spanish market. Founded in 1997 with a focus on TMT and IP, the firm has grown since to accord to the needs of its clients and is now a full-service firm with presence in all areas of law. 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 keeps offices in Madrid, Barcelona and Santiago de Chile, and collaborates in all EU jurisdictions.

Our client base comprises international and domestic companies operating in the main industrial and commercial sectors. The firm's personal loyalty to individual clients is particularly satisfying to its lawyers and is a distinction that has often been noted in the press.

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

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk