Spain

Marc Gallardo
Lexing Spain

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The key piece of Spanish Data Protection legislation is Organic Law 15/1999, of 13 December, on the Protection of Personal Data (LOPD), implements article 18.4 of the Constitution and Directive 95/46/EC and intends to guarantee and protect any personal data processed by public and private entities.

Based on article 18.4 of the Constitution, the Constitutional Court issued a landmark decision in 2002 declaring data protection as a fundamental right that consists in the power granted to data subjects to be in control of their personal data and more specifically how data controllers process and disclose them.

Further, Royal Decree 1720/2007 of 21 December implements the LOPD. The Regulation is meant to satisfy the following purposes:

- to increase the legal certainty;
- to reflect in the legal provisions the consolidated criteria in the implementation of the LOPD, especially in view of case law;
- to respond to the concerns of the European Commission regarding the transposition of Directive 95/46/EC; and
- to incorporate legislative policy criteria and complete the regulatory implementation of the novelties introduced in the LOPD.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Spanish Data Protection Agency (AEPD) is the public law authority overseeing compliance with the legal provisions on the protection of personal data, enjoying as such an absolute independence from the Public Administration. It has jurisdiction over all private entities established in Spain that process personal data.

The AEPD is empowered with broad functions and exercises its powers very intensively to ensure compliance with the legislation on the fundamental right to data protection in Spain. For instance:

- to require information and any assistance to data controllers and data processors it deems necessary for the performance of its tasks;
- to carry out inspections in the premises where any given data processing is taking place (the AEPD officials are considered as public authority);
- to issue instructions needed to bring processing operations into line with the principles of the Law;
- to ensure the respect of the data subject's rights (namely, the rights to access, rectify, erase and object;
- to impose monetary penalties set out in the Law;
- to impose other measures such as the cessation of the processing operation or the erasure of the files in the most severe cases;
- to manage a Register to make known the files in public and private ownership; and
- to monitor and adopt authorisations for international transfers of data.

Moreover, some autonomous communities (for instance, Catalonia and the Basque country) have created their own data protection agency, vesting it with similar powers to AEPD to ensure compliance of the law exclusively by public authorities and entities.

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection principles and guarantees are mostly handled by the AEPD or the autonomous agencies according to the procedure for declaring a breach of the LOPD that is set out in the Royal Decree 1720/2007. Individuals may also present claims for data breaches affecting them before civil courts (that allow claimants to ask for damages) and less likely before criminal courts (reserved for the most severe cases).

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Law mentioned in question 1 is comprehensive, meaning it covers all sectors and types of organisation provided they are established in Spain and process personal data. However, the rules expressly exempt some files or processing. For instance:

- those subject to the legislation on the protection of classified materials; and
- those established for the investigation of terrorism and serious forms of organised crime.

In addition, certain files and processing are governed by specific legislation. This is the case for those:

- regulated by the legislation on the electoral system;
- used solely for statistical purposes and protected by central or regional government legislation on public statistical activities;
- intended for the storage of the data contained in the personal assessment reports covered by the legislation on the personnel regulations of the armed forces;
- contained in the Civil Register and the Central Criminal Register; and
- deriving from images and sound recorded by videocameras for the security forces.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Aside from the LOPD and Royal Decree 1720/2007, there are some specific provisions that cover interception of communications, electronic marketing and video surveillance.

Interception of communications
- Act 9/2014, of 9 May, on Telecommunications. Title III contains the regulation on secrecy of communications and data protection with regard to electronic communications networks and services.
- Royal Decree 424/2005, of 15 April, which approves the regulation on data protection in the provision of publicly electronic communications services.

Electronic marketing
- Act 34/2002, of 11 July, on Information Society Services and Electronic Commerce contains the rule on marketing by e-mail, other equivalent means of electronic communications and the cookie rule (see questions 40 and 41).

Video surveillance
- Act 5/2014, of 4 April, on Private Security.
- Instruction 1/2006, of 8 November, issued by the AEPD, on video surveillance.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Further laws that provide specific data protection rules are:

Health
- Act 41/2002, of 14 December, on the autonomy of the patient and on the rights and obligations in matters of clinical information and documentation.

Consumer Protection
- Act 29/2009, of 30 December, which modifies the unfair competition regime and the advertising for the improvement of consumer protection.
- Act 44/2006, of 29 December, for the improvement of consumer protection.
- Royal Legislative Decree 1/2007, of 16 December, approving the General Law on Consumer Protection and other related laws.

Electronic Signature
- Act 59/2003, of 19 December, on electronic signature.
- Royal Decree 1553/2005, of 23 December, regulating the issuing of the National Security Document and its electronic signature certificates.

Telecommunications
- Act 9/2014, of 9 May, on Telecommunications
- Act 25/2007, of 18 October, on the retention of data generated or processed in connection with the provision of electronic communications services and public communication networks.
- Royal Decree 424/2005, of 15 April, which approves the regulation on data protection in the provision of publicly electronic communications services.

Electronic public administration
- Act 19/2013, of 9 December, on Transparency, Access to Public Information and Good Governance.
- Act 11/2007, of 22 June, on Electronic Access of Citizens to the Public Services.
- Royal Decree 4/2010, of 8 January, which sets the regulation of the National Interoperability Scheme in the Electronic Administration sector.
- Royal Decree 3/2010, of 8 January, which sets the regulation of the National Security Scheme in the Electronic Administration sector.

The LOPD contains specific rules for some data processing, which may be of relevance:
- collection and processing, for police purposes, of personal data by the security forces without the consent of data subjects;
- provision of information services on creditworthiness and credit (see question 11); and
- processing for the purpose of publicity and market research.

7 PII formats

What forms of PII are covered by the law?

The law applies to personal data recorded on a physical support, which makes them capable of processing, and to any type of subsequent use of such data, by the public and private sectors. Personal data is legally defined as 'any information concerning identified or identifiable individuals'. It covers name, surname(s), postal addresses, national and social security numbers, telephone, voice, image, IP addresses and e-mails, among other information that may be associated to a given individual.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

The law governs any processing of personal data carried out by data controllers and data processors that are established in Spanish territory. A controller is any natural or legal entity, whether public or private, that determines purpose, content and use of the processing. A processor is the person that alone or jointly with others processes personal data on behalf of the controller. Both are subject to the penalties set out in the LOPD in case they breach the law when processing personal data in Spain.

The concept 'establishment' refers to any stable premise that allows running activities in an effective manner (for instance, it may be through activities carried out by subsidiaries and branches). It may also apply when the data controller is not established in the EU territory but uses means located in Spain for the data processing, unless such measures are only used for transit purposes. If the data controller is not established in the EU but its data processor is the security measures set out in the Royal Decree 1720/2007 will be fully applicable to the latter.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

The law does not cover all processing or use of personal data. For instance:
- those created or maintained by a natural person in the exercise of purely personal or household activities; or
- those regarding legal entities that only record data of individuals providing services in legal entities, comprising solely their name and surname(s), functions or jobs performed, as well as the postal or e-mail address and professional telephone and fax number. In line with this exemption, data relating to sole traders and professionals are also excluded.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The processing of personal data, including the disclosure of data to third parties, is deemed lawful provided the data controller is able to rely, at least, on one of the following grounds:
- the data controller has obtained consent from the data subject. Consent must be freely given, unambiguous, specific and informed. The request for consent shall refer to specific processing or series of processes, stating the purpose for which they are collected, as well as the other conditions applying to the processing or series of processes. When consent of the data subject is requested for the assignment of his or her data, he or she shall be informed in such a way as to understand unequivocally the purpose for which the relevant data shall be used and the type of activity performed by the recipient. Otherwise, consent shall be null and void;
- it is authorised by a regulation having the force of law or under EU law; and
- the data controller has a legitimate interest in the processing as long as the fundamental rights and liberties of the data subject are not breached.

In some transactions a number of legal grounds could apply at the same time. But, at least, any data processing must at all times be in conformity with one or more legal grounds.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

There are more stringent data protection rules for specific cases:

- Processing data of minors (14 years or less) requires the parent's or guardian's consent. The data controller is responsible for setting up procedures guaranteeing that the age of the minor and the authenticity of the consent given by the parents, guardians or legal representatives have been effectively checked.
- Processing of sensitive data as those revealing the ideology, trade union membership, religion and beliefs may only be processed with the explicit and written consent of the data subject. Moreover, personal data that refer to racial origin, health or sex life may be processed when provided by law or when the data subject has given his explicit consent.
- Processing of personal data regarding financial solvency and creditworthiness is subject to additional requirements such as providing information to the affected data subject prior to and at the moment his or her information is registered and honouring the specific rights of the data subjects to access, rectify and erase. The creditor and the owner of the joint file containing financial solvency and creditworthiness must fulfil these duties according to the requirements set out by the law.

For instance, the creditor shall inform the debtor that should payment not be made, the data relating to this fact shall be disclosed to files relating to the fulfilment or non-fulfilment of pecuniary obligations. The specific requirements to register a debt are: the debt must be due and enforceable regarding which no legal, arbitration or administrative claim has been filed; the debt must be less than six years from its due date; and a prior request for payment shall have been verified. The owner of the joint file is obliged to notify the data subjects for whom personal data has been registered, within 30 days from such registration, a reference of those data that have been included thus informing them of the possibility to exercise their rights of access, rectification, erasure and objection.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

The rules distinguish between data directly collected from the data subject and those collected from other sources.

Data collected directly from the data subject

The rules state that the data controller must inform individuals about the following:

- the existence of a file or personal data processing operation, the purpose of collecting the data, and the recipients of the information;
- the obligatory or voluntary nature of the reply to the questions put to them;
- the consequences of obtaining the data or of refusing to provide them;
- the possibility of exercising rights of access, rectification, erasure and objection; and
- the identity and address of the controller or of his representative, if any.

The information must be provided when the data is directly collected from the data subject or later if gathered from another source. Where questionnaires or other forms are used for collecting data, the notice must contain the above-mentioned information in a clearly legible form.

Data collected from other sources

As a general rule, when the personal data have been collected from other sources, the data subject must be informed explicitly, precisely and unambiguously by the controller within three months from the recording of the data, unless he or she has been informed previously, of the above-mentioned information plus the origin of the data.

If the data come from sources accessible to the public and are intended for advertising activity or market research, where prior consent is not required by law, in each communication sent to the data subject, the data controller must inform about its identity, the origin of the data and the rights of the data subject, especially the right to object.

13 Exemption from notification

When is notice not required?

The duty to inform, as described above, is exempted when data is collected from other sources and any of the following circumstances occur:

- a law expressly exempts the duty to inform individuals;
- the data processing has historic, statistical or scientific purposes; or
- the information is impossible to provide to individuals or would require disproportionate efforts. This must be declared by the AEPD at the data controllers' request according to the procedure set up in the Royal Decree 1720/2007.

Furthermore, the duty to inform can be exempted when the information affects national defence or security and the persecution of criminal offences.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Insofar as data protection is a fundamental right, data subjects must be in control of the data that they hand over to data controllers and specific choice must be given when data controllers would like to use data collected from individuals for purposes other than those covered by the notice.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The law imposes high standards in relation to the fairness, necessity, proportionality and quality of personal data. Thus, personal data may be collected and processed 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. Obtaining consent does not negate the controller's obligations with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data that is excessive in relation to a particular purpose.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

As stated above, the law restricts the amount and type of data that may be processed due to the data quality principle, which requires the data to be necessary for the purposes for which they are collected and further processed. Therefore, data must be erased when it has ceased to be necessary or relevant for the purpose for which it was obtained or recorded.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The finality principle has been adopted in the law, meaning the purpose for which any data is processed needs to be explicit, determinate and lawful. For this reason alone the request for consent, when used as a legal ground, has to refer to specific processing or series of processing.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Any different purpose requires additional information and consent. For instance, if the data controller requests the data subject's consent during the process of drawing up a contract for purposes that have no direct link to the maintenance, course or monitoring of the contractual relationship, he or she must allow the data subject to expressly indicate his or her objection to the processing or data disclosure. In particular, compliance with this duty is met when the data subject ticks a clearly visible box that is not already ticked in the document he or she is given for execution of the contract, or an equivalent procedure is established by which he or she may indicate the objection to the processing.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

The controller or, where applicable, the processor have to 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 art, 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.

Title VIII of Royal Decree 1720/2007 sets out a very detailed list of the security measures to be adopted in the processing of personal data either by controllers and processors established in Spain and regardless of the system they use to process data (automated or not).

There are three levels of security measures: basic, medium and high. The higher the level, the more measures have to be implemented.

All files or processing of personal data are subject to the basic level. From the private sector perspective, there are three types of files or processing that enter into the medium level:

- those relating to financial solvency and creditworthiness;
- those controlled by financial institutions for purposes related to the provision of financial services; and
- those containing a set of personal data that provide a profile of individuals and that permit the evaluation of specific aspects of their identity.

Finally, the high level involves sensitive data such as ideology, trade union membership, religion, beliefs, racial origin, health and sex life. Exceptions may be applicable when processing this type of data for the purpose of fulfilling legal obligations. The measures included in each of the aforesaid levels are the minimum that can be applied. Measures include:

Basic level

- The functions and obligations of staff;
- record of incidents that affect personal data;
- access control:
- managements of supports and documents containing personal data;
- user's identification and authentication to access the information; and
- back up copies and recovery.

Medium level

- Appointment of a security officer;
- audit every two years; and
- more stringent rules on managements of supports and documents containing personal data, identification and authentication, physical access control and record of accidents.

High level

- More stringent rules on management and distribution of supports containing personal data, back up copies and recovery, access record and transfer of data through public or wireless electronic communications networks (which should be encrypted).

All the applicable measures have to be written down in a security document.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

At the moment the duty to notify data breaches to the AEPD or individuals is only compulsory for telecoms operators and electronic communications service providers.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The appointment of a DPO, internal or external, is not mandatory. Only when a file is submitted to the medium or high security level is there an obligation to appoint a person in charge of monitoring the compliance of security measures in a given organisation. It is recommended to appoint such a person even if the processing or data are only subjected to the basic security level. It is also advisable, especially in bigger organisations, to delegate some of the functions entrusted to the person responsible for monitoring the compliance of security measures to other staff.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Controllers and processors are required to create and keep the security document up to date. This document is a common security measure by itself and binding on all staff and employees with access to personal data registered either in an automatised or non-automatised format. It must contain all the security measures according to the security level of the data processed by an organisation.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

Data controllers must notify the data files they own before the AEPD. There are no exemptions. Data processors are excluded from this obligation.

24 Formalities

What are the formalities for registration?

The information that needs to be filed covers the identity of the data controller, what type of data is processed and for what purposes, the source of the data, the identity of the main processor, if any, the security level to which the data file is subjected and possible disclosures and international data transfers. The registered data file must be up to date in case of any later substantial change, including its cancellation, if such is the case.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

Failure to request the entry of a data file in the Register is a minor infringement, punished with a fine from €900 up to €40,000.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The AEPD may refuse to allow an entry to the Register only if the information provided is incomplete or inconsistent.

27 Public access

Is the register publicly available? How can it be accessed?

The Register is publicly and freely available. It can be accessed through the AEPD's website at www.agpd.es.

28 Effect of registration

Does an entry on the register have any specific legal effect?

The purpose of the Register is to facilitate the AEPD's control over the processing of data files notified by controllers while also making it easier for data subjects to exercise their rights.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Access to data by a data processor that is necessary for the provision of a service to the data controller is not considered a data transfer, which essentially means that the data controller does not need the prior and informed consent by the data subject or seek another legal ground. However the requirements to stay in the framework of this controller-processor relationship are quite formal.

In substance, the processing of data on behalf of a data controller must be regulated in a contract that must be in writing, being expressly laid down that the processor will only process the data in accordance with the instructions of the controller, will not apply them for a purpose other than that set out in said contract and will not communicate them to other persons. The possibility to subcontract services by the data processor is allowed if the requirements set out in the Royal Decree 1720/2007 are met.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure of data is subject to the restrictions mentioned in question 10.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

International data transfers, meaning those made outside the European Economic Area (EU countries plus Iceland, Liechtenstein and Norway) require the prior authorisation of the AEPD. The data controller will have to present adequate guarantees to obtain said authorisation either by a contract signed with the recipient or the so-called Binding Corporate Rules if the transfer occurs between companies of the same group.

The prior authorisation is exempted in some cases as stated by the Organic Law 15/999. The most common derogations in practice are:

- the consent of the data subject to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller;
- the transfer takes place to a country that the European Commission, in the exercise of its powers, has declared to ensure an adequate level of protection; and
- a recipient who is established in the US is certified under the safe harbour principles.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

Transfers of personal data contained in a data file must be notified to the AEPD. Only international data transfers are subject to the prior authorisation of the AEPD if no derogation is applicable.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Similar restrictions will apply to international transfers to service providers and onwards transfers. The AEPD has recently published a model of contractual clauses to facilitate the authorisation of international data transfers between data processors and sub-processors that can be downloaded from its website (only a Spanish version is available).

Update and trends

First fines on cookies.
In 2014, the AEPD issued its first fines for infringement of the cookie rule. Google was among the first companies fined (€25,000) due to the fact that Google was not informing customers using its blogger service on how cookies were used and the specific purposes for which personal data was processed. The AEPD has also fined very modestly companies that have failed to comply with the obligation to provide clear and comprehensive information about the cookies they used. There are other minor infringement cases where the AEPD has not fined but issued a warning (without an economic sanction) instead.

Privacy Impact Assessment.
The AEPD has issued a draft privacy impact assessment guide. As well as providing general guidance on privacy impact assessments, the guide sets out a set of basic questions, together with an 'evaluation' tool developed by the AEPD, whereby organisations can verify and find out the legal obligations that must be met in order to implement their intended product or service in compliance with data protection legislation. While this privacy impact assessment is not obligatory in Spain, this type of compliance review could become a legal requirement across the EU, under certain circumstances, if the European Regulation on Data Protection remains as currently drafted. The full guide (only the Spanish version is available) can be downloaded from the AEPD's website.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Data subjects have the right to request and obtain free of charge information on their personal data subjected to processing, on the origin of such data and on their communication or intended communication. The right of access may be exercised only at intervals of not less than 12 months, unless the data subject can prove a legitimate interest in doing so, in which case it may be exercised before then. Access can also be denied if thus provided by law or when this prevents the data controller from disclosing to data subjects the processing of data to which the access refers.

35 Other rights

Do individuals have other substantive rights?

Data subjects have the right to require the correction of inaccurate or incomplete information and the right to require the erasure of data that is inadequate or excessive. Both rights may be denied if thus provided by a law or when this prevents the data controller from disclosing to data subjects the processing of the data to which the access refers. In particular, the right of erasure may also be denied when the data must be retained for the period of time provided in the applicable provisions or, if appropriate, in the contractual relations between the data controller and the data subject that justifies the processing of data. Lastly, the right to object is applicable when consent is not required to lawfully process data.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The law and consequently the AEPD do not award any monetary compensation to data subjects whose rights have been affected by breaches of the law. If data subjects want to claim for damages they have a right of action before the civil courts. However, data subjects have the burden of proof to demonstrate the effective damage caused to them by the breach of the law.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

These rights are enforced by the AEPD. The law sets out a specific procedure for the protection of these rights.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

General prohibitions

- The collection of data by fraudulent, unfair or illicit means.
- Creating files for the sole purpose of storing personal data, which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin or sex life.
- No personal data shall be recorded in files that 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 programs (see question 19).

Exemptions on the consent rule

- Consent for processing data (see question 10) is not required when: data is collected for the functions proper to public administrations within the scope of their powers granted by law; for the purpose of executing a contract or preliminary contract or due to the existence of a business, employment or administrative relationship, to which the data subject is party and are necessary for its maintenance or fulfilment; it is authorised by a regulation having the force of law or under Community Law; and for the protection of an essential interest of the data subject when sensitive data is involved.
- Similarly, consent of the data subject shall not be required for the disclosure of his or her personal data to third parties when it: is due to the free and legitimate acceptance of a legal relationship that necessarily entails the communication of the data for its life, fulfilment and monitoring. In that case, disclosure shall be legitimate to the extent of the purpose justifying it; is destined for the ombudsman, the Office of the public prosecutor, judges and courts; is between public administrations when processing is for historical, statistical or scientific purposes; or data has been collected or drawn up by one public administration to be sent to another or the communication is done in order to exercise identical powers or powers relating to the same matters.
- Should the data controller change as a result of an operation of merger, demerger, global assignment of assets and liabilities, contribution or transfer of business or branch of business activity, or any corporate restructuring operation of a similar nature contemplated by company law, a disclosure of data shall not be deemed to have occurred, without prejudice to compliance by the data controller of the duty to inform.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

The decisions issued by the director of the AEPD may be appealed before the National Court.

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

In May 2012, Spain implemented the 'cookie rule' through amendments to its law on Information Society and Electronic Commerce (34/2002). This new provision is very similar to other EU countries and allows website operators to serve cookies provided individuals have given consent after having been given clear and comprehensive information about the use and purpose of cookies. Exemptions are also foreseen in case of 'technical' and 'strictly necessary' cookies. More recently, the AEPD jointly with the advertisement industry has issued guidance on cookies. According to the guidance, the mere inactivity of the user does not mean he or she consents. However, as a general rule, implied consent would be considered valid if clear and meaningful information about the cookies (type, purpose, etc) is provided. The Spanish guidance itself advises 'there is no general and uniform solution and companies shall assess which solution is more appropriate'. The degree of intrusiveness of the cookies would certainly be an important factor in assessing this solution.

41 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

The 'opt-in' rule, which means the controller has to obtain prior, express and informed consent from recipients to lawfully send commercial communications to them, applies to e-mail marketing as well as fax marketing and robocalls for the same purpose.

In case of e-mail marketing and other equivalent means such SMS or MMS marketing, the 'opt-in rule' is not applicable when there is a prior contractual relation, provided that the provider shall have legally obtained the contact details of the recipient and used them to send commercial communications referring to products or services of its company that are similar to those initially at issue in the contract between provider and customer. At all events, the provider must offer the recipient the opportunity to object, free of charge and in an straightforward manner, to the processing of his or her data for promotional purposes, both at the time the data are collected and on the occasion of each commercial message addressed to the recipient.

Lexing Spain

Marc Gallardo **marc.gallardo@lexing.es**

Ronda General Mitre 164
08006 Barcelona
Spain

Tel: +34 93 476 40 48 / +34 606 86 75 05
Fax: +34 93 476 40 38
www.lexing.es