Hogan Lovells

Data protection compliance in Spain

Mission impossible?

2015

Contents

INTRODUCTION

Spain is well known for having one of the most restrictive data protection regimes in the European Union ("**EU**").

It also counts with some of the highest penalties (fines are up to € 600,000 per infringement), and a data protection authority – the Spanish Data Protection Agency ("**AEPD**") – with a reputation for being one of the fiercest of the EU. Moreover, the penalties envisaged are not only on paper; they are applied on a regular basis by the AEPD. For instance, in the last years, it has imposed **fines of € 450,000, € 900,000 and € 1,400,000**.

The mixture of all the above results in a cocktail that is not easy to swallow for companies operating in Spain. This note aims at helping these companies understand how to meet the Spanish data protection requirements.

With this purpose, the main requirements under the Spanish Data Protection Act 15/1999, of 13 December 1999 ("**DPA**"), and the Regulation 1720/2007, of 21 December 2007 ("**Regulation of the DPA**") are highlighted below.

PERSONAL DATA

Concept of personal data

According to the DPA, personal data is any information relating to an identified or identifiable individual. More specifically, according to the Regulation of the DPA, personal data is any alphanumeric, graphic, photographic, acoustic or any other kind of information relating to an identified or identifiable individual.

An identified individual is one who can be directly identified by the data (e.g. by his/her name, image, etc.). In other words, no other information is necessary to identify the data subject.

An identifiable individual is one who can be identified indirectly, i.e. by reference to an identification number, or to one or more elements specific to his/her physical, physiological, mental, economic, cultural or social identity. However, an individual is not regarded as "identifiable" if such identification requires disproportionate efforts, in terms of time or activities.

The Spanish data protection requirements do not apply to anonymous (*non-identifiable*) data, as it is not regarded as personal data. Anonymous data is that which does not allow the identification of the individual, in any way nor by any person, not even by the person who render the data anonymous. In most cases, anonymous data is nothing more than statistical information.

It shall be noted that personal data refers to the total volume of information held on any individual by a person or entity. It this sense, it would not make a difference if, for example, a division within a company processed only a reference number associated with an individual, if another division of the same company (or, even another company) was able to link such reference number with any other information about the data subject at hand, making his/her identification possible. In a case as such, the reference number would be regarded as data.

In short, personal data means:

- information which relates to a living individual; and
- from which he/she can be identified, whether or not in conjunction with any other information; provided that,
- the process of identifying the individual does not require disproportionate efforts.

It is worth pointing out that the AEPD tends to apply the concept of personal data very broadly. There are many cases where the AEPD has considered that certain information was personal data, even if it was hardly possible to link it with an individual.

In the next section, we provide some examples of information that may be considered personal data.

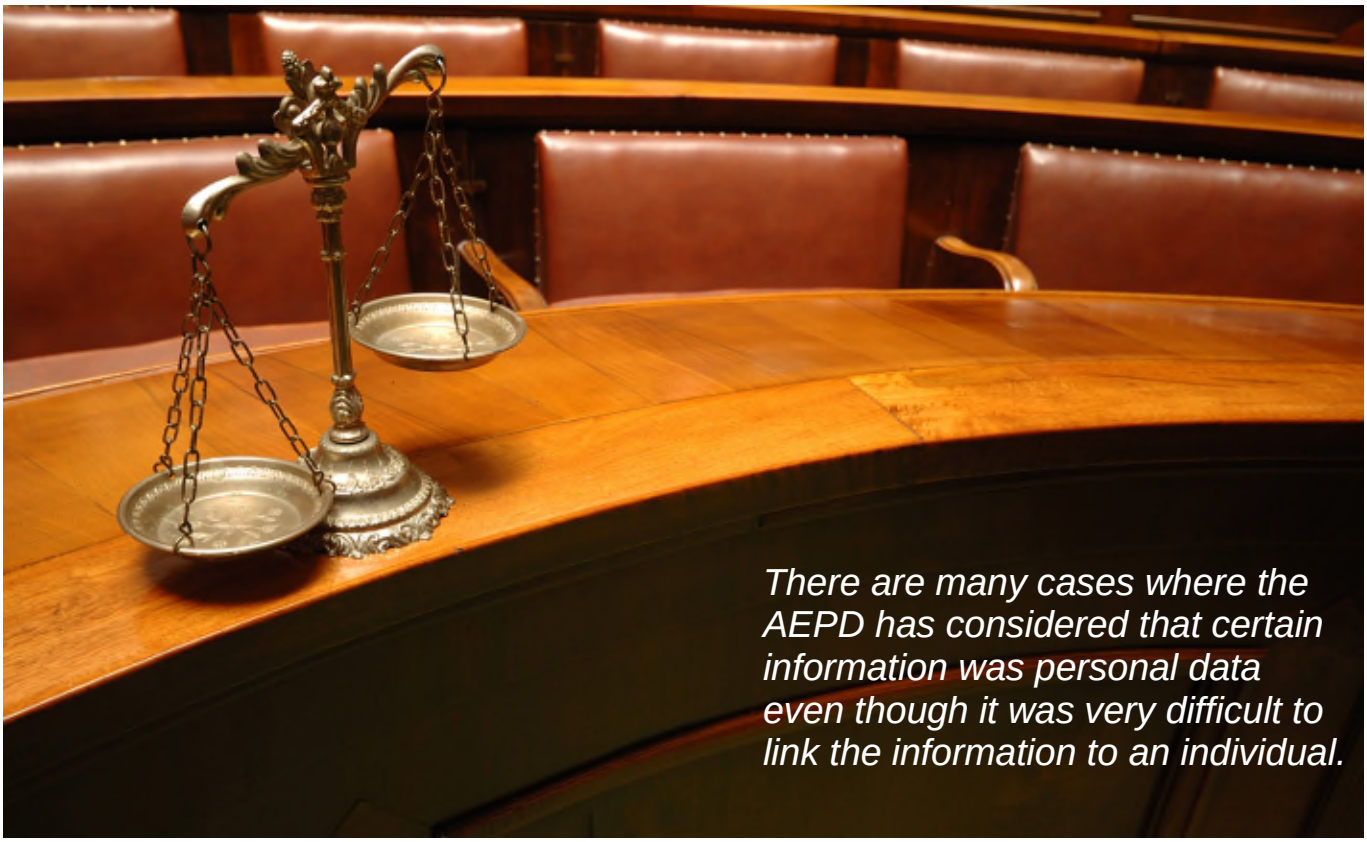
Examples of personal data

Common examples of personal data which may be used by companies on day-to-day business activities include: name and surname; addresses; telephone numbers and other contact details; birth dates; CVs; performance reviews; salaries; statements of opinion or intention about individuals; credit cards; bank accounts; ID cards / passport numbers; pictures / video; fingerprints / voice recordings; health data (e.g. maternity leave); and trade union membership.

However, the existence of personal data is not always so obvious. The following are examples of information that processed on its own (i.e. without any link with other information on the data subject), was regarded as personal data by the AEPD:

- **E-mail addresses:**

  According to the AEPD, e-mail addresses are personal data, even when they do not include information relating to an individual (i.e., name,



company, country, etc.), as the provider of the e-mail service may still identify the individual.

For instance, the e-mail '*[nickname]*@gmail.com' could be regarded as personal data.

- **Voice records:**

  The AEPD understood that, since an individual may be identified by its voice, voice recordings are personal data.

- **IP addresses:**

  According to the AEPD, a company providing Internet access may identify an Internet user by its IP address. Therefore, as with the assistance of such companies an Internet user could be identified (i.e. obtain his/her name, address, telephone number) IP addresses are personal data for the AEPD.

- **DNI (Spanish personal ID card numbers):**

  The AEPD confirmed that a list of containing only personal ID card numbers was governed by the data protection regulations, since, according to the AEPD, an ID card number might easily identify an individual. Thus, such numbers, on their own, are personal data.

- **Licence plate number:**

  In Spain, there is a Vehicle Registry which links number plates with vehicle owners. Citizens who can show a legitimate interest may be given access to such registry. This alone let the AEPD conclude that licence plate numbers should be regarded as personal data.

- **Fingerprint and other biometric data:**

  Fingerprints, as well as any other biometric information (e.g. an image of the iris), are considered to be personal data in Spain, as the AEPD assumes that an individual may be identified by such information without disproportionate efforts.

The above examples illustrate how the AEPD interprets the concept of personal data –which leads to the application of the data protection requirements– to information that can hardly be linked to an individual. For example, the AEPD declared on a case that ID card numbers alone are personal data. However, the truth is that finding individuals behind ID card numbers usually requires access to confidential Police databases, which is out of reach for most people. We believe the AEPD should have assessed such identification, as it may well require disproportionate efforts. However, the AEPD decided that such numbers are personal data.

The same applies for IP addresses or fingerprints. It is not always possible to identify an individual only with this information. Identification usually requires access to information kept by third parties (i.e. the Police, the Internet Services Provider, etc.) who have no obligation to disclose it to other third parties – or, actually, are prevented from doing so –.

As set out above, companies operating in Spain should be very careful when assessing what it is, and what is not, personal data. In general terms, to ensure that certain information will not be regarded as personal data, it has to be almost impossible for anybody to link it with the individual.

NOTIFICATION OF DATA FILES

Requirement

Prior to the processing of personal data, data controllers must register the *data file* containing such personal data with the AEPD (e.g. employees data file, clients data file, etc.). Such registration needs to be carried out by completing a standard notification form called "NOTA".

In general terms, the NOTA must include details as the data controller's corporate identity, the security measures implemented on the processing (indicating whether these are basic, medium or high level measures), the type(s) of data processed, the purpose(s) of the processing, details of foreseeable disclosure(s) and/or international transfer(s), and information about existing data processor(s).

Data controllers are required to keep data file registrations up to date. Thus, they are required to notify the AEPD (again, via a NOTA form) about any changes related to the personal data files registered.

Infringement

The infringement of the abovementioned requirement may give rise to a minor infringement, punished with the penalties detailed in this note below.

INFORMATION

Requirement

Data subjects from whom personal data is requested must be previously provided with specific information regarding the following aspects:

- the existence of a data file or processing of personal data, the purpose(s) of collecting the data and the potential recipient(s) of it;
- the identity and address of the controller or of its representative in Spain (if any);
- the compulsory or voluntary nature of the provision of the data requested by the controller;
- the consequences of providing the data and of refusing to provide it; and
- the possibility of exercising the rights of access, rectification, cancellation and/or objection.

However, note that the information set out in the last three bullet points will not be necessary if the content is clearly deduced from the nature of the personal data that is requested or from the circumstances in which it is collected.

If the personal data is not collected directly from the data subjects (e.g. disclosures of data from third parties) the data subjects must be informed explicitly, precisely and unambiguously by the data controller (the assignee in the case of a disclosure) within three months after collecting the data (e.g. after the assignment takes place) –unless the data subjects have been informed previously– about the following:

- the content of the processing;
- the origin of the data (e.g. the assignor);
- the existence of a file or processing of personal data;
- the purpose of collecting the data;
- the potential recipients of the data;+
- the possibility of exercising the rights of access, rectification, cancellation and objection; and
- the identity and address of the data controller or of its representative (if any).

Infringement

The infringement of the above-mentioned requirement may give rise to a minor infringement (when the personal data is collected from the data subjects) or to a serious infringement (in case of personal data is not collected directly from the data subjects), punished with the penalties detailed in this note below.

CONSENT

Requirement

As a general rule, processing of personal data requires the consent of the data subjects. The consent must be free, unambiguous, specific and informed. In the case of sensitive personal data (e.g. information relating to health, sexual behaviour, trade union membership, etc.), the consent must be explicit and, in certain cases, in writing.

There are some exceptions to the consent requirement. The most relevant are the following:

- when the processing of personal data is expressly authorised by law;
- when the personal data refers to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and is necessary for its maintenance or fulfilment; and
- subject to the comments below regarding the uncertainty of the application of this ground, and assuming the direct effect of article 7(f) of Directive 95/46/EC, it may be acceptable to waive the requirement of consent when the processing is necessary for the purposes of the legitimate interests pursued by the data controller, except when such interests are overridden by the interests arising directly from the fundamental rights and freedoms of the data subject.

In general terms, such exceptions are applied by the AEPD on a restrictive basis, and are assessed on a case-by-case basis. It must be very clear that an exception applies. Otherwise, the AEPD requires the data controller to have gained consent.

Note that the application of the "legitimate interest" exception in Spain is somehow uncertain. On July 2010, the Spanish Supreme Court referred two questions to the CJEU, on whether the implementation of the "legitimate interest" principle in the Spanish laws was consistent with the Data Protection Directive 95/46/EC. On 25 November 2011 the CJEU decided that such implementation was against article 7(f) of the Directive 95/46/EC, as it could only be applied to data collected from sources available to the public. The CJEU declared that said article 7(f) had direct effect in Spain. On 8 February 2012 the Spanish Supreme Court declared that article 10.2(b) of the Regulation of the DPA, which incorrectly transposed article 7(f), was null and void. At the moment, although companies may rely on the direct effect of article 7(f) of the Directive for processing personal data without consent, the AEPD is still reluctant to admit it on a general basis.

Infringement

The infringement of the abovementioned requirement may give rise to a serious infringement (in the case of non-sensitive personal data) or to a very serious infringement (in the case of sensitive data), punished with the penalties detailed in this note below.

SECURITY MEASURES

Requirement

Data controllers and data processors must implement technical and organisational measures necessary in order to ensure the security of the personal data and to prevent its alteration, loss, unauthorised processing or access, in accordance with the current state of the art, the nature of the data stored, and the risks to which it may be exposed.

The Spanish laws on data protection provide a detailed list of security measures to be implemented by the data controllers and data processors. Such measures are grouped in three cumulative different levels ("basic", "medium" and "high") depending on the sensitiveness of the personal data processed.

Infringement

The infringement of the abovementioned requirements may give rise to a serious infringement, punished with the penalties detailed in this note below.

THE SECURITY DOCUMENT

Requirement:

The Regulation of the DPA, as one of the organisational measures envisaged to ensure the security of personal data, establishes an obligation for data controllers to draw up a security document. Such document must contain a detailed list of the technical and organisational measures which should be binding on the personnel processing personal data, and/or with access to the information systems. At the discretion of the controller, the security document can be either general to all filing systems or processing carried out by the data controller, or individual for each filing system or processing. In any case, it shall be considered an internal document of the organisation.

The security document shall cover, at least, the following aspects:

- scope of application of the document, with detailed specifications on the resources to be protected;
- measures, regulations, protocols for action, rules and standards aimed at guaranteeing the level of security required by the applicable legislation;
- tasks and obligations of the staff in relation to the processing of personal data included in the filing system;
- structure of the filing systems containing personal data, and a description of the information systems that process such data;
- procedure for notification, management and response to incidents (e.g. security breaches);
- the procedures available for backup and recovery of the data processed or contained in the automated filing systems; and
- the measures required for transportation of supports or documents containing personal data, as well as the ones to observed for their destruction, or if appropriate, their re-use.

In cases where medium or high-level security measures are required in accordance with applicable legislation, the security document shall also contain:

- the identification details of the data controller(s); and
- the details about the monitoring activities fulfilled by the company from time to time to verify fulfilment of the measures provided therein.

In addition, if personal data is to be processed by third parties, the security document shall contain their identification details and the files and the processing to be carried out by such third parties, with express reference to the contract or document regulating the processing.

The security document should be kept up-to-date at all times and shall be reviewed whenever any material changes are made to the information systems, processing operations, its organisation, the contents of the information included in the filing systems or processing or, if appropriate, as a result of the periodic monitoring carried out by the company. Moreover, the content of the security document shall be adapted, at all times, to the applicable data protection provisions on security of personal data.

Infringement

The infringement of the abovementioned requirements may give rise to a serious infringement, punished with the penalties detailed in this note below.

DUTY OF SECRECY

Requirement:

The data controller and the persons involved at any stage of the processing of the personal data (e.g. data processors) are subject to professional secrecy as regards personal data and to the duty to keep them secret.

Infringement

The infringement of the above-mentioned requirement may give rise to a serious infringement, punished with the penalties detailed in this note below.

DISCLOSURES / ASSIGNMENTS

Requirement:

Personal data may be disclosed or assigned to third parties only for purposes directly related to the legitimate purposes of the assignor and assignee and, in general terms, with the prior consent of the data subject. Disclosures or assignments are also known as controller-to-controller transfers of data. The consent for the disclosure of the personal data is deemed null and void when the information given to the data subject does not enable him/her to know the purposes for which the personal data to be disclosed will be processed, and what are the type of activities carried out by the assignee. Thus, the assignor must inform the data subjects about these aspects before obtaining their consent for disclosing their data.

In addition to this information, the assignor must also indicate the purpose of the file, the nature of the data disclosed and the name and address of the assignee. Note that these details must be provided at the time the first disclosure of the personal data takes place (i.e. not necessarily when the consent of the data subject is obtained).

Notwithstanding the above, there are a number of situations where a disclosure of personal data does not require the consent of the data subjects. The most relevant ones are as follows:

- when the disclosure is expressly authorised by law;
- when the personal data has been collected from sources available to the public (note that sources available to the public are expressly defined in the DPA); and

- when the disclosure is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed (except when such interests are overridden by the interests arising directly from the fundamental rights and freedoms of the data subject).

As explained in the above section on consent, the application of the legitimate interest ground for carrying out disclosures of personal data must be carefully assessed. The provisions of the Regulation of the DPA on the "legitimate interest" ground which were inconsistent with article 7(f) of the Directive 95/46/EC were declared null and void by the Spanish Supreme Court. However, the AEPD is sometimes reluctant to admit the general application of this ground.

Nevertheless, further to the declared direct effect of article 7(f) we believe strong arguments can be enforced in order to carry out certain disclosures of data without the data subjects consent, provided that a legitimate interest exists, and that fundamental rights are not jeopardized.

Infringement

The infringement of the abovementioned requirement may give rise to a serious infringement (for non-sensitive personal data) or to a very serious infringement (in the case of sensitive data), punished with the penalties detailed in this note below.

DATA PROCESSORS

Requirement

Access to personal data by a third party (i.e. a "data processor") is not regarded as a disclosure of data if such access is: (1) necessary for the provision of a service to the data controller; (2) the personal data is processed only on behalf of the data controller; and (3) there is a contract in place in the terms mentioned below.

The DPA provides certain requirements which must be fulfilled by the data controller and the data processor. In particular, the processing to be carried out by the data processor must be regulated in a contract which must be in writing, and must expressly state that the data processor shall:

- process the personal data only in accordance with the instructions given by the data controller;

- not apply or use the personal data for a purpose other than that/those set out in the contract;
- not disclose the personal data to third parties, not even for back-up purposes; and
- implement specific security measures (to be regulated in the contract) in order to fulfil the requirements provided in the DPA.

Moreover, once the service has been provided, the personal data must be cancelled or returned to the data controller, together with any media or documents containing the personal data.

The restriction regarding disclosure of data to third parties does not prevent access to personal data from subcontractors of the data processors (sub-processors). However, such access is subject to restrictive requirements which must be taken into account in the agreement between the controller and the (original) data processor.

Infringement

Access by a data processor to personal data of the data controller without having entered into an agreement containing the provisions required by article 12 of the DPA is regarded as a minor infringement, punished with the penalties detailed in this note below.

INTERNATIONAL TRANSFERS

Requirement

In general terms, any transfer of personal data outside the European Economic Area ("**EEA**") is regarded as an international transfer and is subject to the requirements provided for in the DPA.

As a general rule, international transfers of personal data to public or private entities or individuals located in the territory of a country which is not a member of the EEA or which the EU Commission or the AEPD has not declared that they provide an adequate level of protection are not allowed except with the prior authorisation of the Director of the AEPD. Such authorisation is obtained on a case-by-case basis.

Contrary to other EU countries, the existence of EU Standard Contractual Clauses approved by the Commission Decisions 2004/915/EC and 2010/87/EU, in place between the importers and the Spanish exporters, does not suffice in order to carry out the international transfer of personal data. The authorization of the AEPD is required anyhow.

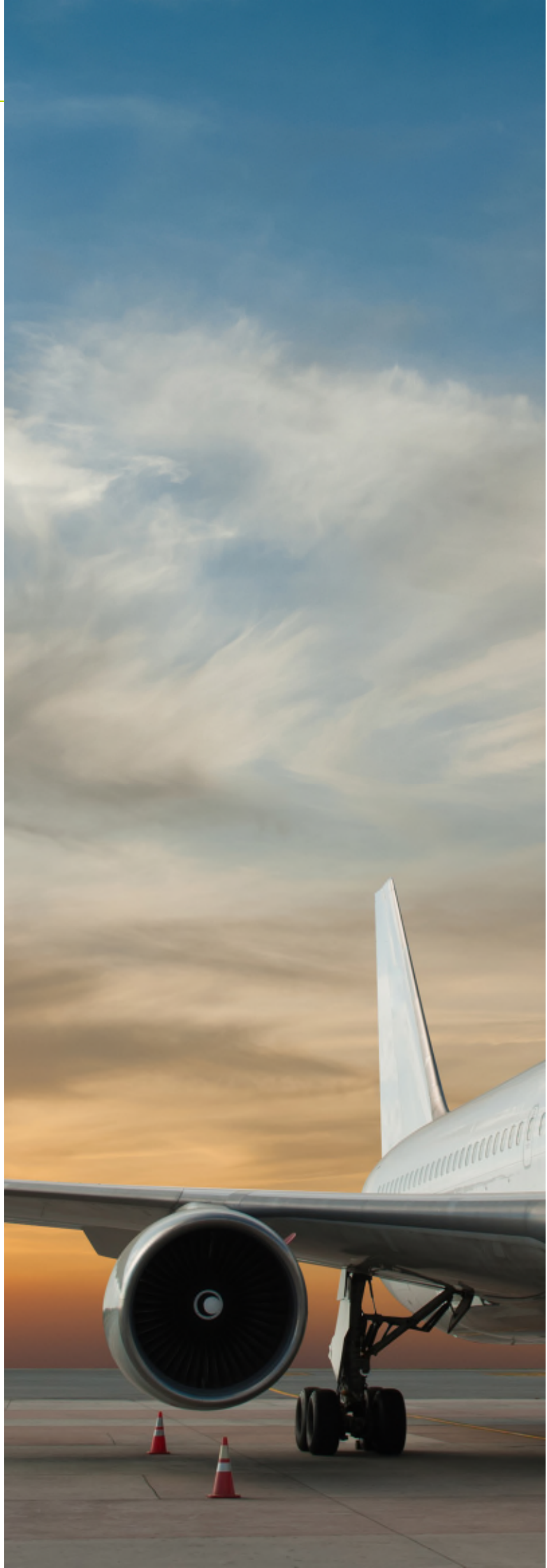
Although the EU Standard Contractual Clauses are designed to be used without modifications, the AEPD tends to require introducing some minor amendments in the clauses, in order to ensure consistency between the Standard Contractual Clauses and the requirements envisaged by the Spanish data protection laws.

Not so long ago, the AEPD has also issued a new set of Standard Contractual Clauses that allow data processors based in Spain to request (as the exporters of the data) the authorization themselves, for the international transfers of the data processed on behalf of their customers (the data controllers). The aim of these new Standard Contractual Clauses is to increase flexibility in the international transfers of data made within the scope of the services that use resources located offshore (e.g. offshore outsourcing, cloud computing, etc.).

There are a number of exemptions which allow carrying out international transfers without the previous authorization of the AEPD. The most relevant are as follows:

- when the international transfer is related to money transfers in accordance with the relevant legislation;

- when the transfer is necessary or legally required to safeguard a public interest (e.g., a transfer requested by a tax or customs authority for the



performance of its task shall be considered as meeting this condition);

- when the data subject has given his/her explicit and unambiguous consent to a specific international transfer;
- when the transfer is necessary for the performance of a contract between the data subject and the data controller or the adoption of pre-contractual measures taken at the data subject's request; and
- when the transfer is necessary for the execution or performance of a contract executed, or to be executed, in the interest of the data subject, between the data controller and a third party.

Note that these exceptions are applied on a very restrictive basis by the AEPD. This is particularly relevant in the last two cases. The "need" identified for the purpose of the exceptions must be a genuine need.

Moreover, note that in order the consent for the international transfer to be valid, the data subject must be provided with information regarding:

- the fact that the transfer is to "x" country not providing an adequate level of protection in accordance with the Spanish and EU data protection regulations; and
- the specific purposes of the transfer.

A note on binding corporate rules

In addition to the above, in order to overcome the restrictions affecting international data transfers in a cost-effective, sustainable and effective manner, some companies choose to adopt and implement binding corporate rules ("**BCRs**"), and most recently, binding corporate rules for processors or binding safe processor rules ("**BSPRs**").

There are many advantages of adopting a model based on BCRs (or BSPRs) for international transfers and Spain is no exception to this rule. Although it is important to note that it will still be necessary for a company implementing BCRs or BSPRs to request an authorization from the Director of the AEPD in order to carry out international transfers of data, it significantly improves and facilitates the process for obtaining such authorizations.

For more extensive information on BCRs (and BSPRs) please review the articles published in our global privacy blog "*The Chronicle of Data Protection*" here:

http://www.hldataprotection.com/tags/binding-corporate-rules/

Requirements on international transfers are in addition to the ones outlined for disclosures / assignments of data, or processing of data on behalf of third parties, as applicable.

Infringement

The infringement of the above-mentioned requirement may give rise to a very serious infringement, punished with the penalties detailed in this note below.

"The team really understands our point of view, so we don't have to explain extensively."

Chambers & Partners 2014

ACCESS, RECTIFICATION, CANCELLATION AND OBJECTION

Requirement

Data controllers are required to grant to the data subjects the right to access their personal data, to rectify or cancel non-accurate personal data and to object to a particular processing thereof.

Note that, in contrast to the position in many Member States, in Spain, cancellation does not imply immediate erasure or deletion of the data. The data must remain blocked for certain periods of time, while any liability connected with the processing of such data is may arise.

Exercise of such rights is subject to specific and sometimes very formalistic requirements.

Infringement

The infringement of the above-mentioned requirement may give rise to a serious infringement, punished with the penalties detailed below.

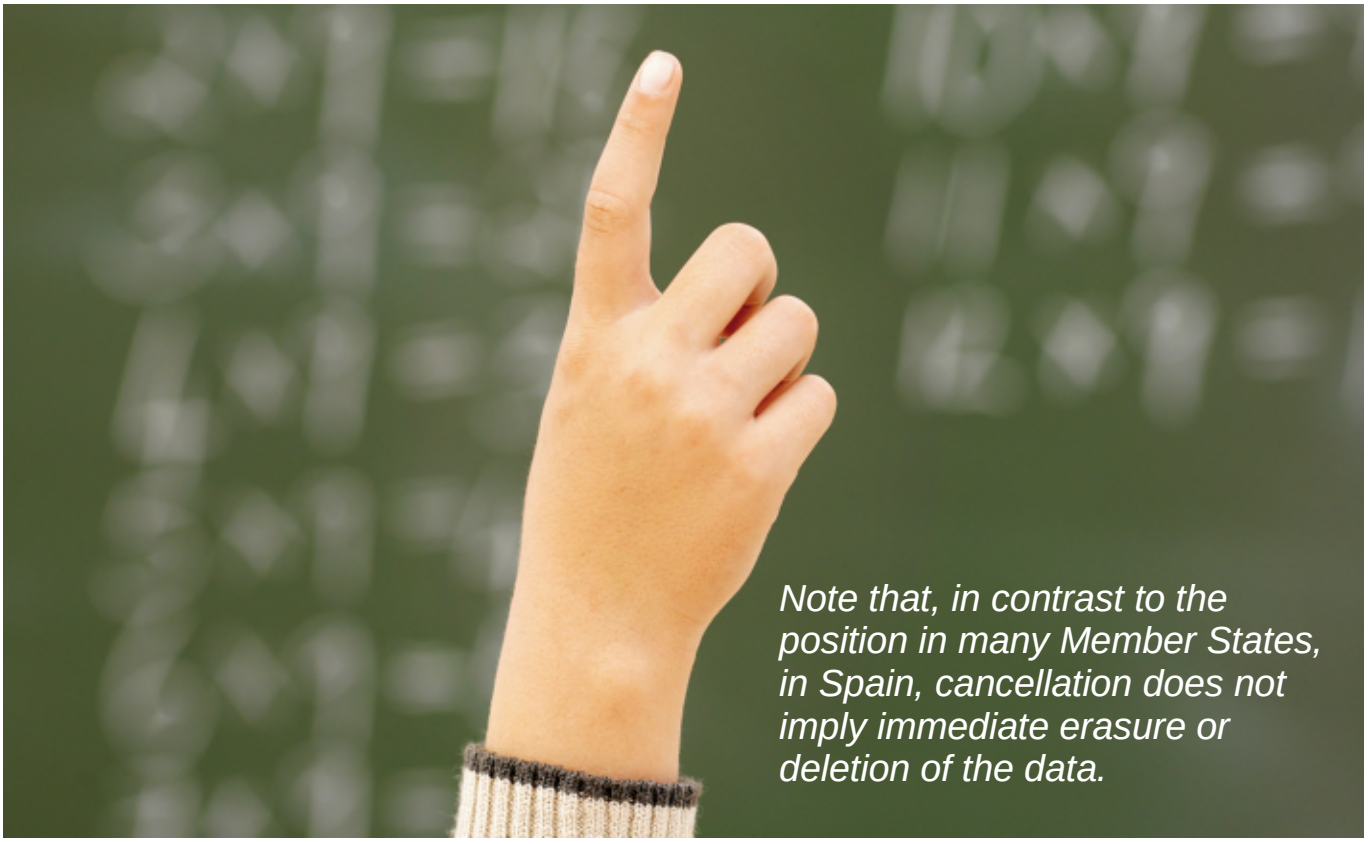
COOKIES

Requirement

Pursuant to article 22 of the Information Society Services Act 34/2002 ("**ISSA**") –as amended by Royal Decree-Act 13/2012 transposing the Directive 2009/136/EC– service providers may use devices for the storage and recovery of data (e.g. cookies) in the recipients' equipment provided that they have obtained the recipients' prior consent for such use. Note that such consent must be obtained before placing any cookies but after providing the data subjects clear and complete information about their use, and in particular, about the purposes for which cookies are going to be processed pursuant to the ISSA and the DPA.

The amended Article 22 of the ISSA makes clear the need to obtain prior opt-in consent from users before placing cookies. Previously, providing adequate information to users about their ability to opt-out was enough. This can be achieved from the data subject's 'implied consent' as long as some specific action is been taken before placing cookies from which his/her consent may be inferred.

In line with Recital (66) of Directive 2009/136/EC, service providers can still rely on the settings of a web browser or other application to provide opt-in consent, provided that users take an express action to establish



the setting when installing or upgrading the browser or application, where technically feasible and effective. However, it is somehow cumbersome to rely on this provision, as it is not possible assume in advance that all users will take such previous express action.

Note that service providers are exempted from the requirements foreseen by ISSA for cookies that only serve the purpose of facilitating the operation of an electronic communication network or to that carry out an explicit request of a user.

Infringement

The infringement of the abovementioned requirement may give rise to a serious infringement of the ISSA punished with a fine from € 30,001 to € 150,000. Please be aware that the AEPD has been very active recently on these matters, being the first data protection authority of the EU to issue cookie-consent related fines to two companies that used cookies without first obtaining informed consent and providing adequate control to data subjects.

SECURITY BREACH NOTIFICATIONS

Requirement

Royal Decree-Act 13/2012 mentioned above has also modified the Electronic Communications Act 32/2003 ("**ECA**") transposing the regulation on security breach notifications provided for in Directive 2009/136/EC.

Pursuant to article 34.4 of the ECA, operators operating networks or providing electronic communication services available to the public must notify the AEPD about the security breaches they suffer (provided that personal data is, or might have been, affected by such breaches).

In cases where a security breach may be specifically adverse to the privacy of individuals (e.g. passwords, payment card numbers, etc.), such individuals must also be notified. However, such notification to individuals can be prevented if the operator is able to prove before the AEPD that it has implemented enough technological measures to protect and prevent third parties from accessing the data which concerned the individuals' privacy.

Infringement

The infringement of the above-mentioned requirement may give rise to a very serious infringement of the ECA punished with a fine up to €2,000,000.

INFRINGEMENT PENALTIES

Non-compliance with the requirements provided in the DPA may give rise to different penalties depending on the seriousness of the infringement, as follows:

- **Minor infringements**: fines from €900 up to €40,000.
- **Serious infringements:** fines from €40,001 up to €300,000.
- **Very serious infringements**: fines from €300,001 up to €600,000.

Moreover, under certain specific circumstances, the AEPD may require the data controller to terminate processing of the data at all, and should there be no response to this requirement, immobilise the relevant data files for the sole purpose of restoring the rights of the data subjects.

For each of the above levels of infringement, the final amount of the fine is graded according to the following criteria: the continuing nature of the infringement; the volume of data processed; the degree to which the activity of the infringer is linked with the processing of personal data; the turnover of the infringer; the profits obtained as a consequence of the infringement; the level of intent; the repeated nature of the infringement; the nature of the damages caused to the data subjects and to other third parties; the accreditation by the infringer of having proper procedures in place for the collection and processing of personal data before the infringement, thus, being the infringement the result of an anomaly in the running of such procedures and not the result of a lack of diligence; and, to any other circumstances that may be relevant in order to determine the level of unlawfulness and culpability in connection with the infringement.

As an alternative to fines, sometimes the AEPD may simply warn the infringer and give a period of time to fix the breach. If the breach is not fixed, the AEPD may then impose fines. This is an exceptional measure applied by the AEPD on a discretional basis. Warnings are not applicable in case of very serious breaches of the law or in case the offender has been warned or punished before.

CONCLUSIONS AND RECOMMENDATIONS

Fulfilment of the Spanish data protection requirements is not an easy task. However, it is not impossible either.

The risk of breaching such requirements is high. The AEPD is continuously monitoring the activity of the companies operating in Spain and everyday imposes fines. Such fines are sometimes very high.

On top of that there is a reputational risk. The resolutions where the AEPD imposes fines are public and are posted in the AEPD's website. It is not uncommon to see news about fines on the media and newspapers, when well-known companies are fined because of breach of the DPA.

There are sectors where the AEPD is particularly focused at the moment, such as banking, insurance, telecommunications and e-commerce. However, the truth is that all the companies are under its "radar".

Companies operating in Spain will benefit from taking the appropriate measures on time, in order to ensure compliance with the Spanish data protection requirements, and avoid the unpleasant experience of going through a sanctioning procedure, and ultimately been sanctioned. The earlier such measures are taken, the better.

Gonzalo F. Gállego
Partner, Madrid
T +34 (91) 3498 257
gonzalo.gallego@hoganlovells.com

Further information

If you would like further information on any aspect of Data Protection and Privacy in Spain please contact the person mentioned above or the person with whom you usually deal.

This note is written as a general guide only. It should not be relied upon as a substitute for specific legal advice.

www.hoganlovells.com

Hogan Lovells has offices in:

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Jeddah*
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington DC
Zagreb*

*Associated offices