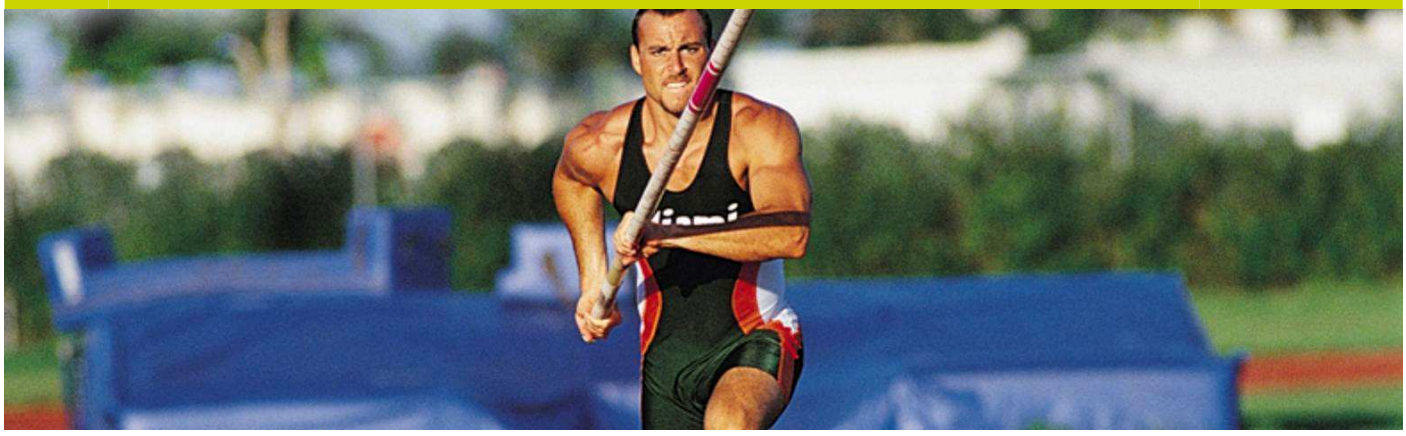
Hogan Lovells

Data Protection compliance in Spain

Mission Impossible?

May 2012



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

Contact
Gonzalo F. Gállego
Partner - IPMT
T +34 913 498 200
gonzalo.gallego@hoganlovells.com

Pablo Rivas
Senior Associate - IPMT
T +34 913 498 200
pablo.rivas@hoganlovells.com

Contents

Data Protection compliance in Spain

Mission Impossible?

INTRODUCTION

Spain is well known for having one of the most restrictive data protection regimes in the European Union.

It also has some of the highest penalties (up to €600,000 per infringement) and a data protection regulator - the Spanish Data Protection Agency "**AEPD**") - with a reputation for being fierce. These penalties are not only on paper. They are applied in practice. For instance, some of the penalties imposed by the AEPD in the last years include fines of **€450,000, €841,000 and €1,400,000.**

The above ingredients altogether make a cocktail that is not easy to drink -and sometimes becomes poisonous- for companies operating in Spain.

The purpose of this note is to help these companies to meet Spanish requirements on data protection.

In this document we include a summary of 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**"). .

Note that the European Union ("**EU**") authorities are currently working in a new EU Regulation on Data Protection that will substantially change the data protection framework in the EU. The draft, which will be discussed soon by the European Parliament, proposes, among others, how companies shall handle its employees and clients' personal data, along with the establishment of serious punitive measures such as sanctions that may rise up to 5% of the total sales of a company. It is foreseen that this new EU Regulation will be approved in 2013.

The information included below is a summary provided for information purposes only and must not be regarded as exhaustive of the entire legal regime which applies to the processing of personal data in Spain.

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.). No other information is necessary in order to identify the data subject.

An identifiable individual is one who can be identified indirectly, in particular 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 periods of time or activities.

However, the Spanish data protection requirements do not apply to anonymous (*non-identifiable*) data, which is not regarded to be 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 would include only statistical information.

It shall be noted that personal data refers to the total volume of information held on any individual by any person or entity. Therefore, it does not matter that, for example, a department in a company merely processes a reference number identifying a data subject, if another department of the same company (or even another company) is able to link such reference number with any other information about the data subject, by which he or she can be identified. In this case, such reference number cannot be considered as anonymous data.

Therefore, personal data means information:

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

The AEPD tends to apply the concept of personal data very widely. There are cases where the AEPD has considered that certain information was personal data although it was very difficult to link the information with an individual.

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

Examples of Personal Data

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

The existence of personal data is not always obvious, as can be seen in the following examples of information that was considered to be personal data by the AEPD, even where the information was processed alone, i.e. without any link with other information on the data subject.

- **E-mail address:**

  According to the AEPD, e-mails are personal data, even when such e-mails do not include information relating to an individual (i.e., name, company, country, etc.), as in these cases the individual may still be

There are cases where the AEPD has considered that certain information was personal data even though it was very difficult to link the information to an individual.

identified by the provider of the e-mail service.

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

- **Voice records:**

  The AEPD understood that, since an individual may be indentified by its voice, then the voice shall be considered as personal data.

- **IP address:**

  According to the AEPD, a company providing Internet access may identify an Internet user by its IP address. Therefore, given that with the assistance of such third party (company providing Internet access), an Internet user may be identified (i.e. obtain his/her name, address, telephone number), then the IP address is considered to be personal data.

- **DNI (Spanish identification number):**

  The AEPD decided that a data file containing only DNIs of individuals (i.e. only the number), was governed by the data protection regulations, since it considered that an individual may easily be identified by his/her DNI and therefore such DNI should be considered as personal data.

- **Licence plate number:**

  Given that in Spain there is a Registry of Vehicles, which may be consulted by citizens with a legitimate interest, and from which an individual may be easily identified using only the licence plate number of his/her vehicle, then such licence plate number is considered to be 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, as the AEPD considers that an individual may be indentified by such information.

The above examples show AEPD's tendency to apply the concept of personal data -and, thus, the requirements provided for in the data protection regulations- to information which hardly can be linked to an individual. For instance, the AEPD considered that the DNI number was personal data. However, generally speaking, in order to find out who is the owner of a DNI it is necessary to check databases which are kept by the Police and are confidential. Thus, although in theory, the DNI is linked to an individual, the truth is that, in practice, it is not possible for most of the people to identify an individual by means of his/her DNI number. This is a case where the AEPD should have considered that the identification of the individual required a disproportionate effort. However, the AEPD did not conclude so.

The same applies in the case of the IP address or fingerprints. It is not obvious that it is possible to identify an individual only with this information. The identification requires access to information kept by third parties (e.g. the Police, or the Internet Services Provider, etc.) who have no obligation -or, actually, are prevented from doing so- of giving access to it to third parties.

As set out above, companies operating in Spain should be very careful when considering what it is and what it is not personal data. In general terms, in order for information not to be deemed as personal data, it has to be almost impossible for any person to link the information to the individual.

NOTIFICATION OF DATA FILES

Requirement

Prior to the creation of a personal data file, data controllers must notify the AEPD of the creation of the data file. This is done by completing a standard form called "NOTA".

In general terms, the notification must contain details of the data controller's corporate identity, security measures implemented (indicating whether they are basic, medium or high level measures), the type of data processed, the purposes of the processing, details of foreseeable disclosures and international transfers of personal data and information about the existence of data processors.

The notifications of personal data files must be kept updated. Thus, the data controllers are required to notify to the AEPD any modifications in the personal data files which affect to the information notified in the past.

Infringement

The infringement of the above-mentioned 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 previously be provided with specific information regarding the following aspects:

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

However, note that the information set out in the last three subparagraphs is not required if its content can be clearly deduced from the nature of the personal data requested or the circumstances in which it is obtained.

On 8 February 2012 the Spanish Supreme Court declared that the article 10.2(b) of the Regulation was not consistent with the "legitimate interest" ground for the processing of personal data provided for in article 7(f) of the Data Protection Directive. Consequently, this article was declared null and void. Unfortunately, the inconsistency with the Directive remains in the DPA which only the Spanish Parliament is entitled to modify.

In addition to this, if the personal data is not collected directly from the data subjects (e.g. as a consequence of a disclosure where the data is collected from the assignor) 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 the collection of the personal data -unless the data subjects have been informed previously- of the following:

- content of the processing,
- the origin of the data,
- the existence of a file or personal data processing operation,
- the purpose of collecting the data,
- the recipients of the information,
- 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 the case of personal data 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 unambiguous 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 as follows:

- when the processing of personal data is authorised by law
- when the personal data relates 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, when the processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Such exceptions are applied by the AEPD on a restrictive basis. It must be clear that the exception applies. Otherwise, the AEPD requires consent.

Note that the application of the "legitimate interest" ground in Spain is somehow uncertain. On July 2010, the Spanish Supreme Court referred two questions to the European Court of Justice ("**ECJ**"), in order to confirm whether the implementation of the "legitimate interest" justification carried out by the Spanish laws was consistent with the Directive 95/46/EC on Data Protection.

On 25 November 2011 the ECJ issued its decision solving the two prejudicial questions. The Court stated that the Spanish implementation of the "legitimate interest" justification was against section 7(f) of Directive 95/46/EC. The ECJ also declared that said section of the Directive had direct effect in Spain.

Further to the ECJ Decision, on 8 February 2012 the Spanish Supreme Court declared that article 10.2(b) of the Regulation of the DPA which incorrectly transposed the "legitimate interest" justification, was null and void. However, the regulation on legitimate interest (equivalent to the one of the Regulation) remains in the DPA as the Supreme Court has no power to modify a law such as the DPA. We will have to wait until a new data protection law (or a modification of the DPA) correctly transposing section 7(f) of Directive 95/46/EC is approved by the Spanish Parliament. In the meanwhile, companies may rely on the direct effect of article 7(f) of the Directive in order to make use of the "legitimate interest" ground for processing personal data.

Infringement

The infringement of the above-mentioned requirement may give rise to a serious infringement (in the case of "normal" 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 to ensure the security of the personal data and prevent its 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 the 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 with respect to the processing of personal data. Such measures are grouped in three different levels ("basic", "medium" and "high") depending on the sensitiveness of the personal data processed.

Infringement

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

The Spanish AEPD has recently approved a new set of Standard Contractual Clauses that can be entered into by data processors based in Spain with sub-processors outside the EEA. This will allow data processors to obtain an authorization from the AEDP in order to carry out international transfers of personal data processed on behalf of their customers.

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 functions of the assignor and assignee and, in general terms, with the prior consent of the data subject. The consent for the disclosure of the personal data is deemed null and void when the information given to the data subject before granting the consent does not enable him/her to know the purpose for which the personal data to be disclosed will be used or the type of activity of the assignee to which the personal data will be disclosed. Thus, the assignor must inform the data subjects about these aspects before obtaining the consent for the disclosure.

In addition to this information, when making the first disclosure of personal data, the assignor must notify this fact to the data subjects, also indicating the purpose of the file, the nature of the data disclosed and the name and address of the assignee. Note that this information must be provided when carrying out the first disclosure of the personal data (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 authorised by law;
- when the personal data has been collected from sources accessible to the public (as this term is 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 where such interests are overridden by the interests for fundamental rights and freedoms of the data subject

As explained in the above section about the consent, note that the application of the legitimate interest ground for carrying out disclosures of personal data is still subject to some uncertainty in Spain. The provisions of the Regulation which were inconsistent with the "legitimate interest" ground provided for in the Data Protection Directive, were declared null and void by the Spanish Supreme Court. However, such inconsistent provisions remain in the DPA.

Nevertheless, further to the declared direct effect of section 7(f) of Directive 95/46/EC and to the foreseen modification of the DPA, we believe that there are strong arguments to defend that disclosures of data may be carried out without the data subjects consent provided that a legitimate interest exists and fundamental rights are not jeopardized.

Infringement

The infringement of the above-mentioned requirement may give rise to a serious infringement (in the case of "normal" 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

Under the Spanish laws on data protection, access to personal data by a third party (i.e. a "data processor") is not regarded as a disclosure of data provided such access is necessary for the provision of a service to the data controller, the personal data is processed by such data processor only on behalf of the data controller and there is a contract in place in the terms mentioned below.

DPA provides certain requirements which must be fulfilled by the data controller and the data processor. In particular, the processing by the data processor on behalf of the data controller must be regulated in a contract which must be in writing, it being expressly laid down that the data processor:

- shall process the personal data only in accordance with the instructions given by the data controller;
- shall not apply or use the personal data for a purpose other than that set out in the contract;
- shall not disclose the personal data to third parties, not even for back-up purposes; and
- shall implement specific security measures (to be regulated in the contract) in order to fulfil the requirements provided in the DPA.

Moreover, note that once the contractual service has been provided, the personal data must be cancelled or returned to the data controller, together with any media or documents which contain personal data processed.

The restriction regarding disclosure of data to third parties does not prevent access to personal data y 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

In contrast to the position in many other Member States, in Spain, cancellation does not imply immediate erasure of the data. The data must be kept "blocked" during a period of time.

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 movement 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 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.

Up to now, the data controllers subject to the DPA where the only ones authorized to request the authorization of the AEPD for the international transfers of data. However, the AEPD has recently issued a new set of Standard Contractual Clauses that allow data processors based in Spain to request themselves (as the exporters of the data) the authorization for the international transfer of the personal 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 transfer of data 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 unambiguous consent to the 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 according to the Spanish and EU data protection regulations; and
- the purposes of the transfer.

Requirements on international transfers are in addition to the ones of disclosures/assignments 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.

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 certain processing thereof.

Note that, in contrast to the position in many Member States, in Spain, cancellation does not imply immediate erasure of the data. The data must remain blocked for certain periods of time, while any liability arising from the processing is determined

On April 2nd 2012, after almost a year of delay, Spain modified its laws in order to implement the so called "Cookies Directive". This modification makes clear the need to obtain the prior, opt-in consent of users before placing cookies.

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**") - recently modified by Royal Decree-Law 13/2012 in order to transpose Directive 2009/136/EC - services 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' consent for such use after providing them with clear and complete information on their use, and in particular, on the purposes for which their personal data is going to be processes pursuant to the DPA.

The new article 22 of the ISSA is a relevant change in the Spanish rules on cookies. It makes clear the need to obtain the prior opt-in consent of users before placing cookies. Previous article 22, only required service providers to inform users of their ability to opt out.

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.

Moreover, the Royal Decree-Law 13/2012, does not modify the exemption in the ISSA that permits service providers to place cookies to facilitate the operation of an electronic communication network or to carry out an explicit request of a user

Infringement

The infringement of the above-mentioned requirement may give rise to a serious infringement of the ISSA punished with a fine from €30,000 to €150,000.

SECURITY BREACH NOTIFICATIONS

Requirement

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

Pursuant to the new article 34.4 of the ECA, operators exploding networks or providing electronic communication services available to the public must notify to the AEPD the security breaches they suffer that affect to personal data.

In case a security breach may be adverse to the privacy of the individuals (e.g. passwords, payment card numbers, etc.), such individuals must also be notified by the operator. However, such notification to the individuals is not necessary if the operator is able to prove before the AEPD that it has implemented enough technological protection measures as to prevent third parties from accessing to the data concerning the privacy of the individuals.

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 €300,000.1 up to €600,000.

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

For each of the above levels of infringement, the amount of the penalty is graded according to the nature of the personal rights affected, the volume of data processed, the benefits obtained, the level of intent, the repeated nature of the infringement, the damage and loss occasioned to the data subjects and to third parties, the connection between the activity of the infringer and the carrying out of processing of personal data, the benefits obtained by the commission of the infringement, the accreditation by the infringer that before the commission of the infringement it had proper procedures for the collection and processing of personal data being the infringement the result of an anomaly in the running of such procedures not due to a lack of diligence of the infringer, and to any other circumstance that may be relevant in order to determine the level of unlawfulness and culpability present in the infringement.

Please note that the DPA has been modified recently and now, as an alternative to fines, 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.

Companies operating in Spain must take appropriate measures in order to ensure compliance with the Spanish data protection requirements

CONCLUSIONS AND RECOMMENDATIONS

Fulfilment of Spanish data protection requirements is not an easy task. However, it is neither an impossible one.

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

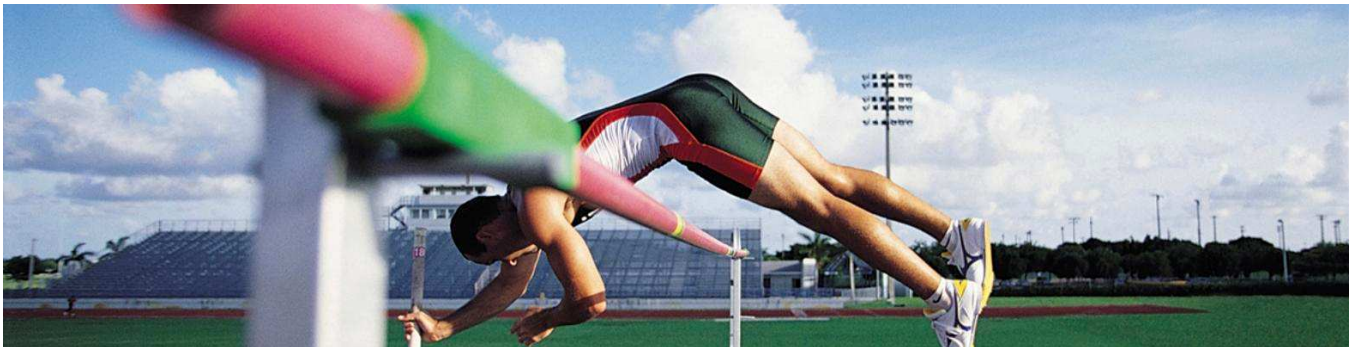
There is also a reputational risk. The resolutions where the AEPD imposes fines, are public and are posted in the AEPD's website. It is not uncommon to see news in the news papers about well-known companies been fined because of breach of the DPA.

There are sectors where the AEPD is particularly focused, such as banking, insurance and telecommunications. However, the truth is that all the companies are under the "radar" of the AEPD.

Companies operating in Spain must be conscious of this situation and take appropriate measures in order to ensure compliance of Spanish data protection requirements. The earlier such measures are taken, the easier the fulfilment of such requirements is.

At Hogan Lovells International LLP, *'the overall service is fantastic' and its lawyers are 'very up-to-date on the regulatory framework in the country'. They are 'very knowledgeable on data protection', and his 'speed and availability are unparalleled'.*

Legal 500 EMEA (Spain),2012



www.hoganlovells.com

Hogan Lovells has offices in:

Abu Dhabi
Alicante
Amsterdam
Baltimore
Beijing
Berlin
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jeddah*
London
Los Angeles
Madrid
Miami
Milan
Moscow
Munich
New York
Northern Virginia
Paris
Philadelphia
Prague
Riyadh*
Rome
San Francisco
Shanghai
Silicon Valley
Singapore
Tokyo
Ulaanbaatar
Warsaw
Washington DC
Zagreb*