INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

COORDINATED BY DR. REINHARD KREISSL
IRKS INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE
WEIN, AUSTRIA

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

LED BY PROFESSOR CLIVE NORRIS AND DR XAVIER L’HOIRY
DEPARTMENT OF SOCIOLOGICAL STUDIES
UNIVERSITY OF SHEFFIELD, UK

SPAIN COUNTRY REPORTS

UNIVERSITAT DE BARCELONA, SPAIN

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN SPAIN – DR GEMMA GALDON-CLAVELL & LILIANA ARROYO-MOLINER

LOCATING THE DATA CONTROLLER IN SPAIN – DR GEMMA GALDON-CLAVELL & LILIANA ARROYO-MOLINER

SUBMITTING ACCESS REQUESTS IN SPAIN – DR GEMMA GALDON-CLAVELL & LILIANA ARROYO-MOLINER
MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN SPAIN

Application (primary and secondary legislation) and interpretation (case law) of data protection principles

Article 18 of the Spanish Constitution establishes that: 1) the right to one’s honour, personal and family privacy [intimidad] and one’s own image is guaranteed; 2) one’s home address is inviolable. No one can enter or search a person’s home without the consent of the owner or judicial authorisation, unless a flagrant crime or offence has been committed. 3) Communications are secret, whether they are postal, telegraphic or via phone, unless there is judicial authorisation. 4) The law limits the use of informatics in order to protect the honour and personal and family privacy of citizens and their full enjoyment of their Rights. Article 10 of the Spanish Constitution also establishes a related right: the respect of one’s dignity.

The right to personal data protection thus stems from Articles 10 and 18.4 and is developed in the Organic Law¹ 15/1999 of Personal Data Protection (Ley Orgánica de Protección de Datos, LOPD, in Spanish), approved on December 13, 1999 repealed the previous Act 5/1992, of 29 October, regulating the processing of personal data (known as LORTAD).

The new Act is divided into seven sections and several transitional provisions and repeals. It lacks a statement of the objectives found in the Organic Law 15/1999. This omission is reprehensible, because the legislature is obliged to make known to the population what is the objective pursued with the approval of any new law.

The purpose of the law is to guarantee and protect, with regard to the processing of personal data, public freedoms and fundamental rights of physical persons, and especially their honour, intimacy and personal and family privacy. It is a law of an administrative nature and it applies to personal data recorded in any medium that enables its processing, as well as its subsequent use by the public and private sectors.

In order to develop the provisions of the Organic Law, the government approved the Royal Decree 1720/2007, of 21 December, regulating the principles of law and the security measures applicable to information systems. These provisions also established the creation of a Data Protection Agency, since 2003 called Spanish Agency for Data Protection (AEPD in Spanish), to enforce the rules in the Spanish territory. In turn, other regional agencies have been created, in Catalonia, Madrid and the Basque Country.

The DPAs are responsible for exercising the power to impose sanctions, which are high in cases of infraction, and publishing the list of sanctioned companies once a year, indicating the amount and date of the fine. Even though Spain appears to be the EU

¹In the Spanish legal framework constitutional matters relating to fundamental rights and freedoms are regulated by Organic Laws, which require a parliamentary debate and an absolute majority to be approved.
country with higher sanctions for breaches of data protection, there is still a large number of companies that do not comply with the law, or do so poorly. For instance, in 2012 the fines issued to companies in breach of data protection legislation increased by 12%. It is interesting to note that the recent passage of the Sustainable Economy Act 2/2011, of March 4, has modified some of the wording under the Title "Offences and Penalties" of the Data Protection Law.

The public sector is more effective in meeting the standard, although its interpretation causes many practical problems, as a rigid interpretation of the Data Protection Act conflicts with the objective of transparency and citizen control of public authorities. Thus in Spain data protection and access to information are two related areas, as a proper application of the right to protect data that should allow progress towards a more democratic society, respectful in turn with the private rights of citizens and the individual and collective right to a more democratic political system.

The principles that the legislator has established, in reference to data protection, are found in Title II (Articles 4-12) of the Data Protection Act:

- **Quality** - The personal data to be collected and/or processed must be adequate, relevant and not excessive in relation to the particular purposes intended to be accomplished with its collection and/or processing. These purposes should in turn be explicit and legitimate.

- **Information to data subjects when the data is collected** – On a general basis, people should be informed explicitly, precisely and unequivocally of the existence of a file or processing of their data, of the purpose of the collection/file, about the recipients of the information, of the consequences of a refusal to cooperate, on how to exercise the rights of access, rectification, cancellation and opposition and on the identity and address of the data controller.

- **Consent** - The processing of personal data requires the consent of those affected, unless otherwise stated by law (for instance when collected in order to allow the normal functioning of public bodies, among others).

- **Specially protected data** - Files having as their sole purpose the collection of data related to people's ideology, trade union affiliation, religion, beliefs, racial or ethnic origin, or sex life are explicitly prohibited.

- **Health Data** - The law refers to sectorial legislation to regulate the protection of health data, recognizing the need for specific regulation in this field, as health institutions, public and private, need to collect and process personal data on a general, regular basis.

---


IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
• Data security – Those agents (data controllers) responsible for the collection and storage of personal data files must be specified and identifiable.

• Duty of secrecy - Any person engaged in any phase of data treatment is bound by professional secrecy.

• Data Communication – Data can only be communicated to third parties if this is necessary for the fulfilment of the purposes related to the functions of involved parties and with the consent of the data subject. The exceptions to this consent are stated in Article 11 of the LOPD.

• Access to data by third parties – If third-party access is necessary in order to provide a service to the data controller, it will not be considered data communication to third parties.

Since the Organic law was passed, there have been numerous court rulings on how to interpret its precepts. One deserving special attention is the Constitutional Court Judgment 290/2000, of November 30, which declared contrary to the Constitution and null Art. 24.2 (exceptions to the rights of data subjects) and modified the wording of Art. 21.1 (communication of information among public bodies) and 24.1 (exceptions to the rights of data subjects). Before this Constitutional Court Judgment data transfer from one public body to another (both the same level or not) was possible without notice or consent on behalf of the citizen, even when the aims were different from the primary data collection (rewording related to 21.1). The second modification refers to the limitation of the basic rights of those affected, such as the right to information before data collection takes place, the right to access once it has taken place and, where appropriate cancellation by a regulatory standards. Following these changes, a stricter regime is now in place which conceives the right of protection of one’s own personal data as an autonomous right.

In 2010, the Supreme Court declared null several articles of the Spanish data protection law as a consequence of three administrative appeals. Those were: Article 11 (data verification in access requests to public bodies) Article 18 (Accreditation of duty of information), Article 38.2 (Requirements for inclusion of data), and Article 123.2 (competent personnel for conducting preliminary proceedings) and the final paragraph of Article 38.1.a) (Requirements for inclusion of data) of the Royal Decree 1720/2007. Generally speaking, this reform led to a scenario where personal data of debtors can be treated without informed consent of the data subject if they can state a “legitimate interest”.

Subsequently, the Supreme Court Judgment of February 8, 2012 (Appeals 23 and 25/2008) is also noteworthy. This case overturned Art. 10.2.b) of the Royal Decree 1720/2007, precisely because it established the need for prior consent for the disclosure of information from ‘non public’ sources, as this was deemed to be in conflict with the European Directive. In this regard, it is mandatory to consider the legitimate interests

---

4Art. 3.j) LOPD and 7.e) in 1720/2007 are very restrictive in their definition of ‘public source’. This means that for the AEPD a website is not a ‘publicly available source’. Only social media sites are ‘public sources’ and therefore only the data used by these sites can be used by third parties without consent.
pursued by those responsible of disclosing data to third parties. The processing of certain kinds of data is strictly prohibited (Ruling of the Court of Justice of the European Union November 24, 2011).

**Application (primary and secondary legislation) and interpretation (case law) of the right of access to data**

Personal data is classified according to its degree of sensitivity, and the legal, physical and electronic security measures are stricter for sensitive data. Moreover, it is mandatory to declare the existence of all data files to the AEPD.

The law establishes that the data subjects must be informed explicitly, precisely and unequivocally of:

- The existence of a file or data processing, its purpose and the recipients of the information.
- Whether responding to a request for data is mandatory or optional.
- The consequences of providing or refusing to supply the required data.
- The possibility of exercising the rights of access, rectification, cancellation and opposition.
- The identity and address of the data controller or, where appropriate, their representative.

The processing of data obtained from sources other than the data subject is allowed, but the data subject must be informed explicitly, precisely and unequivocally within three months after initiation of the processing.

The LOPD grants the citizen the power to exercise the so-called ARCO rights – rights of access, rectification, cancellation and opposition.

Whereas in the previous law the period to make the rights of rectification or cancellation effective was five days, the LOPD extended this to 10 days. Moreover, with the Data Protection law it is mandatory to retain personal data for the periods specified in the relevant provisions or in the contractual relations between the party responsible for data processing and the data subject.

The law also recognizes the right of opposition, included in the EU Directive, by which any interested party may oppose the processing of their personal data whenever there are legitimate grounds relating to a specific personal situation. When this is the case, the data controller must exclude from the file the data related to the relevant data subject.

The right of access allows citizens to protect their privacy by controlling themselves how their data is used. This right is regulated under Title II of the LOPD (Article 15) and Title III of the Royal Decree 1720/2007 (Article 23 to 30). The right of access allows the data subject to access the data controller and request the following information:

- Whether the data subject’s personal data is being processed or stored (‘treated’).
- The purpose of the treatment.
• Any available information on the origin of the data and the sharing (actual or planned) with third parties.

The right of access, as well as the rest of ARCO right, is a very personal right – this means that only the data subject, or an authorised person, can exercise them. Unless the data subject has a proven legitimate purpose, the right of access can only be exercised every 12 months.

The right of access is exercised before the data controller in two ways – either by using the means established by the data controller (customer service) or by requesting it in writing with the information detailed in the Royal Decree. In all cases, the data subject should use a method that allows the data subject to prove that the request has been made and received by the data controller. If the data subject chooses to make the access request in writing, the following information should be included (forms are provided on the website of the AEPD) – data to identify the data subject or its representative (full name, copy of valid ID), information on the specific request, means chosen by the data subject to access the information (on-screen visualisation, written notification, etc.), address for notifications, data and signature, and, if necessary, documents supporting the request.

If forms are sent with missing information, the data controller has the obligation to notify this to the data subject and allow for rectification. Once received, the data controller must respond within 30 days accepting or refusing (with a reason) the request, even if no data is found. If there is no reply within the legal limit, an appeal may be lodged before the AEPD demanding the protection of the data subject’s rights.

If the access request is granted, the data controller will provide the information in writing or have 10 days to provide the information by any other means. This should include all the data held on the data subject, the data resulting from any digital treatment, information on the origin of the data, information on the data grantees, information on the specific uses and purposes that justify the data storage.

The right of access can be denied if a similar request was made less than 12 months before (unless there is a proven legitimate purpose), if there is a law or regulation preventing the data controller from releasing the requested information or when the access right is requested by someone different from the data subject with no legal status as a representative. In any case, the data controller will inform the data subject of the right to seek assistance from the AEPD. If a DPA rules that the denial was not appropriate, the data controller will have six months to respond to the access request or litigate the decision.

Spain has recently seen several controversies in relation to the ARCO rights. One of the most relevant is around the issue of the so-called ‘right to be forgotten’ or ‘right to oblivion’ [derecho al olvido]. While the Spanish DPA does not recognize the right to be forgotten as a right per se, it does recognize the possibility for individuals to demand that one’s stored information is erased if there are good grounds for it – but these must

---

5 The law provides no definition of what is a legitimate purpose, but during the fieldwork of this research, we have learnt that having been a victim of crime (or abnormal behaviour) can be considered a legitimate purpose to get access to CCTV footage, for instance.
be considered case by case\textsuperscript{6,7}. This has generated a debate around the limits of such a right, and its impact on ‘data veracity’ and the individualistic nature of a right that only exists once an individual demands it.

A specific example of this controversy is the case of Google. In 2011 the AEPD filed 90 court orders against Google at the request of individuals who wanted the search engine to remove specific links that, they felt, shed a dim and untruthful light on their past, having bad consequences in the present. This issue is linked to the ability to build – and rebuild – one’s own life.

In one of those 90 cases, the court heard arguments from both sides. Google argued that the search engine is just an intermediary platform for content, and that it is publishers that should be responsible for the content. According to the AEDP however, the original publishers cannot legally be ordered to take content down, and Google, with its cookies and continued collection of personal information, is the one violating Spanish citizens' privacy rights.\textsuperscript{8} Therefore, the AEDP concluded that Google is responsible for the elimination of links to personal information, and this can be requested directly to the search engine even if the relevant information remains in pages of third parties. In May 2014, the European Court of Justice ruled on the matter, finding that Google was indeed responsible for removing results from its search engine in certain cases despite the fact that the content itself was managed by third parties\textsuperscript{9}. The judgement appeared to underscore the so-called ‘right to be forgotten’ insofar as allowing data subjects to request that information about their past is deleted from search engine results in cases where ‘the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed’\textsuperscript{10}. The impact of this finding could be extremely wide ranging and is expected to encourage many citizens to request that search engine results are amended to ensure that information about them is removed.

The issue of the right to be forgotten continues to be controversial, however, and each case is being analysed independently. The range is wide: from the case of a school principal who was fined for urinating in the street to people who have been in jail accused of theft. In 2012 in Spain there was an increase of 80% in complaints related to the right to be forgotten in the internet.\textsuperscript{11}

\begin{itemize}
  \item \textsuperscript{6} The limits of the right to oblivion.
  \texttt{http://www.elmundo.es/elmundo/2012/02/22/navegante/1329915513.html}
  \item \textsuperscript{7} Aproximación al derecho de olvido en el nuevo reglamento de protección de datos.
  \texttt{http://publico.blogs.lexnova.es/2012/07/17/aproximacion-al-derecho-al-olvido-en-el-nuevo-reglamento-de-proteccion-de-datos/}
  \item \textsuperscript{8} In the first case of its kind, Spain takes Google to court over privacy issues.
  \texttt{http://thenextweb.com/google/2011/01/19/is-your-past-etched-in-the-internet-spain-takes-google-to-court-over-it}
  \item \textsuperscript{9} See full judgement of Case C-131/12 available at
  \item \textsuperscript{10} Press release from Case C-131/12 available at
  \item \textsuperscript{11} See full judgement of Case C-131/12 available at
\end{itemize}
National exceptions to the EU Data Protection Directive and to the right of access to data

The LOPD excludes from its scope the following files:

a) Those held by individuals in the exercise of purely personal or household activity.
b) Those subject to the regulations on the protection of classified materials.
c) Those created to investigate terrorism and organized crime. However, in these cases the data controller must previously notify the AEPD on the existence of the file, its general characteristics and purpose.

Specific files fall under regulations different from the LOPD, such as:

a) Those regulated by the electoral law.
b) Those used for statistical purposes only, covered by national or regional legislation on public statistics.
c) Those containing personal assessment reports falling under the labour law of the personnel of the Armed Forces.
d) The derivatives of the Civil Registry and the Central Registry for convicts and rebels.
e) Those containing images and sounds recorded by surveillance cameras (CCTV) operated by the police, in accordance with the legislation on the subject.

However, it is not necessary to inform the data subject about the existence of a file or the treatment of their personal data if the data has been gathered from ‘public sources’. Public sources are those files that can be accessed by anyone, not impeded by any restricting rule and where the only requirement is, in some cases, the payment of a fee. The databases that are considered public sources are, exclusively, the ‘commercial registry’,\(^\text{12}\) phone listings as established in their specific regulation, and lists of people belonging to professional groups as long as they only include name, title, profession, activity, academic degree, address and indication of their professional group. Newspapers, journals and official gazettes are also considered public sources (Art. 3 j) LOPD).

As noted above, the AEPD has a very narrow understanding of what constitutes a public source. This was exemplified when the law established that media material is a public source but the AEPD subsequently ruled that this was only valid for social media, thus altering the terminology used in the Royal Decree 1720/2007. This has caused some debate among lawyers and regulators, who argue that lower regulations should not restrict the provision of a higher regulation.

Compatibility of national legislation with Directive 95/46/EC

The Spanish Data Protection Law (LOPD) was passed in 1999 in order to comply with the Directive 95/46/EC of the European Parliament and the Council, of 24 October 1995

\(^{12}\)A registry including electoral data of all citizens made available to marketing companies.

IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
on the protection of individuals with regard to processing of personal data and on the free movement of such data, which at that time had to be considered directly applicable into Spanish law.

In general terms, the LOPD fits the criteria and definitions of the EU Directive. However, there are some differences that need to be taken into account. Art. 10.2.b) of the Royal Decree 1720/2007 was derogated after the Supreme Court (8/02/2012 STS) acknowledged a ruling by the European Court of Justice (24/11/2011). This was the consequence of an appeal by ASNEF (National Association of Financial Credit Institutions) and FECEMD (Spanish Federation of E-Commerce and Direct Marketing), claiming that the LOPD did not comply with the EU Directive (it was more restrictive in the Spanish legal framework) and thus this was detrimental to their interests. The Supreme Court ruled in favour of the plaintiff and established that all sharing of data obtained from non-public sources required explicit prior consent by the data subjects. Following this ruling, data sharing of debtors’ data to communication companies can be done even when they are not in public databases. In addition, explicit consent of the creditor is not needed. This dictamen seriously affects the right of privacy, particular for vulnerable individuals that, for some reason, have economic disagreements with a company. Simply put, the right of a private company to pursue debtors is given greater protection than the right of privacy of a citizen.

Another controversial case has been CCTV and the EU Directive on services in the internal market. This represents a clear example of national and supranational disparities and lack of consensus, as the adaptation of the EU Directive to the Spanish legal framework has resulted in less legal control on private CCTV devices. Spain has a clear imbalance between public and private CCTV regulations, in the sense that while public CCTV systems are highly regulated, private CCTV schemes are only subject to a minor data protection directive. Therefore, it has been argued elsewhere that a greater control of private schemes would be desirable, even if just to avoid the grey areas that emerge in such an imbalanced context. However, the Spanish ‘Omnibus law’ that adapts the Bolkerstein Directive established the “exclusion of companies related to technical equipments of security. The lenders of services (services providers) or the subsidiaries of the companies of private security that they sell, deliver, install or support technical equipments of security, providing that they do not include the provision of services of connection with head offices of alarm, they remain excluded from the legislation of private security”.

This appears to mean that the already fragile private regulation of CCTV will not have limits and damages any hope of achieving equilibrium between public and private regulation. In theory, anyone will be free to install CCTV and capture footage of other citizens without their permission or assent.

13 Mendoza, Ana Isabel (2011): Deudas de telecomunicaciones y registros de morosos. [], working progress that can be downloaded at https://www.uclm.es/centro/cesco/pdf/trabajos/7/2011/7-2011-5.pdf (last access: 30 April 2014). This paper is from the Centre for Consumption Studies.
Surveillance and access rights: codes of practice at national level. (CCTV and credit rating)

Exercising access rights for CCTV and credit ratings in Spain is identical to processing access requests for any other surveillance or data-mining practice and described in Section Two above. However, this presents some practical problems in the case of CCTV, which need to be addressed specifically.

The legal framework for CCTV is established both in the Data Protection Law as in an ‘Instruction’ drafted by the DPA in 2006 (I/2006). According to this Instruction, in all areas under surveillance there will be at least one sign located in a visible place, both in public access areas, private areas and inside buildings. Also, the entity responsible for the device will have forms explaining Article 5.1 of the Organic Law 15/1999, which reads:

“The persons to whom personal data is requested should be previously, explicitly, precisely and unequivocally informed of:

a) The existence of a file or processing of personal data, the purpose of the data collection and the recipients of the information.

b) Any questions regarding the data file and / or processing that the data subject can undergo (either mandatory or optional nature)

c) The consequences of obtaining data or the refusal to provide them.

d) The possibility of exercising the rights of access, rectification, cancellation and opposition.

e) The identity and address of the controller or, where appropriate, their representative.

When the controller is not established in the territory of the European Union but uses in the data processing means located in Spanish territory and for means that go beyond the bureaucratic processing of the data, appoint a representative in Spain, notwithstanding the actions that could be initiated against the data processor.”

Exercising ARCO rights in the case of CCTV has some peculiarities which have been acknowledged by the DPA. The right of rectification is ‘not possible due to the nature of the data – images taken in actual life that reflect an objective fact.’\(^\text{16}\) The right of opposition also presents difficulties, as if one was to oppose to his/her image being taken, this could be seen as posing a security threat and the right would have to be overridden.\(^\text{17}\) The fact that in most cases an image will contain personal information from more than one data subject means that the data controller would be releasing personal information from third parties to the requested, and so it is accepted that the data controller provides a text indicating what images have been captured (entrance and exit from building, for instance) instead of the actual file.

Moreover, when processing an access request form, it should include an updated image of the person making the request, so that the data controller can identify him/her and


\(^{17}\)Idem. Pg. 42.
certify that his/her image has been captured by CCTV. Some experts have highlighted the fact that in the case of CCTV exercising access rights requires the release of personal data to the data controller that the data controller would not have had access to otherwise.\textsuperscript{18}

Another contradiction that some have raised concerns the 30-day period provided by the law for the data controller to respond to an access request, as this coincides with the maximum time allowed by law to keep CCTV images, thus rendering useless the right to access one’s personal data. When this is the case, the AEPD has ruled that the data controller should only notify the data subject of the fact that the data has been deleted.\textsuperscript{19}

Finally, it is worth noting that in some sites (banks and credit institutions); the Private Security Law\textsuperscript{20} denies all ARCO rights when it establishes that ‘recorded images (…) will only be available to the judicial authorities and law enforcement bodies’. This contradiction and non-compliance with the Data Protection Law has not yet been addressed.

As for credit scoring, centralized credit rankings do not constitute the main piece of information determining whether one is given a loan or service in Spain. Banks make individual risk assessments based on people’s income tax and a recent pay slip, as well as a quick check of the property registry. Additionally, they may check a database such as the privately-owned Equifax, Experian or CIRBE, the public registry dependent on the Banco de España, where people’s outstanding debts are registered.

These databases are covered by Article 29 of the Data Protection law, where they are generally described as ‘solvency registries’. The law mainly addresses the possibility that the information kept in these registries is not accurate. The information included in such registries can only be provided by the creditor, who must be able to prove at any time that the debt has not been challenged in court, that the debtor has been notified about the existence of the outstanding debt and that no more than six years have passed since the debt was accrued.

If the debtor is able to provide any document questioning the accuracy of the personal data kept in such files, the data controller will have to proceed to the precautionary cancellation of the data.

The promotion of access rights by DPAs and national authorities and their role in ensuring compliance to national norms

The Spanish Data Protection Agency (\textit{Agencia Española de Protección de Datos}, AEPD, in Spanish) was created in 1993 and is the control body responsible for the fulfilment of the Spanish Organic Law of Personal Data Protection. It has its headquarters in Madrid and its scope of action comprises the whole country. It is a body of public law with its own legal status and full public and private capacity that act

\textsuperscript{18}http://www.privacidadlogica.es/2013/05/13/existen-los-derechos-arco-en-videovigilancia/

\textsuperscript{19}It can be found following this link: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2007-0252_Cuestiones-Generales-de-videovigilancia-y-ejercicio-de-derechos.pdf

\textsuperscript{20}Article 120.1
independently of the public administration in the exercise of its functions. AEPD oversees the compliance with data protection legislation by people in charge of files that include personal data (public entities, private companies and other organisations). Due to the decentralised natures of the Spanish state, there are also regional DPAs. The Spanish DPA’s main function is to oversee and control the implementation of the legal framework regarding data protection, especially in relation to the rights of information, access, rectification, opposition and cancellation of personal information gathered by any authority, private body or individual. In order to do so, the Agency can issue sanctions and authorizations as stated in the legal framework, to establish measures of correction when a breach of rights is detected, to determine the unlawfulness of specific data-gathering processes and procedures, to provide information and to authorize the international transfer of information. Faced with specific demands by Spanish citizens, the Spanish DPA must provide any information required, to inform of the rights recognized, to attend all claims and complaints and to promote the dissemination of the activities of the agency and data protection issues in general.

**Role of national DPAs in ensuring that data controllers allow citizens to exercise their access rights**

In Spain, the DPAs provide forms to process access requests and provide assistance if the data subject is not granted access to his/her data in the 30 days established by law. When this happens, data subjects can approach their DPA and a new request can be processed directly through them. Besides the standardised forms, the website of the AEPD also provides a specific form to access Schengen data.

Since 2002 the AEPD also provides annual reports presenting overviews of rights requests and other consultations. The amount of ARCO rights requests deserves attention due to its evolution and progress. The right of Cancellation is the most frequently used, accounting for half of requests almost every year and remaining stable over the last decade. The most notable trend points to a steady decline for the rights of Access and Rectification, while the right of Opposition shows an increase. Since 2007, almost the 80% of consultations are related to Cancellation and Opposition, perhaps indicating that Spanish citizens are more interested in opposing the processing of their data than seeing which of their data exactly is being collected.

Most of these reports present a special section attending the protection of rights procedure [Procedimientos de tutela de Derechos]. It assumes the existence of a possible breach of the Act other than establishing infringement, which justifies the arbitral role of the AEPD. Two relevant examples are provided. Firstly, five years ago some abortion clinics were investigated under the premise of patients’ quality of care. The AEPD established that anonymity of women should be preserved unless they provide explicit consent. The second example of the AEPD’s mediation is related to religious freedom. Under apostasy requests the Catholic Church in Spain plead that

---

21 Agencia Española de Protección de Datos. www.agdp.es.
22 Autoritat Catalana de Protecció de Dades. www.apd.cat.
23 All forms and information can be found here: http://www.aepd.es/portalwebAGPD/canalicudadano/denunciasciudadano/derecho_acceso_den/indexides-idphp.php

IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
cancelling membership is not possible for reasons of historical heritage. Facing this argument, the AEPD ruled that instead of modifying the archives, a marginal notation should indicate that someone who was once baptized has expressed his or her desire to no longer belong to the institution.
LOCATING THE DATA CONTROLLER IN SPAIN

Introduction

This country profile summary concerns the experiences encountered whilst attempting to locate data controller contact details whilst researching 30 Spain-based sites. The examples below are illustrative of the individual researcher’s experiences and do not claim to reflect the practices of all data controllers in Spain.

Methodological thoughts

The sampling for this phase of research is made up of the type of personal data which may be captured about a lay person as they go about their everyday life. As such, nine domains were established which were: health; transport/holidays; work; education; finances; leisure; communications; consumerism; civic engagement. Within these domains, specific research sites were identified depending on the individual country. The sampling strategy envisaged was divided in three ways: firstly, researchers would pick the site located geographically closest to their place of work (i.e.: the school located closest to their place of work). If this did not apply, researchers would secondly pick the site they would usually use (i.e.: the search engine they would usually use). Finally, if this did not apply, researchers would thirdly pick the national market leader (i.e.: the insurance provider national market leader).

In the case of CCTV systems, the mandatory signage should have meant that we would be able to locate the data controller without speaking to any members of staff in person. However, we found that we did need to speak to staff as 1) We could not initially locate the signage for CCTV in a transport setting, as we chose a large station and the signage was posted just before entering the site; 2) The CCTV cameras we found in the city centre had no signage at all; 3) The small store we chose had a sign without details. Only in the case of the large supermarket and bank were we able to find the data controller details without assistance. In the case of CCTV and ANPR, pictures have been taken of all the relevant sites, and some are included in the report.

Data controller details were most often located online through individual organisations’ official websites, and links to the relevant URLs are provided below. In the cases where the websites were not useful to locate the data controller details, the phone was often used. Our experience was that when we spoke to members of staff on the telephone, a general lack of expertise about data protection and access rights was evident. These conversations proved difficult due to the systematic suspicion of respondents who appeared sceptical that we wished to access our personal data simply because we were curious. In several cases, many phone calls were needed as we often encountered suspicion of members of staff who were unsatisfied that our ‘curiosity’ was sufficient to allow access to our personal data.

<p>| Contact details identified via official website | 15 of 30 cases |
| Contact details identified after speaking to member of staff on phone | 11 of 30 cases |</p>
<table>
<thead>
<tr>
<th>Contact details identified after speaking to member of staff in person</th>
<th>4 of 30 cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>No data controller identified</td>
<td>6 of 30 cases</td>
</tr>
</tbody>
</table>

This phase of the research took place in June and July 2013 and was conducted by one researcher, but access requests were sent using the personal details of three people in order to cover as many of the sites as possible. This report counts with 24 successful\(^\text{25}\) cases.

**Public**

**Good practice**

*Membership to political organization*

Information on how to exercise access rights was found after two clicks on the corporate website, though the ‘legal notice’ link. The process was straightforward and the information provided was very general but clear. A postal address and e-mail was provided, and we were therefore successful in locating the data controller’s contact details.

**Bad Practice**

*Nationally-held patient health records*

Spain has a universal public health system, and so all health institutions are ultimately dependant on the government. Therefore, for this case the website of the regional institution was explored first. After a few clicks, a tab called ‘rights and obligations’ led us to a list of rights which included ‘the right of the user to access information relating to his/her medical record’. Surprisingly, however, in the three paragraphs detailing who can access medical records and who is supposed to store them, a name or address for a data controller was not found. The phone was then chosen as a second option, and after speaking to two people, a general address was provided. So while we were ultimately able to locate the data controller, it was necessary for us to call. In effect then, the insufficiency of the online content forced us to phone the organisation and speak to two different people before obtaining the data controller information. This lack of transparency of information appears to put the onus on the citizen to pro-actively dig out data controller information and may be termed a strategy of denial. This is the case because the ability of a citizen to exercise his/her rights is restricted by the fact that he/she must make some concerted effort simply to locate the contact details to whom he/she should make an access request.

*Locally-held patient health records*

The local clinic was approached by exploring the website, which did not include any mention on data handling or access rights. The furthest we managed to go using the

---

\(^{25}\) We include here the cases of CCTV in a bank and a public space, where we only located the data controller details through the DPA or by submitting a formal complaint. It was thus impossible to identify the data controller via the required CCTV signage.

IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
website was falling back on the general public health agency’s website. In the end, the phone was chosen. After speaking to two people, the ID number of the researcher was requested and written down, as well as a phone number. The person answering the call promised that someone would call back with an indication of what to do to locate the data controller. After two weeks, no reply had been received so the process was repeated and after being put on hold for several minutes, a person who didn’t understand the request provided us with the name of the director of the institution, and their general address. As an interesting note, the person answering the phone mentioned that ‘data files’ did not exist as everything was done electronically. Similarly to the example above, while we were eventually able to obtain details of the data controller, this was only the case having had to telephone the organisation following the lack of information online. Having been advised that we would receive a return phone call, our request was ignored and it was only after our second telephone call that we finally obtained requested the information.

Driving license records

No information was found on the website of the public agency and no contact phone number was located. A Madrid-based press contact was found on an unrelated press release, and this proved to be a good source. While they don’t handle the data and were not sure what the procedure was (they suggested a visit in person to the Barcelona-based delegation to make a written request and so that they could certify that we weren’t asking for our data ‘just out of curiosity’), they gave us a direct phone number. The person who answered the phone offered to give us ‘yes’ or ‘no’ answers on our personal data through the phone by checking their website. When we stressed that we wanted to formally process an access request, we were offered the general e-mail of the service. Here once more, we eventually received the details we had asked for but only after a process of negotiation with the representative of the organisation. This reinforces the notion of a strategy of denial insofar as data controller contact details are ‘buried’ behind several layers of denial (i.e.: absence of information online; no contact details available online; refusal of representative on the phone to answer our query directly).

Border control

No information was found on the website of the interior ministry and no contact phone number was located. However, in this case the Spanish DPA provides a specific template with an address at the Ministry of the Interior to access Schengen-related data. This template is provided as an example of the data needed to exercise the access right. There is any special reason or law for what they provide the form for this type of data.

Passport service & ID cards

Both passports and IDs are issued by the Ministry of the Interior. No information was found on the website and no contact phone number was located. In this case, none of the leads found on the website were useful, and all phone calls led to dead-ends. In the end, the DPA was approached, which suggested the access request is sent to a general

26http://www.agpd.es/portalwebAGPD/canalciudadano/denunciasciudadano/derecho_schengen_den/common/DERECHO_DE_ACCESO_Schengen_Es.pdf

IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
address of the Ministry or any police station. This seems to be extremely bad practice – one must firstly consider the sheer coverage of this type of data as passport and ID cards are held by most Spanish citizens. Given the breadth of this coverage, the absence of any data protection/privacy related content online and the lack of contact details can only be described as extremely poor practice.

Locally-held secondary school records

School records are not kept locally or centrally – or so have we been told by the Ministry of Education (national) and Department of Education (regional). Some relevant data is gathered for statistical purposes, but is always anonymised and so personal data files are not kept. Therefore, we approached individual primary and secondary schools (see below for our discussion of the (private) primary school).

The secondary school approached was a public school (government-funded). Again, the website did not provide any information on data gathering or access rights, and a legal notice was absent. We chose to use the phone as a second option, and after speaking to several people (who didn’t understand the request) we were directed to the Head of Studies. The Head of Studies suggested that we visit the site in person, but finally agreed to discuss the matter with the Director and requested our name and phone number to return the call. A few hours later we received a phone call from the Director, who reluctantly agreed to provide us with an e-mail address. The unwillingness to provide the information was accompanied by several questions about the nature of the requests and its aim. The denial strategy came along with evident ignorance about the right exercise and came along with Director’s attitudes of annoyance and irritation.

Electoral roll/register

The website of the superior entity of the Spanish electoral administration provided no information on personal data gathering and processing, so we chose to use the phone. The central Madrid office informed us that personal info was kept at the local level, and so we needed to contact our local census office, and provided us with a number. The second person we spoke to initially told us that our data was confidential and that we could not have access to it. When we mentioned the guarantees of the Spanish Data Protection law, the same person insisted that the data they kept was data provided to them by town halls, and so that we should contact our local city council. Again, we mentioned that we wanted to exercise our access rights before the electoral registry and not the town hall. In the end, and after several attempts to avoid the loop in the same conversation at making us give up, we were given the general address of our local census office. Here again, we underwent a negotiation process during which the representative of the data controller attempted to refuse to answer our query. Taken together with the lack of information online, the approach employed by this organisation is yet another example of bad practice particularly with regards to the lack of transparency.

Europol

The first step was exploring the Europol website looking for dedicated information on data protection and/or a Spanish representative body. After five clicks, we reached a page entitled ‘Management and Control’ and downloaded a report called ‘Data
Protection at Europol’ which on page 32, point 6.2 includes a section on ‘The Joint Supervisory Body’ and its national counterparts. While the section made some general remarks, there was no specific information on who to address regarding data gathering and processing at the EU or national level.

Our second option was to use a general search engine which produced a website in Spanish of the ‘Autoridad Común de Control de Europol’ mentioned in the booklet. Under the heading ‘Your rights’, we accessed a section dedicated to ARCO rights where the ‘National Competent Authorities’ was listed. Interestingly, the information in Spain included a postal address and fax number for Europol Spain, but the e-mail and website provided were the general contact details for the Spanish Data Protection Agency. Interpol’s website therefore lacks clarity in terms of outlining to citizens how and to whom they should make a subject access request. This ambiguity, whether deliberate or not, represents a strategy of denial since the citizen is forced to either search elsewhere for this information, or simply give up his/her attempts to access her/her personal data.

Police record

Police records (‘antecedentespenales’ in Spanish) are relatively easy to request as several administrative processes request that the citizen provides a form stating that one does not have a police record. Since initially we did not look for ‘antecedentespenales’ but a thorough police record, the search took a bit longer than expected. Once we realized what we were looking for, accessing the specific information on the website was relatively easy and under a page entitled ‘Forms’, and a template was provided. Locating this content took 10 clicks but the general quality and depth of information about personal data is lacking and there is no explanation of exactly what type of data the organisation routinely collects and stores. Moreover, it is unclear whether following a request, a citizen just gets a statement saying that they do not have a police record, or if an access request will provide further information.

Private

Good Practice

Locally-held primary school records

The primary school we approached is a private school (privately funded by parents). No information on data handling was found on the website, and the legal notice, which had proven useful in other cases, was disabled. We decided to call the school directly, and, having being asked to provide our name, we were given the e-mail address of the school’s manager. Generally speaking then, whilst the information was not available online, we were able to obtain the required information relatively easily and avoided the lengthy process of negotiation experienced in several other sites. While this organisation did not display best practice then, it may be said to have displayed relatively good practice.

Banking records

Information on how to exercise access rights was found after two clicks on the corporate website, though the ‘legal notice’ link. The process was straightforward and while the

---


IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
legal jargon was difficult to understand and the information on the kind of data that is gathered and who it is shared with was not too clear, the website included some level of detail on this matter. A postal address and an e-mail address were provided and we therefore successfully located the data controller’s contact details. As a result of the transparency and accessibility of data controller contact details, the bank’s approach is found to have demonstrated good practice.

**Insurance records**

Similarly to the approach of the above site, information on how to exercise access rights was found after three clicks on the corporate website, through a specific ‘Data Protection’ tab. The process was straightforward and while the legal jargon was difficult to understand, the information on the kind of data that is gathered and who it is shared with was very detailed. A postal address and an e-mail address were provided, and we therefore successfully located the data controller’s contact details. As above then, this was deemed an example of good practice.

**Credit reference checks/rating**

In this case, the most difficult part was identifying where to start the research to access our credit ratings. After some online searches, a ‘Central de Información de Riesgos’ (CIRBE) dependant on the bank was identified as the main national registry for credit checks. Their website was located through a quick search and, three clicks later and using their search function, a page dedicated to requesting one’s personal risk assessment was located.

It is worth noting, however, that in this case we are not talking about a regular access request procedure. The bank seems to have specific legislation regarding such risk assessments, and requests are answered within 10 days (less that then 30+10-day period established by the Data Protection law).

After conducting an interview with a bank worker, other databases commonly used by Spanish banks were identified. We concluded that centralized credit rankings do not constitute the main piece of information determining whether one is given a loan or service in Spain. Banks make individual risk assessments based on people’s income tax and a recent pay slip, as well as a quick check of the property registry. Additionally, they may check a database such as EQUITAX or EXPERIAN (as well as CIRBE). Finding the data controller was very different in these cases. EQUITAX mentions the right of access in its main page on the website, and highlights how after January 1st they do not require a visit in person in order to exercise data protection rights. Access is online and immediate if one has a letter with a reference number (proof that one has been included in their database as a defaulter). Otherwise, a letter can be sent to an e-mail, fax or PO address (this option is not mentioned explicitly, but the data is offered to exercise the rights of rectification and cancellation)\(^\text{28}\). This therefore appears to be good practice insofar as the information detailing how to make a subject access request is not only easily accessible but it is also very detailed and clear.

EXPERIAN, on the other hand, seems to be completely oblivious of data protection legislation and only mentions data protection for those who send CVs or fill out forms

\(^{28}\)https://www.equifax.es/ederechos/ederechos.html
in their website. A search for the word ‘access’ in their website, however, led to a template and an address. As a result, EXPERIAN’s approach to enabling citizens to exercise their informational rights is mixed – the level of information on their website is relatively poor (especially in comparison to EQUITAX) but our use of their search function led to us locating not only the address of the data controller but also a template with which to make our request. Moreover, from a purely practical perspective, our search also demonstrates that the website’s search function is effective and does not simply produce several pages of irrelevant content with the relevant data ‘buried’ under non-useful information. So there are some elements of good practice in this case.

Membership to leisure time/sports clubs

Information on how to exercise access rights was found after two clicks on the corporate website, though the ‘Legal Notice’ link. The process was straightforward and while the information on the kind of data that is gathered and who it is shared with was not too clear, the website included some level of detail on this matter. A postal address and an e-mail address were provided, and we therefore successfully located the data controller’s contact details. As a side note, there was an issue of ambiguity in this case as a general paragraph on Data Protection legislation access rights was included under the heading ‘Personal data of the website user’. It was thus unclear whether the access information was related to the general business or only online use of the website.

Internet service provider & mobile phone data

Information on how to exercise access rights was found after two clicks on the corporate website, though the ‘Legal Notice’ link, under the heading ‘Privacy and Data Protection’. The process was straightforward and the information on the kind of data that is gathered and who it is shared with was clear. A postal address and an e-mail address were provided, and we therefore successfully located the data controller’s contact details. Once more then, this demonstrated clear good practice and the company appear to employ a strategy of facilitation with regards to enabling citizens to exercise their informational rights.

Worth noting is the fact that, according to the company’s website, the cancellation of one’s personal data is only possible three months after the cancellation of the service.

Loyalty card scheme for a national supermarket

Information on how to exercise access rights was found after two clicks on the corporate website, though the ‘Legal Notice’ link. The process was straightforward and while the information on the kind of data that is gathered and who it is shared with was not too clear, the website included some level of detail on this matter. A postal address, a phone number and a link to a general ‘customer service’ form including a drop-down menu with a tab for ‘Data Cancellation’ were clear and visible under the heading ‘Data protection & Privacy’ in the ‘Legal Notice’ section.

However, this section kept making reference to the data gathered through the ‘website’, even if later other data that cannot be gathered through the website was also mentioned. As we had found in other sites, it was unclear whether the access information was

29 www.experian.es/assets/legal/white-papers/acceso-badexcug.pdf
IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
related to the general business or only online use of the website. We expect to find out once we receive a reply to our access request, and will submit a second form if necessary.

Loyalty card scheme for coffee chain (or similar)

Information on how to exercise access rights was found after two clicks on the corporate website, though the ‘legal notice’ link. The process was straightforward and while the information on the kind of data that is gathered and who it is shared with was not too clear, the website included some level of detail on this matter. A postal address was provided, and we therefore successfully located the data controller’s contact details.

As in the examples above, in this case, a general paragraph on Data Protection legislation access rights was included under the heading ‘Personal data of the website user’, thus making it unclear whether the access information was related to the general business or only online use of the website.

Bad Practice

\textit{ANPR}^{30}

We found neither signage nor personnel on site. A picture has been taken of the cameras (ANPR and CCTV) (see Picture 1 below), but no other means of contact was found. A phone number was finally located in the yellow pages, and after speaking to two members of staff, the general address of the parking lot was provided. The person at the other end of the line, after asking for the motive of the request and insisting on knowing whether we had found that something was wrong with the parking lot or what our relationship to the business was, informed us that the letter would be forwarded to a lawyer. In this case then, the complete absence of signage as well as any personnel on site restricted our ability to locate data controller details. Having being ‘forced’ to attempt to find this information another way, the representative who answered our phone call asked several questions before finally answering our query. Taken together, these factors represent poor practice by this private organisation given the general lack of transparency and willingness to impart what should (in theory) be openly accessibly information.

---

\textsuperscript{30}Unlike other country reports featuring ANPR in a law enforcement capacity, the ANPR site visited in this context was for parking enforcement in a private accommodation complex.
Human resources/personnel file at your place of work

After unsuccessfully trying to locate the details in the workplace’s intranet, the human resources department was contacted by phone. Three different people answered the phone, and all insisted that all our data was available via the university’s website. After insisting that we had a right to access our data, we were promised someone would call us back. A couple of days later we received an e-mail stating that all our data could be accessed and modified using the intranet system, and that our data would be shared in compliance with the law and the consent form all workers sign when joining the institution. A copy of this form signed by the researcher was attached. In response, we sent a link to the DPA’s website explaining what access rights are and that we needed to identify a data controller. Following this, our request was forwarded to the ‘Head of Technologies’, who volunteered his name and e-mail address to handle the request. In a similar manner experienced in many of the public sites and the private site above, we were once again required to negotiate with the representatives of this organisation in order to finally receive the answer to our query. The recurring failure in this case to answer our question directly and indeed correctly necessitated repeated phone call/emails in order to receive an answer to a relatively simple request. It is unclear whether this failure to answer was the result of a deliberate denial of our rights or whether it was simply the result of a lack of understanding of our request due to little data protection procedural knowledge.

Facebook

No data controller details found on the website. Report and expanded report on data kept available from personal settings. Non-compliance with Spanish law, so we suggest a request via the DPA is processed.

Email data - Gmail

Settings section describes info kept in detail, but no contact address or e-mail is provided. As we mentioned in the case of Facebook, we suggest this is processed via the Spanish DPA.
Search engine

The level of information regarding how personal data is gathered and shared was probably the most extensive in this site in comparison to all other sites in this report. The website had an easy to find privacy tab and a thorough description of privacy issues. However, a contact address is only provided for the U.S. Therefore, questions remain over how a subject access request originating from Spain would be processed if sent to a U.S. address. This leads to ambiguity for the citizens in terms of how to access their personal data. As we mentioned in the case of Facebook and Gmail, we suggest this is processed via the Spanish DPA.

CCTV and signage

CCTV in a transport setting

The signage in this site was found with assistance from a member of staff onsite as it was located in access to the transport hall. The signage was in full compliance with Spanish data protection law and included a full postal address for enquiries to the data controllers.

![CCTV camera in metro station](Image)

*Picture 2: CCTV camera in metro station*
No signage was present and the office was closed on our first visit. We visited in person and were asked to leave our details (name and telephone number, and whether we were lived in the area), but one week later no one had contacted us. We then chose to access the District Office were the cameras are located by phone, but found out there is no direct number and were left with no alternative than to call a special 010 (paying) number. Our first call was terminated when the operator was transferring us to a second agent. On our second phone call we were informed that no information was available and were encouraged to submit two complains (one for the lack of signage and one requesting the details of the data controller). We did as instructed and at the time of writing have received no reply. Taken together, this organisation appears to demonstrate very poor practice. The lack of signage is an evident error and the lack of information we were able to obtain from the various representatives of the organisation we spoke to meant that we were ultimately unable to locate the data controller contact details.
CCTV in a large supermarket/department store

The signage in this site was very clear and easy to locate. The content of this signage was in full compliance with Spanish data protection legislation and included full contact details for the detail controller. However, we also found that there was no signage for the external camera located at the entrance to the store used by staff. Therefore the store was in non-compliance of data protection law with regards to its failure to include signage in all CCTV camera locations.
During our visit to this site, we quickly located a CCTV sign. However, as per the pictures below, this signage was a blank template without contact details. Having enquired about this to this shop owner, he proceeded to fill out the template sign following our request and thus we were able to obtain the data controller contact details.
Picture 7: CCTV camera in local store

Pictures 8 & 9: CCTV signage before and after completion by store employee (detailed entered are blurred in picture)
**CCTV in a bank**

We found no signage when attending on site and the bank closed when visited. As a result, we chose to contact the branch by phone and were asked to leave our name and number. A few days later we were contacted by a bank teller, who informed us that we have no access rights as these can only be exercised by the police. We questioned this information, but the teller was just telling us the information received by the bank’s security services. We contacted the Catalan DPA by phone to receive guidance and were advised to send an access request form to the branch’s address.

**Concluding remarks**

Some general impressions can be put forward as a preliminary analysis. For this phase the sample has consisted of 30 sites and 24 successful cases. As a starting point, the following table provides information about the difficulty of identifying data controllers:

| Data controller contact details successfully identified in first round of visits | 10 of 30 cases (33.3%) |
| Data controller contact details unable to identify in first round of visits | 14 of 30 cases (46.7%) |
| Data controller contact details not identified at any point | 6 of 30 cases (20%) |

Only in one out of three cases was it enough to conduct just one visit in order to successfully obtain data controller contact details. In almost a half of the sample (46.7%), a second round of attempts was necessary to identify data controllers, and finally an 80% success rate was reached (24 successful cases of 30 in total). Successful cases are those sites for which a contact has been obtained, although the contact may be or not the data controller specifically. Not always finding an identified and known data controller but at least a contact has been provided towards whom address the correspondence.

Focusing upon strategies used by data controllers to either facilitate or deny citizen’s access rights, when approaching the staff of the site or by phone, a general lack of expertise about data protection and access rights was evident. Online exploration has been the most successful source as most of the first-round identifications have been achieved through this virtual approach, with the remaining phone and on-site visits generally unhelpful. Direct intercourses have highlighted the general lack of awareness about citizen’s access right along with (in some cases) complete ignorance of relevant procedures. Despite the fact that websites are a good source, we uncovered some ambiguity. In some cases, it remains unclear whether the access information is related to the general business or only online use of the website (related to cookies and navigation-related information).

The private sector is where good practices are concentrated. Large corporations are the most efficient agents with regards to providing information on data controllers and strategies of facilitation are predominant in these sites. Still in the private sector but referring to small companies, we found mixed situations, mostly good and reasonable but also poor and bad practices to a lesser extent. In the public sector one can state the prevalence of bad practices, both in terms of guidance on data controllers and denial strategies as well, accompanied by generalized attitudes of suspicion. Figure 1 shows the comparison between public and private sectors, differentiating large and small businesses for the latter:

IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
In the case of CCTV sites, irregularities were found with the signage due to poor location and invisibility, no signage at all or signage without data controller details. Only in two out of five sites was signage found with good compliance with the Spanish law.

The concluding remark is that compliance with law is not the general scenario. Those who are more compliant are the large corporations in first place and the private sector in general in second position. What is undeniable is that public administration and public institutions in Spain are the less efficient and the less compliant with the law. This is associated with frequent use of denial strategies and reluctances.
SUBMITTING ACCESS REQUESTS IN SPAIN

Introduction

This country profile depicts the experiences of researchers in real fieldwork requesting access to personal data to 21 Spain-based sites. The cases are outlined in detail below and cannot be considered as representative of all data controllers in Spain. Nevertheless, they are representative of a number of sites and domains in which Spanish data subjects may expect to encounter data controllers on a systematic and habitual basis.

Overall Summary

It is difficult to depict a general image since responses from data controllers are uneven with some being far from clear, direct and complete in most cases. While we have been able to successfully close a few cases, for others, we found ourselves involved in a “never ending story”. By this we mean that after our second letter, still we are provided with ambiguous or incomplete information (basically related to automatic decision process and data sharing with third parties).

<table>
<thead>
<tr>
<th>Public/Private</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Public</td>
<td>CCTV in an open street</td>
</tr>
<tr>
<td>2 Public</td>
<td>CCTV in a transport setting</td>
</tr>
<tr>
<td>3 Public</td>
<td>CCTV in a government building</td>
</tr>
<tr>
<td>4 Private</td>
<td>CCTV in a stadium</td>
</tr>
<tr>
<td>5 Private</td>
<td>CCTV in a large department store</td>
</tr>
<tr>
<td>6 Private</td>
<td>CCTV in a bank</td>
</tr>
<tr>
<td>7 Public</td>
<td>Vehicle licensing</td>
</tr>
<tr>
<td>8 Public</td>
<td>Police criminal record</td>
</tr>
<tr>
<td>9 Public</td>
<td>Europol</td>
</tr>
<tr>
<td>10 Public</td>
<td>Border Control</td>
</tr>
</tbody>
</table>

A further 14 requests were sent as part of the CCTV side study.
<table>
<thead>
<tr>
<th>Public/Private</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Private ANPR</td>
</tr>
<tr>
<td>12</td>
<td>Private Loyalty card (food store)</td>
</tr>
<tr>
<td>13</td>
<td>Private Loyalty card (supermarket)</td>
</tr>
<tr>
<td>14</td>
<td>Private Mobile phone carrier</td>
</tr>
<tr>
<td>15</td>
<td>Private Banking records</td>
</tr>
<tr>
<td>16</td>
<td>Private Advanced passenger information</td>
</tr>
<tr>
<td>17</td>
<td>Private Facebook</td>
</tr>
<tr>
<td>18</td>
<td>Private Amazon</td>
</tr>
<tr>
<td>19</td>
<td>Private Microsoft</td>
</tr>
<tr>
<td>20</td>
<td>Private Google</td>
</tr>
<tr>
<td>21</td>
<td>Private Twitter</td>
</tr>
</tbody>
</table>

**Methodological thoughts**

First to data controllers approaches were mainly sent by registered letter (see explanation of the Spanish postal system below) accompanied by a copy of our ID card. Our requests consisted of three basic questions:

1. What data do they hold about us?
2. How is this processed? – Automatic decision making
3. Who do they share it with?

Furthermore, for CCTV sites, we send each data controller the written request, a copy of our ID card and a current image of the requester. Spanish law establishes that signage must be displayed in a visible location (within a surrounding area of 500m) and it has to be readable. Such signage might mention the relevant legislation, express explicitly that an area is under CCTV surveillance and state the name of the data controller. In cases where footage is
recorded, it is a requirement to include an address or other form of contact in order to enable citizens to exercise their informational rights.

When sending our requests, we used a postal tracking system in order to ensure that we could monitor the receipt of our requests. In Spain, sending a certified letter means that the document is given a code and it can be tracked. Alongside this, an acknowledgement of receipt can be attached to the letter which provides the sender with irrefutable proof that the recipient (or someone on behalf of the recipient) has collected the correspondence. Thus, these are two methods of tracking documents: with the certified mode we can know whether the letter has been delivered or not, and with the acknowledgement of receipt we can now that it has been collected, on which date and by whom. Letters including both options are delivered by hand. In case the recipient is absent, he or she will be left with a notice in the mailbox stating at which local postal office they can collect the correspondence and which is the maximum term in which they can collect this (this can be 7 or 15 days, depending on the urgency of the situation). After this period, when documents are not collected, these are returned to the sender by the post office. It is also worth noting that the cost of sending letters using this system is 4.5 euros, denoting the financial burden the requester must bear in order to know for sure whether a letter has been received by a data controller.

A note may be made here regarding the number of interactions we had with data controllers when they failed to respond to our requests adequately. Given the timeframe of the research, it was agreed in conjunction with the project leaders that a complaint to our national DPA should be submitted in cases where unsatisfactory/non-legally complaint responses are received after two sets of correspondences are exchanged between the requester and the data controller. Since we are of course restrained by time in this project, it is unlikely our complaints will be resolved before the end of the study. However, the submission of a complaint at least provides a sort of 'closed loop' insofar as a complaint to the DPA represents a last resort which denotes poor practice on behalf of the data controller.

If we have sent several correspondences to a data controller and we were making no progress, then we have proceeded to an official complaint. However, in those cases we felt that we might receive a satisfactory answer after some negotiation, we proceeded with these negotiations and did not send complaints to the DPA.

The report distinguishes between good (or facilitative) practices and bad (or restrictive) practices. Good practices involve those sites that present a facilitative process, requiring relatively low effort on behalf of the citizens. On the contrary, bad practices are those cases with restrictive characteristics. The range for this complicated process is wide and there are different levels of bad practices in terms of legal compliance. When we found at least one substantial barrier (a denial strategy that could lead to a lay person abandoning their request), the site is considered as an example of bad practices, in terms of discouraging people from exercising their informational rights.

General overview and emerging trends

Requesting access to personal data in Spain is generally not as easy and straightforward a process as it perhaps should be. In terms of facilitative/restrictive practices one can observe different trends. In most of the cases in which we have received responses, these have been incomplete. While personal data disclosure seems a relatively achievable task, the other two aspects of our requests have scarcely been addressed (automatic making decision processes and data sharing with third parties). The levels of recognition of the right of access as a
citizen’s democratic right vary widely, as does the fulfilment of citizen expectations. While in a few cases our requests have been treated in a respectful way, for others, they seem to have been viewed as a threat, especially for those who are not used to receiving these types of requests.

Due to the different levels of knowledge around privacy and data protection matters held by data controllers, the procedures we experienced presented notable variations. In general terms, we can state with some confidence that in the case of exercising one’s informational rights in Spanish, the impact of gender has been irrelevant. With reference to data vulnerability and the so-called privacy paradox, it must be said that when submitting an access request, it is mandatory to present a copy of one’s ID card to accompany the request. This supports the notion of data protection insofar as data controllers ensure that personal data is only disclosed to those legally entitled to receive such data.

Case by case analysis

This analysis has been organised according to different axes. We have considered sites with good practices those cases in which we have been able to exert our right and where data controllers have shown facilitative practices. In every case we explain how much effort has been needed to reach the aim of obtaining satisfactory responses to our requests. In this report we differentiate sites by sectors (public or private) and good and bad practices. CCTV sites, due to their particularities, are outlined in a separate section.

Public - Facilitative practices

Border control – Schengen Information System

Although locating the data controller was difficult, requesting access to personal data was fruitful and straightforward. It took a couple of weeks to get a letter informing us that they were processing our request and this entitled them to 10 extra days. This reflects their familiarity with the regulations and the procedure. After that, a response was sent by the beginning of October but the date by which the data controller could collect our letter from the local post office expired without any attempt on their behalf to collect it. As a result, the letter was sent back to us by the post office. After speaking to data controller, we decided to resubmit the request again. Having done so, they were still within the time limits (30+10 period). Finally when we got the information they claimed that there is no data on the SIS (Schengen Information System) corresponding to the requester and we considered this site finished on time. Their letters came from the assistant Director from the Unit of Information Systems and Communications for Security (i.e. a stable and specific department solving these issues). It was a concrete and formal letter. We received the data we had sought at the first attempt, although it was not an example of good practices while locating data controllers.

Police records - Ministerio del Interior, Dirección General de la Policía

32The SIS holds information on persons who may have been involved in a serious crime or may not have the right to enter or stay in the EU. It also contains alerts on missing persons, in particular children, as well as information on certain property, such as banknotes, cars, vans, firearms and identity documents, that may have been stolen, misappropriated or lost. Information is entered into the SIS by national authorities and forwarded via the Central System to all Schengen States. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm
Accessing the information required to identify the data controller on the website was relatively easy. Three days after we sent our first request, the data controller sent a notification informing that our request was being processed and they would try to give us a satisfactory answer as soon as possible. It is clear that they are used to this sort of requests and they were using a template. One month after (slightly out of time) their response stated that there is no information in their archives about the requester. A citizen just gets a statement saying that they do not have a police record, without providing further information. However, since no data was held about us, we considered this case successfully completed. The letter was signed by a high ranking officer within the department, with a formal and neutral tone.

**Public - Restrictive practices**

**Driving license records**

This public agency demonstrated poor compliance in terms of identification of the data controller. It has also proven difficult for us to obtain a satisfactory response from this data controller. Their first response was to inform us that the request had been forwarded to the competent agency (so there is no correspondence between the data controller details provided and the actual Data Controller). This entitled them to an extra of 10 days but we subsequently received no response after those 40 days. This letter presented some degree of receptiveness, and was respectful but not encouraging.

After expiring the date, we decided to send a fax complaining that they had not answered. More than a month later, we received a formal letter from a very senior figure within the agency. The content seemed to be quite informative, with several mentions of different regulations. However, their response was incomplete, so we sent a final fax explaining that we believed they had missed information about automatic decision making processes and the specification of which data has been shared (since they mention many public institutions that are seen as possible third parties to whom share data with). At the end of the message we added the threat of making a complaint but even so, we did not receive an answer. Finally we made an official complaint through the Spanish DPA and we are still waiting for their administrative resolution.

**Europol - Eurocargador**

The information provided by the data controller regarding subject access requests was unclear and we chose to use the general postal address to send our initial access request form. Their first letter came within the time limit, containing five numbered pages. The letter included an excessive amount of legal articles with jargon difficult to understand by a lay person. The quotes outlined why our request was deemed unlawful and the duties and rights of the security forces. However, we found that there were three missing pages so the information was incomplete. As such, we called the Police Department asking them to send the entire document. In this second letter (with the previous five pages and three more) our request was denied (which was explicitly stated in one of the missing pages). In both cases, these correspondence were delivered at home personally, by an official. This personal method of delivery was both somewhat surprising. Although we were personally not negatively affected by this (and indeed the official himself was extremely friendly and duly informed about the contents of the letter) we felt that our request had led us to a situation in which we felt we were potentially vulnerable. As a side note, every time we called the police department to
arrange a meeting with the official, we could notice that all people surrounding him were informed about our case (it was “vox populi”).

The tone of the letter itself was impolite and complicated to understand, using legal jargon and legislative quotations. They argued that our request is considered unlawful. (“Those responsible for the files containing the data referred to in paragraphs 2, 3 and 4 of the preceding article [i.e.: security forces] may refuse access, rectification or cancellation depending on the dangers arising for the defence of the State or public security, protection of the rights and freedoms of others or the needs of the research being conducted”). However, at the end of the notification they duly informed the recipient about the right to present an official complaint to the Spanish DPA. Our point of contact was the general secretary of the General Directorate of Police.

Despite the fact that it might be familiar with the procedure, the data controller did not encourage citizens to approach them, belittling the requester. Overall, for this site we would highlight their restrictive practice, firstly denying our request, and secondly because they seemed to use legal jargon as a shield. Finally we made an official complaint through the Spanish DPA.

Following our complaint, the DPA liaised with the data controller. In their response to the DPA, the data controller outlined its reasons (based on many legal articles) to the DPA for denying the access to the requester. Thereafter, we received a letter informing us that the Spanish DPA wished to hear our side of the argument in this case. By the end of February, we received the arguments on behalf of the National Police forces and we were given 15 days to present ours. In their case, the data controller insisted that they duly processed our request and they provided proofs of their correspondences to us (post office receipts mainly). As they considered our request unlawful, we decided not to allege anything new. We can consider this site is closed.

ANPR – Servei Català de trànsit (Catalan Traffic Service)

We located the data controller by phone (calling the general information service number since this is a unit of the Catalan Interior Department). Our first request was unanswered, so we sent a second letter adding that we would make an official complaint to the DPA if no response was received. This second letter was answered out of time and with incorrect information. Moreover, they did treat our letter as an access request but rather a cancellation/erasure request (it seems they might have been more used to cancellations than request for access).

Our contact person was a high rank person within the Catalan Traffic Service. The response of the data controller neither addressed our inquiries about automatic decision making processes nor data sharing with third parties. We sent a fax for the second attempt. In the meantime, we received a letter reiterating the response of the director of the Catalan Traffic Service. This was due to poor coordination, caused by the slow pace of the administrative processes. Moreover, there was a 10 day gap between the date on the letter and the date on the stamp. This therefore meant that we incurred a delay in our attempts to access data.

We expected that after our second (faxed) letter, they would understand that we were not trying to exert the right of cancellation, but rather access. We didn’t receive any other information after they had twice exceeded the time limits. In the end, we made an official complaint through the Spanish DPA. Three weeks later we received a notification on behalf
of the Spanish DPA, informing they were forwarding the case to the APDCAT (the Catalan DPA). After five days we received another notification of admission on behalf of APDCAT, providing the name of the person pursuing the procedure. At the time of writing, we are still waiting for their administrative resolution.

Private - Facilitative practices

Mobile phone carriers

Locating data controller contact details was straightforward and the information on the kind of data that is gathered and who it is shared with was clear. Using the contact address we found online, we wrote to the national headquarters in Madrid. The data controller responded to us (within the time limit) but we were not available to collect their letter. As a result, the post office returned the letter to the data controller. After speaking to the data controller, we decided to resubmit the request. This time we didn’t receive any response so we submitted another letter advising that we would make a complaint to the DPA if no further response was received.

Before a complaint could be submitted however, we received a letter from the data controller which included our personal data. The tone of the letter was formal, with no suspicion, providing a reference number (starting with ARCO) and a file number. It came from the general address in Spain and not from a specific unit. The letter explained that they do not practice automatic decision making processes and data sharing is limited to those actions necessary for the fulfillment of the services offered by the organisation. The letter was signed with handwriting but without providing any name or specific department. As a result, we considered that we had been successful in receiving our personal data together with answers regarding automated decision making processes and third party data sharing.

Loyalty card (supermarket)

Information on how to exercise access rights was found after two clicks on the corporate website, through the ‘legal notice’ link, and it was easy to send the request. The process was straightforward and the company was competent.

Their first answer came after a couple of weeks in burofax format (i.e.: a letter signed by a lawyer). This site shows a disproportionate measure which could be reflecting defensive behaviour without diminishing citizens’ rights. The letter was polite and aimed to satisfy the queries of our request, without traces of suspicion. They provided all the information required regarding which personal data they have, how they obtained them, and for what purposes. The letter also mentioned that no data is shared with third parties and explained how the logic employed by automatic decision making processed is used. As this is a supermarket and the request related to its loyalty card scheme, automated decision making processes are applied to adverts and promotions based on those products frequently purchased. In summary, we were able to exercise our rights with little difficulty.

Loyalty card (food store)

Information on how to exercise access rights was found after two clicks on the corporate website, though the ‘legal notice’ link. They answered on time, claiming that they have no data available about the requester, despite the fact that the researcher has the “fan’s club” (loyalty) card. They explained the purposes and data gathering.
We decided to resubmit the letter and provided the number of the customer’s card. Their second answer explained that the loyalty card club is anonymised (the number of the card fan’s club is associated to a name except for those cases without incomplete data). This could be the case, since the requester habitually provides the minimum data she can when filling forms. Since in our case the card is anonymised, we didn’t need any further information concerning our personal data.

We considered this case as a good practice example since we were successful in exercising our rights. Some effort was expended in sending two letters because having a “fan’s club card”, we needed to clarify why they claimed not to have any data on us. However, the answers received have been satisfactory and this site is considered successfully completed. In every interaction they have been polite, respectful. The reason why they didn’t match the number of the fan club and the name of the member is because they were only able to link one to the other in cases when the customer provides full data in the registration form.

Amazon

Data controllers are identified but they don’t have any office or contact point in Spain specifically for Data Protection. They provided only a postal address in Luxemburg. We sent it there in Spanish. Before sending a response, they made a call (a couple of weeks after the request) to ensure that we were requesting the information specified in order to proceed and send the info. We were advised that the purpose of the call “was just to confirm that it was you and not someone else requesting access to the data”. Two days later, we simultaneously received two separate envelopes: one contained information about their privacy policy and two passwords that were supposed to unlock a CD-ROM containing the disclosure of personal data (which came in a separate envelope). The answer provided was incomplete but was fairly good in terms of amount of information, receptiveness and respect towards the access request. The letter was signed by the legal department, but no name was provided. However, despite these extensive security arrangements of double passwords, we actually couldn't unlock the document containing the personal data disclosure. We assumed this was a casual error. In their letter they encouraged the requester to contact them by phone or e-mail if further information was needed. We chose the e-mail contact this time.

After sending via e-mail the second request stating the password problem and the missing information, they answered that they needed more information to provide us with an answer and they sent e-mails with contact forms. We called them and underwent many interactions with different officers during which every new e-mail was from a different person. This continued until the researcher requested that we be assigned a single person to pursue our case. Finally we were assigned with a specific officer who became the only contact point.

Given the continuing delays, even though the data controller responses were polite, we made an official complaint to the Spanish DPA on 05/12/13. At the end of December however (almost two months after we had sent our first request) we received the CD with correct passwords. It contained information about Amazon.es only (this is that they do not share information with Amazon accounts in other countries. The requester has accounts in Amazon US and Amazon UK, dating before there existed Amazon in Spain). It contained personal data, payment methods, transactions, orders history, Kindle information and purchases as well as history of notifications with the data subject regarding to transactional activities. They also included extended information on their policies about data sharing with third parties. They provide detailed information about the Safe Harbour programme, the marketplace
policy and they agree that they share data with some intermediaries in the process of packing and sending orders. However, they failed to answer which of our data has been concretely shared to whom (if this is the case). We must state that although our question wasn’t answered, data controllers still acted according to the letter of the law when providing generalised answers about third party data sharing practices.

This is a very good example of facilitative policy undermined by totally inefficient practices and bad time keeping. However, as their activity is totally customer-oriented, all their approaches were kind, respectful and aiming to please. We contacted the DPA in order to withdraw our official complaint once our request was satisfactorily answered.

Private - Restrictive practices

Banking records

Information on how to exercise access rights was straightforward and found on their website. Our first attempt was sent by mail and we did not get any answer apart from the acknowledgement of receipt from the post office which confirmed that the letter had been delivered. Having had no response, we then submitted a second request advising that we would submit a complaint to the DPA if no response was received. This time we sent it by e-mail to the Customer’s Service Office. In response to our e-mail, they answered (with a brusque and short message from the Customer’s Service office) that they had already sent a letter but we did not receive it. We asked them to send it again or provide an identification code for making the follow up via the post office. Two weeks later we hadn’t any response. Finally we made an official complaint through the Spanish DPA and we are still waiting for their administrative resolution.

It is worth mentioning that this company is experiencing some structural changes in Spain (such as reducing offices and staff). This probably contributed to their poor performance in dealing with our request. However, in terms of the project aims, they have shown non-facilitative practices.

Facebook

Facebook is a clear case of bad practice of personal data protection. A letter, written in Spanish, was sent to the general European Facebook address in Ireland in. While locating the data controller details, all that we gleaned from the website was how to download our own personal data.

One month and a half later, we had not received either an answer from Facebook or the acknowledgement of receipt from the post office. It therefore appeared that our request hadn’t been delivered to the data controller. We sent a second letter advising that we would submit a complaint to the DPA if no response was received to our second letter. Given our difficulties in obtaining a response (or confirmation from the post office that the letter had been delivered) we began to be dubious about whether the address provided on Facebook’s website actually exists or at least, whether this address accepts postal letters. We checked once again with the post office and the tracking system stated that the letter had been delivered to the recipient. Having received no response from Facebook thereafter, we made an official complaint through the Spanish DPA and, at the time of writing, we are still waiting for their resolution.
Google

Google is another example of extremely bad practices in terms of locating data controllers and in terms of data protection. We located a general address on their website which is located in the US (California). However, we sent the request to the national headquarters in Madrid, as suggested by the coordinators and according to collective strategy.

They answered out of time, so a second request was sent a few days after we received their response. In any case, it was an incomplete response: in their letter they kindly claimed that the branch in Madrid is just a marketing headquarters and thus they do not have a role as a data controller. However, they included a paragraph explaining that they did not have any personal data about the requester. They encouraged us to submit the request to the Californian Headquarters.

This meant that we found some difficulties in the process as (1) we had incurred additional cost by sending our request to the USA, (2) we incurred a time delay by sending our request to the Spanish offices and finally, (3) Google Spain did not offer to forward our request to the California office but instead put this burden onto us. This situation would discourage anyone to pursue the process.

However, we did as advised and sent our request in Spanish to the Californian headquarters. They have exceeded the time limits and we have not received any response. Finally we made an official complaint through the Spanish DPA and we are still waiting for their administrative resolution.

Advanced Passenger Information

This case presented a straightforward process for data controllers’ location. The only reproachable feature is that they do not have any branches in Spain, thus the request has to be sent to the Netherlands (with extra charge). Our first attempt was in Spanish though.

The request was sent in mid-September and many days after we received a kind response in English via e-mail from the Corporate Privacy Officer. In his message, the respondent claimed that their records showed had a different mailing address than the one we had specified in our letter, so the purpose of the e-mail was to clarify to which address we were expecting to receive the information (although we had stated this clearly in our letter). The e-mail was friendly as well as the letter they sent (although it was a bit beyond the time limit).

A month later (slightly out of time) they offered a short and incomplete response. They provided the data gathered but without specifying which concrete data has been treated under automatic decision processes and no mention about data sharing. They attached screenshots of all the flights the requester has taken with the company, apparently from their system directly, since there was a black background.

We sent a second request by e-mail directly to the Corporate Privacy Office. Since the correspondence has been maintained in English after his first e-mail with reference to the delivery address, we responded in English also to avoid delaying the request any further. After our e-mail, the officer detected that he was receiving similar responses from several other people and so he wrote an open e-mail to all those that had approached him with the same message. He wrote an open e-mail to several partners showing annoyance and reluctance after discovering we all were in the IRISS project.
After this unexpected fact, we sent again the e-mail presenting ourselves as researchers but also asking for the missing information. They exceeded the time limits and in fact, to date we haven’t received any new correspondence. Finally we made an official complaint through the Spanish DPA.

We subsequently received a response from the DPA related to this case. They claimed that since this corporation is not located in Spain, we have to write to the Dutch DPA directly. They provided us with the postal address but without offering any other guidelines about expenses, forms or information that we should submit.

We searched for more information about the Dutch Data Protection Agency without success (their website is little self-explanatory) but we nevertheless submitted a letter in Spanish.

One week later, we received an informative letter on behalf of the Dutch DPA as a confirmation receipt. They advised that their response will be in Dutch and they provided us with a reference case number to be used in all correspondence. The letter was signed by the Senior Employee Information Management. This case is therefore ongoing pending further communication from the Dutch DPA.

**Microsoft**

In phase one it was easy to find the Microsoft online privacy statement through their website. Microsoft provided a form to contact them (one for each product). We chose to use the generic Microsoft software. Besides, they offer a mailing address in compliance with Safe Harbour located in Washington. This means that the data controller was identified successfully but there is no branch or headquarters located in Spain. This is not in compliance with the local law (which states that any company operating in a country should have a country branch) and implies extra charges to the requester.

In our first attempt we sent a letter in Spanish to the US headquarters. We didn’t get the receipt back and after the 30 days period we had no answer. We made a second attempt, submitting the template for non-response within the form they provided. In return we received an e-mail providing direct links to their privacy policy, without personal data disclosure and without giving responses to the automatic decisions on personal data or third party data sharing. They therefore did not treat this case specially, and they did not obey the period provided. They gave the possibility of responding to the e-mail in case the information they provided was deemed unsatisfactory, and so we did so, but there was no answer after this last attempt. We made an official complaint to the Spanish DPA. Ironically, they sent an e-mail with a satisfaction survey and we presented a complaint explaining our dissatisfaction towards their general treatment of the case (not in specific terms, as we have requested). Unsurprisingly, our request has been greeted by silence. At the time of writing, we are still waiting for the DPA’s response.

**Twitter**

It was easy to locate the data controller and their privacy policy. It was clear which data they collect and for what purposes under the privacy tab on their website (without logging in). They provided two means of communication: a specific e-mail for Privacy policy issues and a mailing address located in San Francisco, California.
We chose to make our first attempt by sending the request to San Francisco. We obtained no answer after the 30 days period, so we submitted a second request, this time via e-mail. Automatically we were provided with a case number. We received a general e-mail (an auto-reply) as response, clarifying that this address was specifically for account and personal data inquiries and providing several support links for other issues. Since we received a generic response, they did not address our request attentively and we did not get the information requested, we sent a third message adding that we would make a complaint to the DPA if we continued to receive unsatisfactory responses from the data controller. We had no response after the 10 day period, so finally we made an official complaint through the Spanish DPA.

In response, the Spanish DPA informed us that since Twitter is a corporation from the US, if falls beyond the jurisdiction of the DPA. As such, we were advised to contact the American DPA. In this case, the Spanish DPA did not provide any further advice or guidelines on how we might go about this.

We sent an e-mail to the AEPD asking for the information on where to send our complaint. They did not answer but the AEPD website provides several links to other DPAs, mainly from other European countries. With reference to the US, the website indicates that correspondences should be sent to the Department of Homeland Security. After a 15 minutes search, we found the contact of the Privacy Office (a telephone number and an e-mail address), under the tab of DHS white pages. We sent an e-mail with our request in Spanish (10/03/2014).

Immediately we got an automatic response stating that they would respond as soon as possible. Ten days later, we received a kind response suggesting that we submit our complaint via Safe Harbor (we maintained an e-mail conversation with the Senior Director, Privacy Oversight of the US Homeland Security Department. She advised us to go through Safe Harbor and we did so in March 2014).

Safe Harbor subsequently wrote to us many days later claiming that they have contacted Twitter and that in principle they were about to duly address our request.

A few minutes later, we received an e-mail from the Trust & Safety Team of Twitter asking us to confirm “your lawful consent to this disclosure by responding to this message from the email address of record for this account”. Right after our confirmation we received a full disclosure e-mail with a zip file containing all the personal data and the historical activity carried out from the account. However, the issues about data sharing and automatic decision making processes remained unanswered since the email provided only general information on these issues.

This is one of the examples of how the intervention of a DPA unlocks the process.

**CCTV and signage**

**CCTV in a Stadium**

We attended the stadium in person and found clear signage all over the perimeter of the surrounding fence and particularly in every single entrance. There actually are two data controllers: one is the football club and the other is the local police, thus the site is private but there is a two-fold data controller (a private and a public one).
The Police didn’t accept or deny the request; they simply asked us to provide more information to exert the right of cancellation (although we had just asked for access). They asked for a certified copy of the ID card or passport (“fotocòpiacompulsada”). They explicitly said they give a 15 days’ time limit (not specifying the starting date) so we could have missed the period without noticing it. We duly proceed and we received a late response stating that they do not have any footage of the requester. They also advised that we should address our request to the responsible authority, which they stated is the football club. However, in the pictures we took of the signage of the CCTV, the local police station was named as the data controller. This can be a deterrent practice and a restrictive manner of behaviour.

We then contacted the football club and our first letter was sent on 24/10/13. We subsequently received a receipt certifying that the letter had been received. On not receiving a response thereafter, we contacted the data controller by email and on 02/12/13, we received a response saying that they had not received the original request. They politely asked us to provide the letter again (thus adding extra time and effort to the process). We could at least do this by e-mail, which is a slightly simpler process. Subsequently, we received several emails from the Supporter’s Office advising us that they were now processing our request. We were advised that they had forwarded our request to the legal department but we have no confirmation that this had happened so we could not keep track of the process of our request. We wrote to them once more but our letter was greeted with silence. Given that a response was not forthcoming and legal time limits had been exceeded, we submitted an official complaint to the DPA regarding both data controllers. At the time of writing, we have received no response from the DPA.

CCTV in a public space/city centre

This was a site without signage at our first visit. We presented two complaints to the city hall (one for the lack of signage and one requesting the details of the data controller). In the meantime, while waiting for their response to our both complains, we had passed again and sent the letter to the Council of the district.

Several weeks after our complaints, we passed again around the area and unexpectedly found several new signs providing information on data controllers with clear details of a link where one may exercise informational rights through a dedicated form. However, checking this page we found that the town hall had a list of sites with CCTV controlled by this institution, and actually this “CCTV public space” was not in the list. Probably is not updated, but actually this could indicate this is not a high priority issue.

Almost out of time, we received a communication from the district. Their answer was a single sheet of paper (without envelope) that was brought to us at home personally by a messenger. Our subjective response to this was a good reaction in first place (because the delivery at home is easier for us) but we were disappointed that the information arrived without an envelope (meaning that anyone can read it). Furthermore, the messenger came from the city hall and after the delivery of the contents to the requester’s home address, he knows where the requester lives. As such, some semblance of vulnerability exists and demonstrates the way in which a request for information can lead to the disclosure of additional personal data. In terms of contents, the answer was quite complete, containing certain amount of generic information about their archives, but they denied us access to the footage. Their denial strategy was that footage had already been erased. The district manager was the signatory of the letter (so it is a high rank position). They claimed not to have any
other personal data, and advised that they had not undertaken any data sharing with third parties and had not used automatic decision making processes. At the bottom of the page they provided some legal information about the law of data protection and how to exert the ARCO rights.

We passed again around the area and sent another letter requesting the access to the footage, this time sending the request immediately (and received by them the following day), but they responded according to the calendar of the first requests, so they ignored that we were submitting a new request with reference to a recent footage. Moreover, the district manager signed this letter once again and, while his first letter had been polite and cordial (“we communicate the inability to get access to the footage…”), the second sounded irritated, remarking his words, such as “we reiterate the inability to give you access to the footage”. This showed little attention while attending our request and aggressive manners after our second attempt. The letter had the same general information at the foot page.

Finally we made an official complaint through the Spanish DPA and we are still waiting for their administrative resolution. The DPA informed us that this case is competency of the Catalan Authority, thus the file was transferred to them. At the time of writing, the case was still in progress.

**CCTV in a transport setting**

We chose a central metro station and the signage was in full compliance with data protection law. Their first answer was received within the time limit but they stated that the images had already been eliminated after one week. No other information was mentioned about the requester, and no information about sharing with third parties. The message was unhelpful and showed hostility and the time limit and correlating retention periods of footage were used as a denial strategy. The researcher appeared in the footage recorded on 04/09/13; letter was sent the next day and received by the data controller on 09/09/13. Their response was dated 16/09/13. It was signed by a lawyer of the company (but they do not have a specific department to deal with data access issues).

We wrote a second request (this time via e-mail) asking the same information as the response was incomplete and assuring that the CCTV had captured the requester the previous day (as such trying to make it impossible for them to use the same denial strategy). A few days later, they respond detailing that the data was available by contacting another department, not the general one to which we were directed by the signage. They did not mention either automatic decision processes or third party data sharing. We therefore sent another e-mail asking for this missing information. In their third e-mail, they answered that there was no automatic decision or data sharing. Regarding CCTV, they asked us to provide more information. We sent another e-mail with extensive details regarding our clothing etc. to facilitate identification in the footage.

In this site, we have had to interact with a number of different contact persons, so there is not a unified response and information is fragmented, which requires an extra effort on behalf of the citizen. Besides, the time management for this data controller was very poor. After a couple of weeks we had not received any satisfactory response. Following further interactions with the data controller, we made an official complaint through the Spanish DPA since the legal response time limit had expired.
However, few days after the complaint was made, we received a final response from the customer service office, where they had identified the requester in the CCTV footage. They did not provide access to the footage but simply described what appears in their recordings (this is in compliance with law). It is worth mentioning that this description actually consisted of just two lines this displaying a generally passive attitude. They were unreceptive and as if they were satisfying a whim of the requester. The feeling is that our request had been useless and time-consuming for them.

**CCTV in a large supermarket/department store**

Although CCTV signage was easy to locate in person and provided the data controller’s contact details, this data controller generally showed poor practices in this case. The images were captured on 04/09/13 and the request was sent on 05/09/13. As a result, the data controller claimed that they received our request on 12/09/13. However, the postal office gave us a receipt stating that the letter was actually received on 11/09/13 (which is a national holiday in Barcelona but not in Madrid, where the letter was addressed).

Their first letter was short and incomplete but respectful. The letter argued that footage is deleted after seven days. Given that the letter had been received prior to the seven day period, we can only assume that this reliance on the data retention deadline was a denial strategy. Moreover, the letter did not provide any other information with regards to data sharing practices or the use of automated decision making processes. As a result, we sent a fax in November asking for more information about our unanswered queries and requested access to CCTV footage again. We passed once more around the area and this time sent the request immediately (and received confirmation that the letter had been received the day after). However, the response we received from the data controller thereafter dealt with our first request and therefore ignored the fact that we had submitted a new request. Thus, their second letter showed poor administrative performance in terms of the attention dedicated to reading the content of our request. Both letters were signed by a man from the legal advice department, writing cordially. Since the access was denied and we considered they were using restrictive and disregarding practices, we made an official complaint through the Spanish DPA and we are still waiting for their administrative resolution.

**CCTV in a Bank**

There were only indoor cameras in this site. Signage at the door was completely visible (a picture of a camera), but the identification of the Data Controller and contact details were not so readable (since it was a sticker with letters in green, it faded into the background of the other colours on the office). It was difficult to read at first sight and also difficult to read once the photo was taken.
Our letter was sent and they answered that they do not have any personal data on the requester (so it is not necessary to respond to other related issues). Concerning our request for the footage, they denied our request providing legal arguments and informing of our right to make an official complaint. As a result, we made an official complaint to the DPA. In response, the Spanish DPA explained that in their view, our access request had received the legally required response. The answer is that this bank does not hold data on us. With reference to the CCTV, it remarks that as stated by law in credit sites CCTV measures are compulsory and that the footage can only be accessed by security forces of the state. The only purpose is to identify criminals and the footage must be stored for 15 days unless stated otherwise.

**CCTV in a Government Building**

In this government building there are integrated cameras inside and outside the building. The signage was in full compliance with law: visible, located in every entrance of the building, there were several posts and provided complete information. When trying to enter to the Citizen’s Service there is a surveillance area by private security agents and we were told not to take pictures of the building. Onsite, the data controller was completely identified via the signage provided which includes contact details for the data controller.

We submitted our request and a couple of weeks later we received the response. They sent a letter giving the impression that the request was not legitimate and that it was out of place. They said that in case they had some data on the data subject captured by the CCTV, the quality of the footage is so low that identification of individuals is difficult in general terms. The only exception is unless a crime occurs and then the security forces broaden the image and gain more details on people appearing there. They added that in any case, they had been revising their recordings and they hadn’t found the requester in them. They also added that we were talking about a time slot when many people are entering the building (including workers and other citizens), and therefore giving access to footage would violate their rights. Only in the event that a crime was committed, permission of access would be given to the state security forces.
Finally we made an official complaint through the Spanish DPA because we considered that negotiation with this site would be unfruitful. We assume they received our complaint because we have received a notification on behalf of the Catalan Data Protection Agency. This means that the file has been transferred but this time we haven’t received any communication announcing the transfer among national and regional authorities. As a result, this case is ongoing pending further communications from the Catalan DPA.

**Concluding thoughts**

As this report has shown, the general degree of legal compliance and the performance of good practices are low when citizens attempt to exercise their access rights in Spain. There is a wide range of attitudes and knowledge about the access rights procedure amongst data controllers which makes it difficult to summarise the landscape in a few words. The purpose of this report has been to demonstrate how much effort a data subject must expend in order to exert his/her right. In general terms, the answer is much more than one may reasonably expect.

Several sites have concluded in an official complaint to the Spanish DPA. Some data controllers have failed to answer our requests at any point and only a minority of cases have been successfully closed after a relatively easy and straightforward process. It is worth mentioning that our experiences differed based on the type of data we requested. While it proved much easier to obtain personal data disclosure, questions about automated decision making processes and data sharing with third parties remained unanswered. We propose that there is no tracking of data usage, and for those cases that it might exist, those who are in charge are not aware of it. Meanwhile, requests to obtain CCTV footage demonstrated entirely different practices. This is partly explained by the fact that sites involving CCTV have required a particular treatment since footage contains biometrics and are subject to specific legislation. In this section we present some concluding remarks, paying attention to the differences between public and private sectors and offering general reflections to conclude the report.

**Emerging trends**

We find that in depicting emerging trends, it is much more interesting to focus on the denial strategies and the restrictive practices found in the study. All of these can be summarised in several patterns. Below we present them by general categories. Bear in mind that restrictive behaviours are different for common personal data and for CCTV footage. They are grouped according to what they are related to.

We found problems from the very beginning of the submission process, namely in the sending of requests. Some organisations claimed not to have received our requests or claimed that they had already sent an answer that we hadn’t received. Moreover, we often received no response at all to our requests and two features of such responses should be noted here. Firstly, in most cases we know that the data controllers received our request (since we obtained conformation of delivery from the post office). So their claims not to have received our requests appear to be false. Secondly, those sites in which we did not receive confirmation of delivery tended to be large multi-national corporations, particularly those with headquarters locating in the United States. Why these organisations displayed such similarly poor practices was unclear but nevertheless interesting.
We were frequently denied access to our personal data based on (incorrect) legal reasoning. This denial strategy included reliance upon overlapping laws or competing legal frameworks. We were also denied access by relying on the nature of the data stored (such as the National Intelligence Centre) with the law providing data controllers with exemption categories. Another point causing trouble was the means of communication used by data controllers. In one case, they do not consider e-mail as a valid means for sending a request, while in other cases they did not want to provide the information in writing and through postal mail. In these cases, the alternative was to attend to our request by asking us to personally check their archives. Related to this, we found one site where they considered that they did not have to disclose our personal data due to format of storage (i.e.: they were arguing that since it was not computerised, they didn’t count on it as form of owning someone’s data).

Generic answers and automatic responses have been common practices in large private companies. By this we mean that we have obtained generic responses not addressing our request particularly. In these cases we received general responses with links to the privacy policies and other support sites of the companies in question.

Another recurring feature has been the lack of knowledge and familiarity with the access request procedure amongst data controller representatives which has led to misunderstandings and delays. In one case, the data controller treated our request as a cancellation. In another case, we were told that our data was located, but they couldn’t address our request since the information was paper-based only and had been computerised (illustrating confusion between the information gathered and the format for storing it). Another example of lack of knowledge was the lack of understanding of the notion of data sharing, insofar as data controllers often did not consider certain situations as data sharing and thus these situations were not reported to us.

Some other minor restrictive practices can be noted here. For instance, we encountered instances when the details provided for the data controller are not the correct place where the response to our requests comes from (i.e.: data controller supposedly located in Barcelona but the office who responds to our request is based in Madrid). Moreover, we found cases when the local branch of an organisation deals only with specific queries and we are asked to send our request again to the US headquarters, thus incurring additional fees and delays. Lastly, we came across instances in which several different departments within one organisation were responsible for the processing of our personal data. However, rather than one central contact point dealing with our access request, we were required to contact each different department individually in order to obtain all our personal data and receive a complete response.

With regard to requests made for CCTV footage, we consider that we have found three main strategies for denial:

(a) The footage is not stored anymore: after a period of 7, 15 or 30 days, our footage if erased and is no longer available. However, in many cases, we know that our requests were received prior to the date of deletion and thus we can only infer that data retention deadlines were used as a strategy of denial.

(b) Insufficient information in the request, making difficult the identification of the requester in the requested footage: this was often due to the quality of the footage, crowded situations or being advised that a copy of our ID card and a picture of the requester were not enough to help the data controller identify us on the footage. In
several cases, data controllers requested more information, but this lengthened the period of answering and we ended up with the (above) reason that the footage had erased.

(c) The law provides data controllers with a legal exemption from disclosing the footage: this was mainly experienced with referral to the law of private security forces which prescribes that for some sites, only the state security forces can get access to the footage in case there has been a crime and under especial permission. Using the legal bases as a shield has been used to deny some requests but also putting legal jargon and making the communication unfriendly between the requester and the data controller.

In contrast, we also found data controllers that demonstrated considerably better practices. These data controllers tended to be familiar with the access request process and treated our requests with respect, thus legitimating our requests. For those cases where there was receptiveness to our request, staff tended to be courteous and helpful. In a few salient sites, data controllers have maintained contact with the data subject in several occasions in order to clarify points while trying to offer a satisfactory response.

**Public vs. Private**

The difference between public and private sectors is important. We found that private organisations performed significantly better in the study. Among these private corporations however, there are clear differences between small and large companies. The general pattern is that cross-national companies tend to perform badly (especially technological corporations such as social networks like Facebook, Twitter or Google). Amazon has been an exception in the Spanish study insofar as they displayed demonstrably good practices and this may be explained by their “customer oriented” structure.

In relation to banks, we have experienced quite different patterns between regular banking records and credit reference checks/rating. This is potentially the case because of the additional risks to the banks in revealing data regarding credit scoring systems.

With regards to public sector sites, we found that those sites habitually used to processing personal data tended to respond better to our requests (such as the police). In contrast, other public sites demonstrated completely unlawful behaviour despite the fact that they are part of state structures that are, in turn, those that promote the Data Protection Laws.
SIGNIFICANCE OF FINDINGS - SPAIN

Several key findings have emerged from the empirical phase of this research. In several cases our requests have been treated as an exceptional situation. This has been evidenced by the involvement of high ranking officials and lawyers as part of the response to our requests. In a few cases, our requests were treated with normality, especially where there is a specific unit for the processing of such requests. Generally speaking, negative reactions to our requests and misunderstandings reflected a lack of knowledge regarding data protection and privacy as well as fearful reactions once we advised data controllers of our intention to make an official complaint to the DPA.

With reference to automated decision processes and data sharing with third parties, our requests yielded general answers and ambiguity when we asked for specific information about specific data of the requester. Thus, data controllers tended to avoid giving a response or preferred to provide general outlines of their practices.

Throughout the research, we have been in contact with the National DPA and equivalent regional authority at the Catalan level. Both of these organisations demonstrated good performances in general terms. Moreover, both are citizen-oriented. Regarding inquiries and doubts, we have generally been satisfied after contacting these organisations for general advice. Staff had enough information about what we were asking in most of the cases. Their websites are clear, helpful and provide documents that are useful for both citizens and companies. The Spanish DPA is completely citizen-oriented, helping and encouraging data subject to exercise their rights. The Catalan Authority is a bit more institutional in their processes. They show good communication and cooperative synergies among them, providing citizens with a quality attention. However, we found that for cases that are apparently similar we received different patterns of response. In most of the sites they are not admitting our requests (especially those involving CCTV footage).

The Spanish DPA offers the possibility of seeking protection [“recabar tutela”] which is a process that can be done without any cost (aside from the cost of sending the information in writing). They need about a month to close cases. This process is flexible and they allow complainants to provide any new information at any point of the process, as well cancelling the official complaint in cases where the data controller is successful in its task. They do not have a legal period to give answers, but in average they spend between one and two months considering their response.

The Catalan DPA is specialized in institutions that are responsibility of the Catalan Government (such as schools). The law establishes a six month deadline to communicate the outcome of any complaint proceedings. Once this period has elapsed, the complaint can be considered as rejected if no notification has been received. This agency makes a difference between legal entities and individuals: while consultations on the legislation can only be submitted by a legal person, official complaints may be presented by individuals.

We also found that when submitting complaints against non-Spanish sites, the level of support and assistance provided on behalf of the DPAs was particularly uneven, giving the impression that it depends on the person who is dealing with the case. It is also worth mentioning that after submitting our complaints, we detected that when the DPAs begin the process of resolving our complaints, some sense of a catalyst reaction emerged. For example, some complaints that had previously been unanswered began to be addressed and for those

IRISS WP5 – Spain Country Reports
Final Draft
30 April 2014
complaints in which we had received only a partial response, we obtained more in depth responses. It is possible therefore that the DPA reacted to the large volume of our complaints as we began to submit increased numbers of complaints.

We would like to close this report by proposing some ideas that can be useful to shed a light on the Spanish situation. Firstly, making requests actually “puts you in the focus” insofar as making a request may lead to one’s profile being raised and as a result one’s privacy being further compromised. We have been monitoring this notion through the raising of searches of the requesters’ names on Google. However, it is difficult to make definite conclusions through the site academia.eu (which uses Google analytics to determine when a search for a name has occurred and where it originated from), because one of the researchers has several media appearances every week and in the other case, the variations are overlapped with academic activity undertaken (such as giving lectures, attending conferences, etc.). However, some peaks can be found in one of the months in which we sent the most access requests (image 20/10/13 to 19/11/13):

Above all, we conclude this research by reflecting on how far removed we are from our own personal data. Something that belongs to us and something about us should be protected by law. When a regular citizen, without a particular reason other than a wish to increase his/her informational awareness, submits an access request, there starts a sort of gymkhana in most of the cases or, at least, a steeplechase. This report has shown how easy it is to have personal data spread among different archives, files and organizations and how tough it can be for a data subject to track down this data and find out who knows what about him/her and what they know.
References


Mendoza, Ana Isabel (2011): Deudas de telecomunicaciones y registros de morosos. [], working progress that can be downloaded at https://www.uclm.es/centro/cesco/pdf/trabajos/7-2011/7-2011-5.pdf (last access: 30 April 2014).


List of Abbreviations

AEPD - Agencia Española de Protección de Datos (Spanish DPA, national level)
ANPR - Automatic number plate recognition
APDCAT - Autoritat Catalana de Protecció de Dades (Catalan DPA, regional level)
ARCO rights - Access, rectification, cancellation, opposition
ASNEF - Asociación Nacional de Establecimientos Financieros de Crédito (National Association of Credit Institutions)
CCTV - Closed circuit television
CIRBE - Central de Información de Riesgos del Banco de España (Central Credit Register of the National Bank of Spain)
CNP - Cuerpo Nacional de Policía (National Police, security forces)
DGT - Dirección General de Tráfico
DPA - Data Protection Agency
EU - European Union
FECEMD - Federación Española de Comercio Electrónico y Marketing Directo (Spanish Federation of E-Commerce and Direct Marketing)
LOPD - Ley Orgánica de Protección de Datos (Data Protection Act)