Exercising access rights in Spain

A comparative study before and after GDPR

info@eticasfoundation.org | +34936005400
Eticas Foundation. Calle Mir Geribert, 8, 08014 Barcelona

List of acronyms

Acronyms	Definition
APDCAT	Catalan Data Protection Agency
CCTV	Closed circuit television
DNI	Documento Nacional de Identidad (National Identity Document)
DPA	Data Protection Agency
GDPR	General Data Protection Regulation
HTML	Hypertext Markup Language
LOPDGDD	Ley Orgánica de Protección de Datos y de Garantía de Derechos Digitales (Organic Law on Data Protection and Guarantee of Digital Rights)

Introduction

This study describes the experiences of trying to exercise the right of access to personal data in Spain.

Using different ethnographic examples, the study tests how easy or how difficult it is for a data subject based in Spain to obtain their personal data, firstly by **locating the required information about the organizations and their data controllers**, and secondly, **sending access requests to these organizations.**

The **first part of the fieldwork** was carried out a few years ago, in 2014, when Eticas was participating in a broader European research project, in which different European countries made requests for access to find out how public and private organizations complied (or not) with the law.

The **second part of the field work** was carried out in **2018** by the Eticas Foundation team and collaborators, to better understand how the new European General Data Protection Regulation **(GDPR)** was being applied, in relation to the right of access to data personal information.

The **right to the protection of personal data** is derived from **articles 10 and 18.4** of the **Spanish Constitution** that safeguard the dignity and privacy of people, respectively. It was developed in the **Organic Law 367 15/1999 on the Protection of Personal Data** (Organic Law on Data Protection, LOPD), which was the applicable law in Spain before the **GDPR**. The European General Data Protection Regulation that came into force in May 2018 entailed a new Spanish law, which was approved in December 2018: **Organic Law 3/2018**, of December 5, on the protection of personal data and the guarantee of digital rights.

With **GDPR**, the **entities responsible for the processing of personal data** must offer a **person that requests the right of access** the following information:

(1) the **categories of personal data** that are processed, (2) what are the **purposes of the treatment**, (3) to **which recipients** or categories of recipients these data were communicated or will be communicated, (4) information about the **origin of the data** when the origin has not been the same interested person, and (5) a **copy of the personal data** object of treatment if the interested person so requests. In addition, (6) you must report the **expected period of conservation of the data** and (7) the **criteria** that have been followed to determine said periods. Finally, you must inform (8) that the interested person also has the right **to request the rectification or deletion** of their data, the **limitation** of the treatment, **opposition** to the treatment, and also to file a complaint with the control authority (protection agency of corresponding data for each territory).

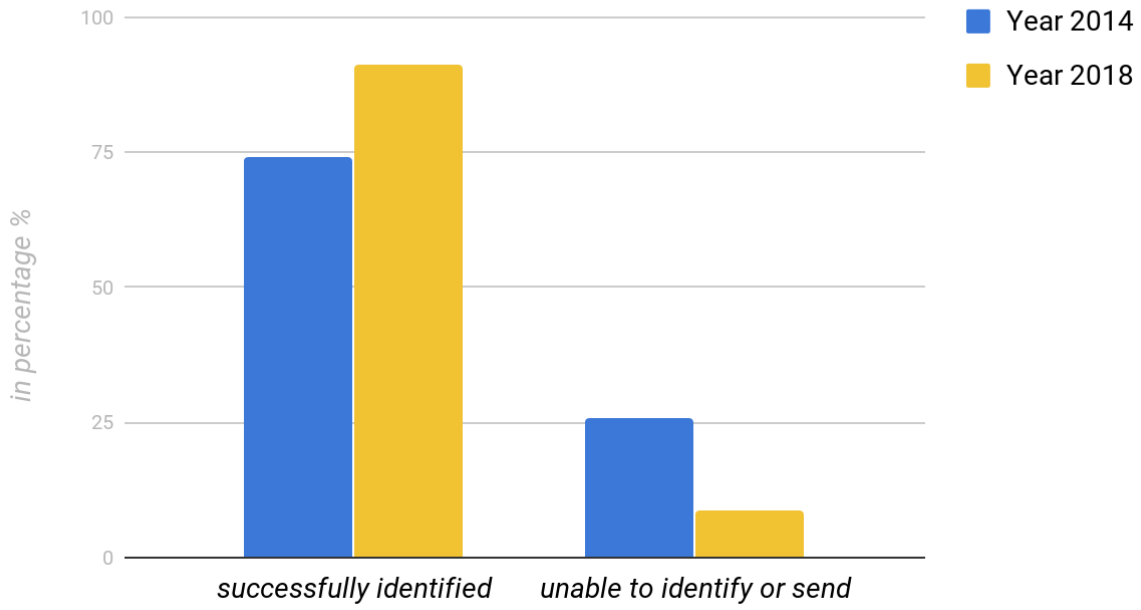
Access rights in Spain: year 2014

This part describes, analyses, and summarizes the experience accumulated during our **attempts to locate data controllers** and, once this is done, **send access requests** to organizations.

As part of this process, we tried to place the data controllers of **30 organizations** and subsequently send **21 requests for personal access** to a wide range of data controllers in **both the public and private sectors in Spain** and, in the case of certain multinational companies, beyond national borders.

The details of the data controller were **usually found on the official websites** of the organizations. In cases where websites were not helpful, it was often **necessary to contact organizations by phone**.

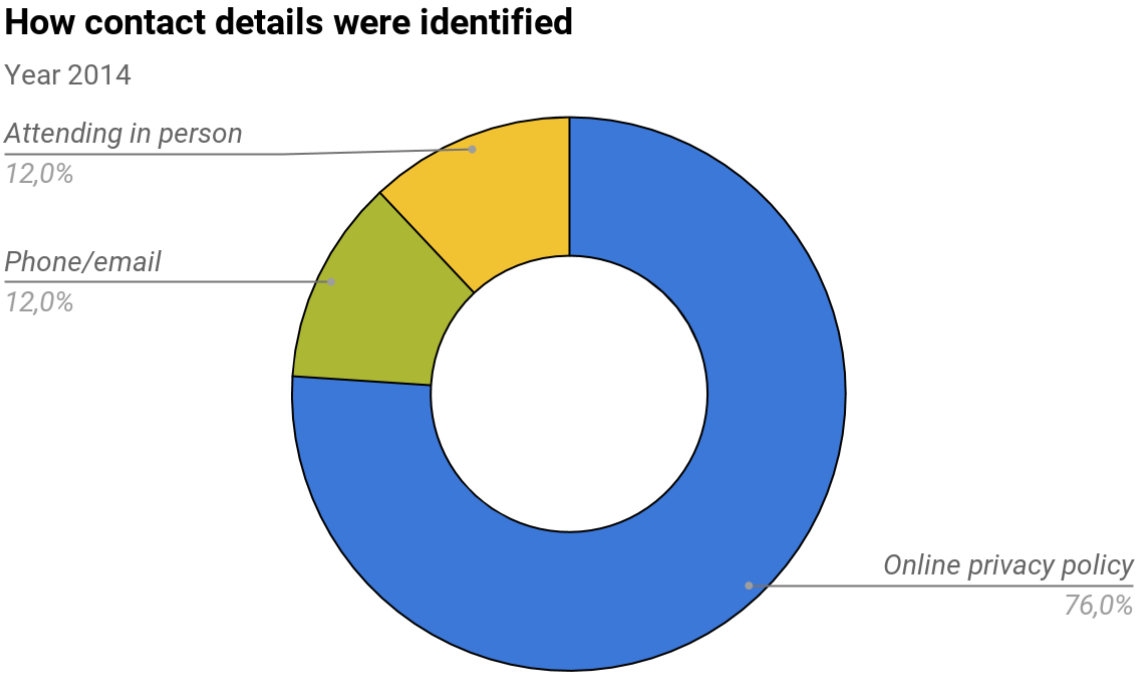
Reaching data controller contact details



In 2014 we were able to successfully identify 74% of the organizations' contact details, and in **2018 we were able to obtain better results**, correctly identifying the contact details in **91.18% of the cases**. Put another way, in 2014 we were unable to obtain the information to exercise the rights of access to our data in 26% of the cases, while in 2018 it was “only” in 8.82% of the cases where we were unable to resolve the submission of our requests. There are signs of improvement, but we still detect some level of non-compliance.

Our experience was that when we spoke to staff members over the phone, a **general lack of experience with data protection and access rights** was evident. These conversations were quite difficult due to the **systematic suspicion** of the respondents, who seemed sceptical that we wanted to access our personal data simply because we were curious.

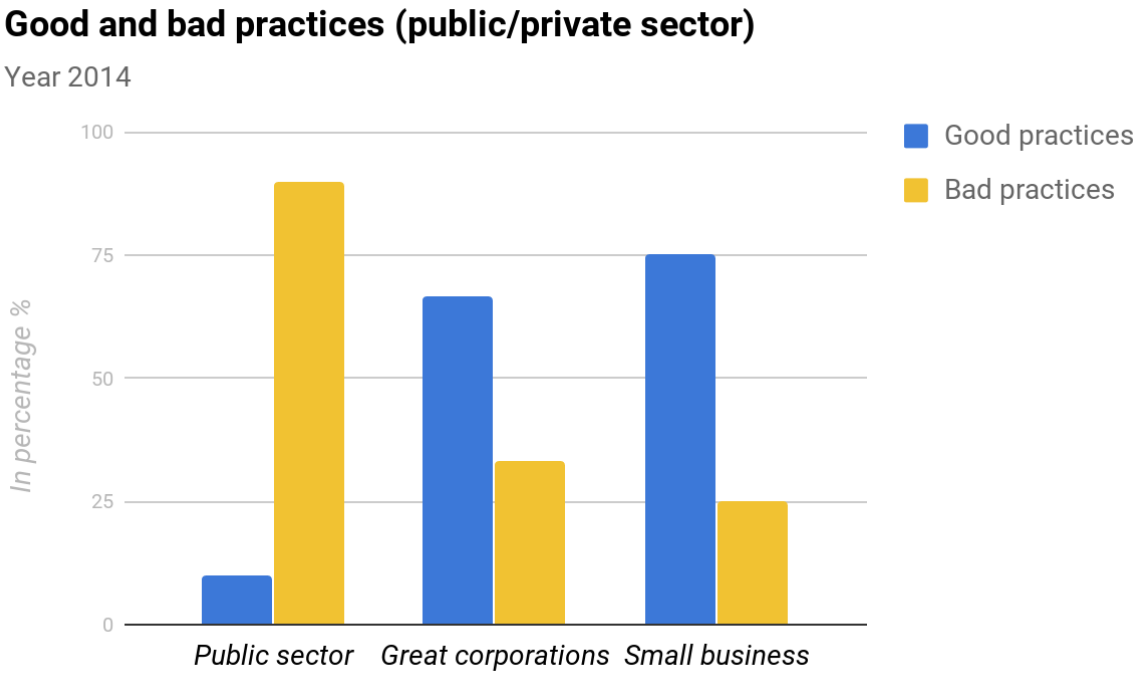
The cases in which **we were able to find the contact information through the privacy policies of the organizations' web pages** were the most, a total of **19 cases**, while in **3 cases we had to speak by phone** with the personnel of these entities, or in **3 other cases we had to speak in person** by physically going to the headquarters of the organization.



In the case of **CCTV systems**, the **mandatory signs** should have meant that we could locate the data controller without speaking to any staff member in person. In the case of CCTV sites, **irregularities in sings were found due to poor location and visibility**, no signs, or signs with no data controller details. **Signs in compliance with Spanish law were found in only two of five sites.**

The request for access to personal data in Spain is generally not as simple a process as it probably should be. In terms of facilitating / restrictive practices, different trends could be observed. **In most cases where we had received responses, they had been incomplete.**

Thus, when we carried out this field work (year 2014), **we discovered that the general degree of legal compliance and the performance of good practices when citizens tried to exercise their access rights in Spain was low.** Some organizations did not respond to our requests at any time and only a minority of cases were found to have resulted in legally adequate responses after a relatively straightforward and simple process.



The public sector, especially, showed a low level of compliance, **with 90% of bad practices**, and only 10% of good practices, while the **private sector** always had a much higher compliance, **66.7% of good practices in large corporations and up to 75% of good practices in small businesses.**

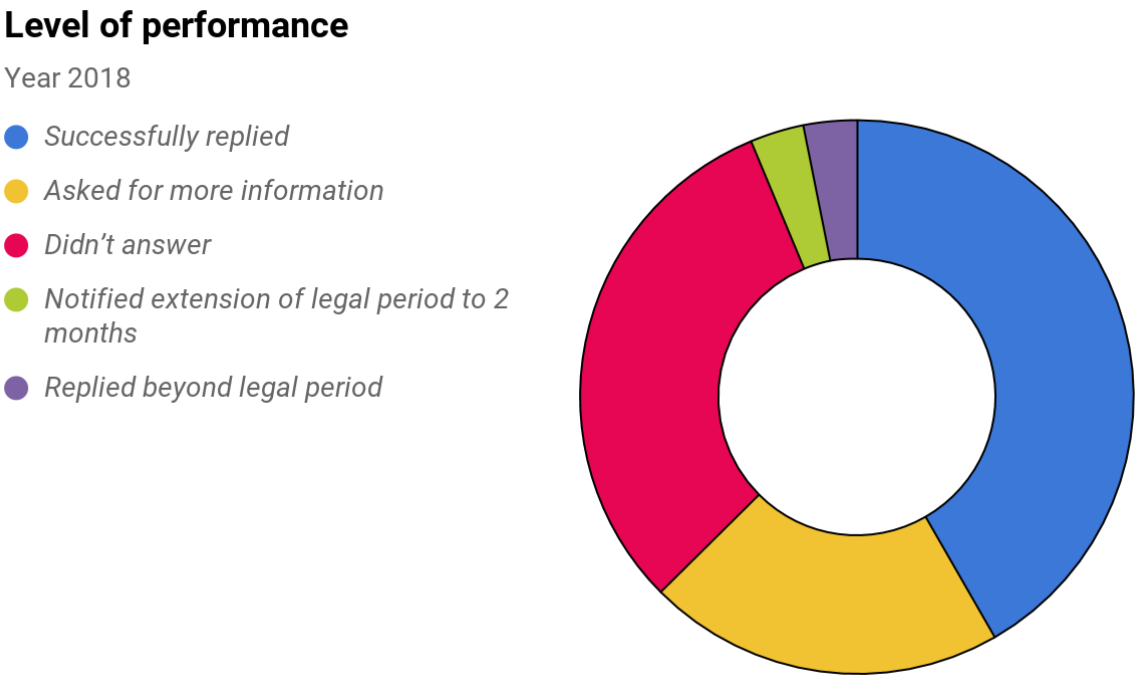
It is worth mentioning that **our experiences differed depending on the type of data we requested.** While personal data disclosure was much easier to obtain, questions about automated decision-making processes and data sharing with third parties remained unanswered. This could be the result of a failure to track how data is used and shared, so some organizations were unwilling to answer our questions about this.

After this study, **we concluded with a reflection on how far away we were from our personal data.** Something that belongs to us and something about us must be protected by law. When a common citizen, for no particular reason other than a desire to increase his informational knowledge, submitted requests for access, they often began a journey that led them to navigate a maze and ended, not always happily, when they had completed an entire obstacle course.

In this sense, **what would the situation be like 4 years later, and with the new European regulation on data protection already in force?** To answer that question, we decided to put our access rights back into practice.

Access rights in Spain (2018) under GDPR

This time, to carry out the field work, **we sought the contact information of 34 data controllers**, of which we were finally able to **make 31 requests for access** to personal data (91.18%), corresponding to both companies and organizations of the public sector and the sector. private. **The 3 access requests that we were unable to carry out** (8.82% of the cases) were, in two of them, because it was not possible to locate the contact information to submit the request, and in the other case, the form contained an error and would not allow the insertion of the corresponding postal code, and therefore did not allow to send the request.



The **level of compliance** was quite uneven. Of the 31 access requests that we were able to make, only **12 were responses received in an optimal and direct manner (38.71%),** which is to say, responses that offered correct information within the established period. On the other hand, **6 responses received requested a bit more information** from the person concerned

(19.35%) so that the request could continue to be processed: 2 asked to send a copy of the identity document; **1 even made a telephone call to the interested party** asking them what data they wanted to receive information about **(and for what reasons)**; and in 2 cases they requested both, that is, that we provide an identity document and that we specify what information we wanted to access.

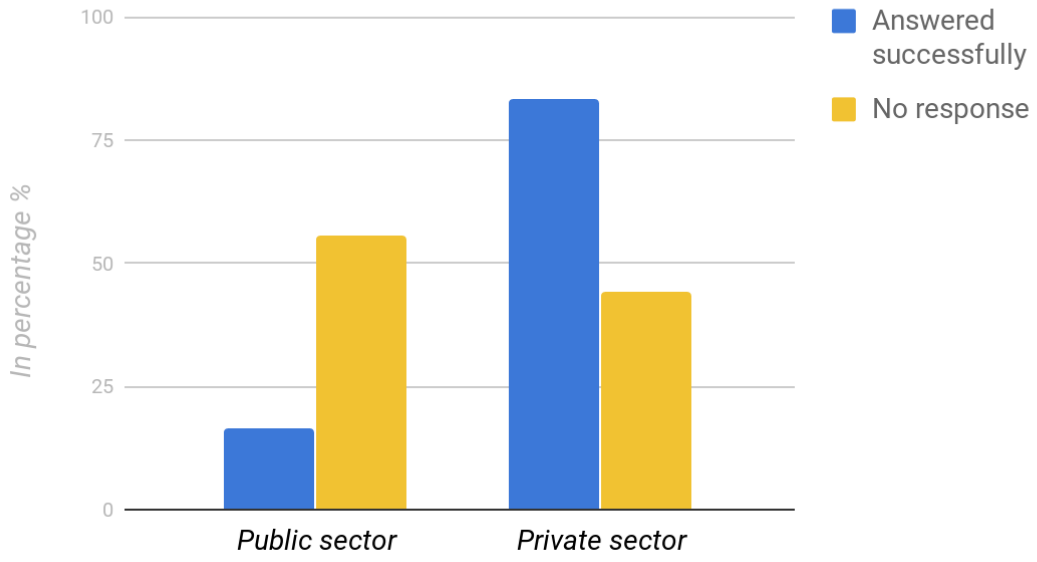
Only in **1 case** we received a response that was a com**munication extending the legally established period from 30 days to 2 months** to give a response, as provided in the GDPR, arguing that it was a complex request given the large amount of data it manages the organism.

If 12 were direct responses, and 7 were responses that didn't initially offer the requested personal data, **the requests sent from which we did not obtain any response were a total of 9, which is almost 30% (29.03%).** In addition, in addition to these, **in 1 case, we received a response outside the period established by law.**

By sectors, **the private sector in general responds better than the public sector.** The same trend found in 2014. We considered 34 data controllers, of which 21 were private actors and 13 public actors. **Of the most satisfactory responses,** only **16.67%** correspond to **public sector entities**, and the rest **(83.3%)** are **private companies**. On the contrary, of the cases for which we did not receive a response, 55.6% corresponded to public sector entities, and 44.4% to private entities.

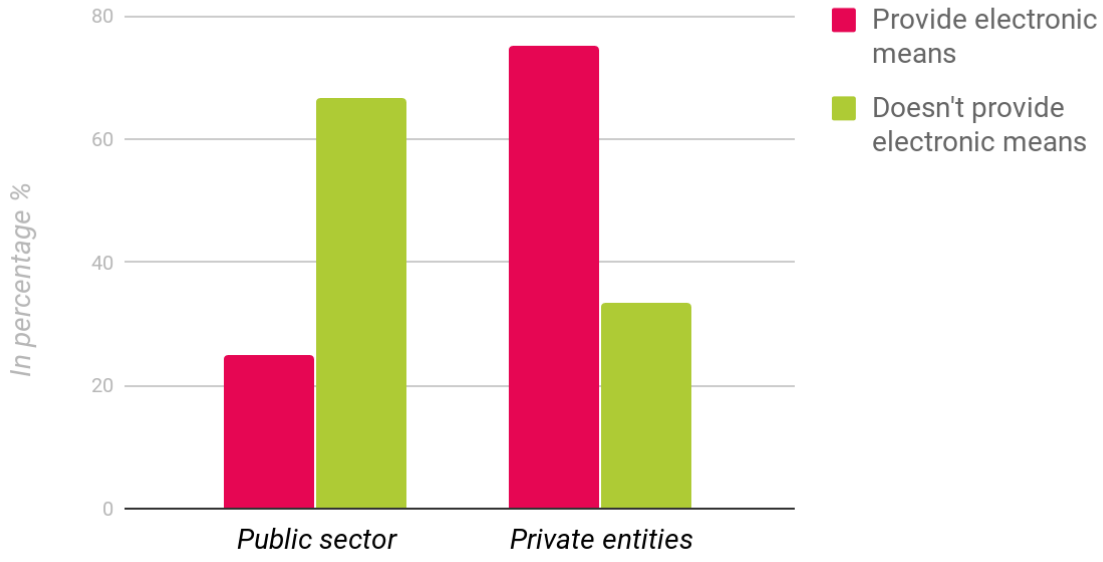
Good and bad practices (public/privacte sector)

Year 2018



Electronic means to access data

The data controller provides electronic means to excercise right of access (year 2018)



As for the option included in the new European legislation regarding providing an electronic means by which to exercise the right of access (GDPR, recital 59), in the LOPDGDD it is not considered an obligation but one more option among others. Thus, of the organizations

included in the study, **20 offer it (64.52% of entities)**, but **12 do not, that is, 38.71%.** And by sectors, **those that are not mainly from the public sector, 66.67%, compared to 33.33%** for private sector companies. As for those that do comply with this option contemplated by the law, 15 are private companies and 5 are public, with 75% and 25% respectively.

Of the cases of access to data that we request, **it is worth highlighting when we received a phone call** with questions about the reasons why this action was wanted to be carried out, which ultimately is nothing more than exercising a right: looking for what information, if we were doing it for professional or private reasons, if there had been a problem with the specific entity, etc. Thus, we experienced the trace of **mistrust and suspicion** that still remained, like those we had experienced in the previous wave of requests in 2014. In another case, they even asked us to go personally to identify ourselves. Or even the case where we received an email that could hardly be read, a plain text, with html code and using legal jargon.

Conclusion

We have somewhat improved, yes: in ac**cessing the contact data where we can exercise access rights,** going from **74% success in 2014 to 91.18% in 2018.** And we have also improved in **being able to access this data from contact through online means** (without having to visit the organization personally or having to call by phone), but we still see a fairly low level of offering the right of access by electronic means, since almost 40% do not provide it (38.71 %).

And there are still practices little related to data protection, such as the one we reported about the phone call, although in this case, since the personal interaction is less, we have only found one.

Finally, **the public sector continues to lag behind the private sector in good practices**, **but it is improving,** since it showed 90% of bad practices in 2014, and in 2018 it represented 55.6% of the entities that did not offer any response. They also continue to lag behind, as we saw in the percentages, in offering an electronic way to exercise the right of access, with respect to private entities.

Case studies – year 2104

Public sector

Border control - Schengen Information System
Requesting access to personal data was fruitful and simple in this case. Therefore, the procedure was relatively simple and straightforward, and can be considered as an example of good practice.
Police records - Ministry of Interior, General Police Directorate
Three days after we sent our letter, the data controller sent a notification informing us that our request was being processed. A month later, (slightly beyond the legal time limit for responses), their response concluded that there was no information in their files about the applicant. The letter was signed by a high-ranking officer within the department, in a formal and neutral tone.
Driving license registration
This public agency demonstrated poor compliance in terms of obtaining a satisfactory response to our request. After three attempts to obtain the desired information, we were left with few options except to file an official complaint with the national DPA. Subsequently, we received a response from the DPA in which they indicated that our access rights had been satisfied. However, we did not agree, as one of our questions had been ignored.
Europol
We submitted our request for data about us to Europol's databases through the Police. Their letter was based on a legal exemption that allows security forces to deny access to citizens. Overall, we found that this case exhibited restrictive practices. The use of complex legal jargon appeared to be used as a shield to discourage citizens from submitting follow-up inquiries.
Servei Català de Trànsit (Catalan Traffic Service)
Our first request for a phone call went unanswered. We sent a second letter adding that we would file an official complaint with the Spanish DPA if there was no response. This second letter was answered beyond the legal time limit and with incorrect information. We made an official complaint to the Spanish DPA which was forwarded to the APDCAT (the Catalan APD). Five months later, the Catalan DPA ruled that the organization should review our application and reveal our personal data, which they did.

Private sector

Mobile phone operator
The information found on the official website was clear and straightforward. The data controller responded within the legal time limit. The letter explained that they do not practice automatic decision-making processes, and that the exchange of data is limited to the actions necessary for the fulfilment of the services offered by the organization. The letter was signed but without giving any specific name or department.
Loyalty card (supermarket)
We quickly found information on how to exercise access rights on the company's website. We submitted our request and received a response within a couple of weeks. In short, we were able to exercise our rights with little difficulty and it can be said that the organization employed open and facilitative practices.
Loyalty card (food store)
The organization responded within the legal deadline, claiming that they had no data available on the applicant, even though the investigator had the "fan club" (customer loyalty) card. In a second letter, the company explained that the reason they had no data about us was because the loyalty card club's data is anonymous. We consider this case as an example of good practice.
Amazon
Two days after talking to someone on the phone, we received information about their privacy policy and passwords that were supposed to unlock a CD-ROM. The answer was incomplete, and we were unable to unlock the CD-ROM. Almost two months after our first request, we finally received the correct passwords. It contained valuable information, such as a list of recipients with whom the data is shared. This was a great example of a facilitation policy undermined by inefficient practices and poor maintenance over time.
Bank records
Information on how to exercise access rights was easily found on the official website of the organization. After sending two unanswered requests, we filed an official complaint through the Spanish DPA. During the resolution process, the bank did not contact the DPA despite having the opportunity to provide counterarguments. Therefore, the DPA found that the bank had acted incorrectly through poor administrative practices.
Facebook
The website only offered information on how to download personal data. As we did not want to do this but to submit a request to the company, we sent a letter to their European headquarters in Ireland. Several weeks later, we assumed that our request had not been delivered, as we had not received a response from Facebook or an acknowledgment from the post office. We sent a second letter saying that we would file a complaint

with DPA if no response was received. Facebook did not respond, so we filed an official complaint with the Spanish DPA. Although we had sent our request to Facebook in Ireland, the Spanish DPA responded to our complaint and contacted Facebook. After considering our complaint, and waiting for a response from Facebook, the DPA informed us that they would be in our favour.
Google
Google was another example of extremely bad practices in terms of data controller location and data protection. They responded beyond the legal time limit and their response may be considered incomplete. In the end, we made an official complaint through the Spanish DPA. A few weeks later, we received a response from DPA saying that our complaint would not be confirmed. This was attributed to the lack of information in our original complaint. This appeared to be somewhat unusual as our complaint was similar to other (confirmed) complaints that were submitted as part of this investigation.
"Advanced Passenger Information" Data system
This request had to be sent to the Netherlands (with an additional postage charge). A month later (slightly beyond legal limits), we received a second, rather short and incomplete reply. We responded asking for more information but received no response. As a result, we filed a complaint with the Spanish DPA, which told us to contact the Dutch DPA directly.
Microsoft
The online content provided by Microsoft was somewhat complicated. Although its privacy policy was easy to locate, it did not provide a way to make an access request. We did not receive a response to our first request, so we made a second attempt. This time, we received a generic email that did not consider our query correctly. We responded and asked for more information, but once again there was no response. We made an official complaint to the Spanish DPA, which then decided not to defend our complaint as we had apparently not provided sufficient information.
Twitter
The official Twitter website offered clear information, through its privacy policy, about what data they collected and for what purposes. We sent our first request by mail but got no response after the 30-day period, so we sent a second request by email. They gave us a case number, but we did not receive any subsequent response and therefore we proceeded to file a complaint with the Spanish DPA. The Spanish DPA told us to contact the US DPA. In the end, neither Twitter nor the Spanish DPA seemed inclined to resolve this issue through the use of transparent facilitative practices. Instead, the burden fell on the applicant.
CCTV (closed circuit television) in a stadium
There are two data controllers in a stadium: the football club and the local police. We submitted our first request to the Police. They asked us to provide more information, so we sent the requested documentation and they responded saying that we should send the documents to the football club. This can be considered a deterrent practice. We then contacted the football club by postal mail and received no response, so we contacted the organization again by email. The club responded by saying that they had not received the

original application (which contradicts the delivery receipt we got from the post office). After a few more attempts, we made an official complaint to the DPA regarding both data controllers.
CCTV in a public space / city centre
We were unable to locate any signs once we visited the site in person, but we were able to identify the responsible organization such as City Hall and submit our request. Several weeks after our request we revisited the site and found several new signs providing information on data controllers. Then we received a response from the city council. Their response was a single sheet of paper that was personally delivered to us at home by a courier. The lack of an envelope demonstrated how requesting information may lead to the disclosure of additional personal data. We were denied access to the images, so we requested again and received another rejection. The regional DPA did not confirm our complaint basing its response on the erasure of the images and the inability to access our registered data.
CCTV en el transporte público
Signs at the site properly identified the data controller. We sent a request to this organization and they responded within the legal time limit, but the message was not helpful and showed hostility. The delivery receipt obtained from the post office showed that the data controller had the opportunity to save these data but did not. After two more unsuccessful attempts, we submitted a complaint to the Spanish DPA. A few days later, we received a response from the customer service office where they identified the applicant on the CCTV footage. They simply described what appears on their recordings (this complies with the law). In short, they acted as if our request was useless and time consuming for them.
CCTV in a large supermarket
Although the CCTV sign was easy to locate and provided the data controller's contact details, this organization generally exhibited poor practices. There was administrative confusion when the organization received our letter. Therefore, their reason for deleting the footage was based on an inaccurate time frame. We saw this as a denial strategy. Given that we consider that they used restrictive practices, we filed an official complaint through the Spanish DPA. The DPA did not confirm our decision and said that the department store had provided the legally required response (that is, the recording cannot be viewed because it has already been erased). However, we were disappointed that DPA did not acknowledge that we had submitted the request twice. In our second request we had been especially careful with the time precisely to avoid this excuse.
CCTV in a bank
The sign on the door was clearly visible, but the CCTV operator's identification and contact details were not very legible. We submitted our request to the bank in writing and they responded by explaining that they had rejected our request because of a variety of legal obligations that state that CCTV captured in financial venues can only be disclosed to law enforcement. We asked the DPA if this was a correct reading of the law and the DPA responded in line with the bank's interpretation of its non-obligation to disclose the images.
CCTV in a government building
The signs displayed at this location were in full compliance with the law. They were visible, located at every entrance to the building and provided contact information. We submitted our request in writing and received

a response a few weeks later. The letter was not helpful, so we made an official complaint through the Spanish DPA. The complaint was transferred to the Catalan Agency for Data Protection. In the end, our complaint was rejected because the DPA found that in our request, we should have specified exactly which databases / files we wanted them to search. The DPA's decision was noteworthy, as it seemed to require that we know, before making a request, where our personal data can be located and, therefore, exclude general requests to find out if an organization processes any type of information about one's self.

Case studies - year 2018

Public sector

Cat Salut
A posted letter was sent without any response. On the other hand, there was a response from CAP Drassanes, also managed by Cat Salut (a case that we will explain below).
CAP Drassanes
The person making the request receives a call on their mobile phone, and the interlocutor identifies herself as a member of the team responsible for CAP Raval Nord, CAP to which the owner of the data was registered at for a few years. It was not the CAP Drassanes, to which the request had been addressed, but from what she explained during the call that the two centres shared some procedures or responsible teams. The reason for the call was to inquire about the reasons why she wanted to access the data, as well as asking if there had been a problem, if she had had a negative experience, or if she was doing it for professional or personal reasons. She also asked what specific data she was interested in knowing if they had. The person who made the call claimed a certain normality in this management but it was quite grotesque, since it denoted a concern and lack of normality due to the exceptional fact of precisely calling the mobile phone of the requesting person. Finally, a few days later, we received by post an acknowledgment of receipt, and a few days later another letter informing about what the data management is carried out based on the legality and related policies and where it was announced that they attached documents, like the medical history, but there was no attached file. After a few days we received the same letter, but this time with the attached files.
Passports and DNI (National Police Corps)
A letter was sent. No response was received.
Electoral Census Office
A letter was sent and in two weeks we received a letter with a satisfactory answer.
Bank of Spain
We sent the request via email. The following day we received an acknowledgment of receipt. Three weeks later we received a notice of extension of the deadline of 2 months to respond to us (we actually received it in 3 different emails from 2 different addresses), arguing that the request was very vague and that the Bank of Spain is a very complex entity: "in response to the complexity of the application due to the diversity of processing carried out by the Bank of Spain and the lack of specificity of the application". Towards the end of

this period we received a reply. And the following day we received an extension of the information provided the day before.
Police records - Ministry of the Interior, General Directorate of Police
A letter was sent. No response was received.
Europol
We sent the request and after almost two months, we received a response by post.
Border control - Schengen Information System
We sent an email. We received no reply.
High school
We sent a request. We received no reply.
Sciences Po (Paris)
Request made via email. After 15 minutes we get a short response from the automated assistant, saying that access requests are automatically sent here and that we should contact Sciences Po's administrative services, and they provided an email. We contacted them and received an automated response saying that the administrative services were currently very busy and that they will respond when they can. We received no further response.
UCL (University College of London)
We received an automatic response: "If you have made an access request, please consider this email as a receipt notice and you should receive a response from us within the next 40 days" (40 days seems to be beyond the one month period established by law). Later we receive another email requesting an identity document and more specific information about what type of data we are requesting (if a specific document, or the correspondence of e-mails, and if not, that we specify the departments or the names of the people who could have data of the person concerned, as well as if we could specify a period of time for which we were looking for information).
Driving license registration

We received an email where we were informed of the data they had, in a clear and explanatory document. In this case, we sent the request by post, and we received the response in digital form to the e-mail address provided in the request.
Gaudir+ Program (Barcelona City Council)
We made a request via postal mail since we did not find access to how to do it on the website (currently we have found that you can reach a form after a few clicks if you visit the Legal Notice section at the bottom of the page). In any case, when we sent the request, it was returned to us with a response saying that the request does not meet the requirements since it is required to attach a copy of the DNI and they also asked that given the large amount of data that exists in this public body, we must specify what data we want to obtain information from.

Private Sector

Twitter
Once the form had been filled out and sent, the same day they sent us an acknowledgment of receipt. The next day they sent a reply email, indicating how to access the data. Quick and satisfactory response.
Equifax
Sent a request via email. In less than a week they sent back an email with the answer.
Experian
Sent by email, and within the term we received a response containing an encrypted file with the requested data, of which they sent the password for in a second email.
Loyalty card (food store)
The request was sent. We got no response. It so happens that the website has a section dedicated to privacy but does not contain information on how to exercise ARCO rights (among which are the rights of access), it also says that it facilitates the privacy policy but where there should be a link or a file to download, it appears written in parentheses "it's the other file". I is obviously a mistake, but it shows how necessary it is to refine the data policy of this company.
Loyalty card (supermarket)

At the time of making the request we were unable to find any contact on their website.
Mobile phone operator
A letter was sent. No response was received.
Bank records
The form did not accept the postal code of Spain and could not be sent.
Private primary school
Once the request was sent, they responded by asking us to go in person to identify ourselves.
Sage Publishing
Request sent. No response
Facebook
Accessed, information was correct.
Microsoft
Accessed, information was received correctly.
Google
Once the online request was made, we received the file with the data the same day. Data classified in different categories, not too useful.
Mozilla
July 2018. Impossible to find a place to exercise access rights, apart from an address in the US, even with the company's pro-privacy marketing. There is no point of contact anywhere.

Eurotunnel
Request made via e-mail. They responded right away saying that they had looked at the database and could not find anything about the requesting person. They also asked to provide information on what specific data they should have, and if the person holding the request could provide their identity document, which would be erased immediately.
WhatsApp
Request made via web. Through a link we gained access to download the data, which we obtained without problem in a complete report after three days.
Protonmail
Request made via email. The legal team responded the same day explaining where we could access to find the different types of data and for what purposes they have them. They specified that the data included is always and only that entered by the user, and that this information is never shared with third parties, except when required by Swiss law (in research cases).
Idealista
We sent the request by email and we received the response within the deadline, in an HTML text format that is not easy to read. They explained their legal obligations, and they responded to each point in a generic way that tried to demonstrate that they comply with the law. One of the most difficult answers to read that we have received, although in short it could be understood. But the presentation was very messy.
Amazon
Request sent by email. They sent a response the same day saying that we could access more information through the options of the account's configuration, with instructions: "If you require further personal data, you can log into your account to verify your identity and submit your request. You can submit this request through the "Contact Us" page in your Amazon customer account after logging in: https://www.amazon.co.uk/gp/help/customer/contact-us Once there, click on "Prime and more ","" Tell us more about your issue ","" request my data, "and follow the instructions."
Aparcaments Garví (private parking)
Once the request was made, we received a letter requesting the DNI, once we sent it, we received another letter detailing the personal data they have of the person who has made the request. Complete and correct information provided.
Political party
Sent letter by post requesting access to the data. We received no reply.

Insurance company
We received a letter within the terms established by law informing us that our request for access does not meet the necessary requirements to prove the identity of the person affected, and they asked us to send them the request with a copy of the ID or residence permit.