
Article:
L'Hoiry, XD and Norris, C (2015) The Honest Data Protection Officer's Guide to Enable Citizens to exercise their Subject Access Rights: lessons from a ten-country European study. International Data Privacy Law, 5 (3). pp. 190-204. ISSN 2044-3994

https://doi.org/10.1093/idpl/ipv009

Title: The Honest Data Protection Officer's Guide to Enable Citizens to exercise their Subject Access Rights – Lessons from a Ten Country European Study

Authors: Xavier Duncan L'Hoiry (University of Leeds) & Clive Norris (University of Sheffield)

Article Category: Article

Summary:

- This article describes a ten-country European study investigating the practical aspects of exercising access rights from the perspective of data subjects.
- It uses a mixture of quantitative and qualitative methodology to illustrate the restrictions faced by data subjects in exercising their access rights.
- It concludes by making key recommendations to assist data subjects in their attempts to exercise access rights.

Key Words: Access Rights; ARCO Rights**;** Data Protection; Privacy; Subject Access Request; Surveillance

1. Introduction

Access to personal data is the natural pre-condition of data subjects' ability to exercise the remainder of their ARCO rights (access, rectification, cancellation, opposition). Put simply, citizens cannot exercise their rights of informational self-determination in an informed and conscious manner without knowing what is held about them. The importance of informational rights is set to grow. This is true not only because of the Snowden revelations as to the mass surveillance activities of the state, but also in the wake of recent judgements concerning various aspects of data protection and privacy such as data retention protocols and the so-called right to be forgotten[1].

For data subjects to be able to exercise their rights and for informational self-determination to work in practice, citizens, in their role as data subjects, must be able to find out what personal data is stored about them, have access to this data and be able to know how this is processed and with whom it is shared. In the European Union, the EU Charter of Fundamental Rights highlights the right of citizens' access to their personal data as a component of Article 8's protection of personal information. Moreover, EU Data Protection Directive 95/46/EC[2] (hereafter 'The Directive') empowers citizens to exercise this right by explicitly granting

[1] See for example *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12 on the right to be forgotten. Full judgement available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=260714#Footnote*. See also Joined Cases *Digital Rights Ireland Ltd* (C-293/12) *v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission,* and *Kärntner Landesregierung* (C-594/12), *Michael Seitlinger, Christof Tschohl and others,* on the invalidity of the Data Retention Directive 2006/24. Full judgement available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281 , 23/11/1995 P. 0031 - 0050*

them the right to submit a subject access request to any organisation that holds their personal data.

Previous research and jurisprudence exists at national and supranational levels across Europe concerning informational rights law and specifically the right of access. However, the majority of this has been focussed upon various aspects of the law rather than the *practical* enactment of the law from a citizen's perspective. For instance, the European Court of Justice (ECJ) and the European Court of Human Rights (ECtHR) have both emphasized the fundamentality of the presence of an independent and impartial authority in mediating disputes between data subjects and data controllers[3]. In *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* meanwhile, the ECJ took a wide interpretation of the extent of the right of access, ruling that that the exercise of access rights not only relates to the present but also refers to the past[4]. At national levels, courts have attempted to clarify problematic aspects of the interpretation of the Directive into national legislation. Some national courts, such as those in Germany and Hungary, have tended to interpret informational, and specifically access, rights broadly[5]. However, others, most notably in the UK, have interpreted access rights exceptionally narrowly, removing many obligations from data controllers[6]. Elsewhere, research conducted by the likes of Korff[7] and Rempell[8] has investigated facets such as the implementation of the Directive into national legislative frameworks. Gellert and Gutwirth[9] have attempted to research access rights from the perspective of data controllers. Most recently, the European Agency for Fundamental Rights (FRA) has investigated the obstacles faced by data subjects in attempting to access redress mechanisms when faced with abuse of their informational rights[10]. These restrictions included a consistent absence of expertise in data protection and privacy issues throughout the legal landscape. Similarly, FRA has researched the role of Data Protection Authorities (DPA) in attempting to strengthen informational rights in Europe[11]. The study found a series of deficiencies at national levels amongst DPAs including a lack of resources, funding and limited powers.

---

[3] See for instance the following cases: ECtHR, *Leander v. Sweden*, application no. 9248/81, judgment of 26 March 1987; ECtHR, *Gaskin v. the United Kingdom*, application no. 10454/83, judgment of 7 July 1989; ECtHR, *M.G. v. the United Kingdom*, application no. 39393/98, judgment of 24/12/2002; ECtHR, *Odièvre v. France*, application no. 42326/98, judgment of 13 February 2003.

[4] ECJ, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, case C-553/07, 7 May 2009.

[5] See for example Bundesverfassungsgericht, decisions volume 65, p. 1 ff; Metropolitan Court 26.K.32.704/2012/5.

[6] See for example *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

[7] Korff, Douwe (2002) *EC Study on Implementation of Data Protection Directive 95/46/EC – Report on the Findings of the Study*

[8] Rempell, S. (2006) 'Privacy, personal data and subject access rights in the European Data Directive and implementing UK statute: Durant v Financial Service Authority as a paradigm of data protection nuances and emerging dilemmas', *Florida Journal of International Law,* 18: 807-842

[9] Gellert Raphaël, and Serge Gutwirth (2012) "Citizens access to information: the data subject's rights of access and information: a controllers' perspective", in PRESCIENT, Deliverable 3, *Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data*

[10] European Union Agency for Fundamental Rights (FRA) (2013) *Access to data protection remedies in EU member states* & European Union Agency for Fundamental Rights (FRA) (2011) *Access to Justice in Europe: an overview of challenges and opportunities*

[11] European Union Agency for Fundamental Rights (FRA) (2010), *Data protection in the European Union: the role of national Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*.

This previous literature has examined the law in books and the structural problems of enforcement but what has not been subject to scrutiny is the practical enactment of the right of access from the perspective of the citizen. This paper seeks to begin the process of filling this gap.

Whether a data subject is able submit a subject access request is an empirical question, but it is a fundamental one in being able to exercise their rights. To be able to exercise one's right, one must be able to identify a person or office within an organisation who has been tasked with the responsibility to respond to their request.

The right of access is a legally enshrined right: all members of the European Union have had to transpose the Directive into their own national law. It is therefore incumbent on organisations to assist data subjects in making requests about what data is stored about them, how it is used, how it is processed and with whom it shared. Whilst there are legal exemptions, data subjects have a legal right to be informed of the grounds as to why their requests cannot be fulfilled.

The legal definition of data controllers can and often does include organisations in and of themselves. As such, an organisation collecting person data *is* the data controller rather than an individual or a department/office within that organisation. For the purposes of this research, we sought to locate those individuals and/or offices specifically responsible for responding to subject access requests. This is because simply identifying an organisation as being a data controller is of very little practical help for data subjects seeking to exercise their informational rights. As such, where the analysis below discusses locating data controllers, this should be taken to mean locating specific contact information (i.e.: geographical/postal/email address) for individuals and/or offices tasked with processing and responding to subject access requests. Without locating this type of information, it becomes extremely difficult (if not impossible) for data subjects to exercise their access rights.

With this in mind, we have sought to deconstruct the processes and dynamics of exercising one's right of access to personal data. We begin from the assumption that data subjects believe that their personal data is collected by organisations that they interact with, but have less certainty as to what is retained and how this is then used. From this starting point, citizens must first be able to identify to whom they should make a request to access the data that an organisation holds about them, and secondly to determine the process they need to follow to submit a request. Data subjects will therefore need to be able to:

- Identify the data controller who is legally responsible for the care of one's data.
- Identify where a request should be submitted (i.e.: if there is a specific department/officer to whom to address access requests)
- Determine *how* to submit a subject access request (i.e.: online, via post, etc)
- Determine if the data controller in question processes requests in a particular way (i.e.: via templates)
- Determine the cost of making such a request
- Find out if there are time limit obligations on either the requester or the data controller
- More generally, data subjects will need to know, before submitting a request, the range of data that is collected and stored about them in order to decide whether they wish to proceed with an access request and incur the associated costs of time and money that arise from such requests

With these considerations in mind, this paper presents the findings of a ten country European research project which sought to collect data demonstrating how citizens might fare in their attempts to locate information enabling them to submit access requests and thus begin to exercise their informational rights. We start by presenting a brief summary of our overall research findings.

Following an outline of the key findings of the research, this paper focuses on the key recommendations emerging from the research. In the context of these recommendations, the findings from the research are presented, outlining how and why the key recommendations have arisen and how these can lead to greater opportunities for data subjects to exercise their right of access.

2. Methodology

The sampling strategy for this research was based upon the two central tenets. Firstly, the research sought to include a broadly equal representation of public and private sector organisations in order to (partly) compare the findings of the research along this axis. Secondly, the sampling strategy was based on the notion of selecting sites in which the data subject comes into contact with organisations/data controllers who collect and store the subject's personal data on a systematic and habitual basis (i.e.: daily/weekly/monthly/annually).

As Table 1 shows (*Domains and sub-categories included in sample*), the research sites were drawn from ten socio-economic and legal domains within which three/four specific categories were identified, leaving a total of 35 potential site categories for researchers to investigate. This sampling method sought to encompass a wide range of data drawn from different sources. The end result was that many different types of organisations were investigated in the research from large multi-national companies to small independent organisations located in both the public and private sector. Moreover, the organisations investigated collected and processed different types of personal data including digital data, data held in hard copies and CCTV footage[12] - all of which can be defined as personal data according to European and national legislation. Researchers were instructed to select a minimum of 30 sites from across the ten domains.[13] Researchers were then tasked with pursuing the following sampling/selection strategy to identify specific research sites:

a) Pick the site geographically closest to your place of work or your home – i.e.: the school closest to your place of work.
b) If the above does not apply, pick the site you would usually use – i.e.: the search engine you normally use.
c) If the above does not apply, pick the national market leader – i.e.: the insurance provider national market leader.

For example therefore, the sampling strategy underwent the following process:

Domain: Education → Site category: Secondary school records → Specific site: local secondary school

[12] Attempting to locate data controllers who process different types of data can raise different issues. For instance, the issues raised by sites using CCTV surveillance may lead to context-specific recommendations. The authors acknowledge this and indeed sites of CCTV surveillance are dealt with specifically where appropriate in the recommendations below.

[13] Some research sites did not exist in some countries hence in some cases it was not possible for researchers to investigate some sites i.e.: ID cards exist in most countries but not the UK.

In total, 327 individual cases were investigated by researchers. These included 236 websites visited across the research and this figure includes instances where interaction with data controllers was carried out via email. In a small number of cases, the same websites were visited by researchers in different countries (i.e.: multinational organisations such as Facebook and Google). These are counted as separate cases as the issues faced by one researcher in one country tended to be different to those faced by another researcher in a different country[14]. Researchers also attempted to locate data controllers by telephone in 91 cases while in 50 cases[15] researchers visited a physical location in person to try and locate a data controller. In some instances, cases are double-counted since researchers will have 'failed' to locate the data controller using one method and as such will have tried again using a different method(s). As such, one research site may be counted as many as three times in the research but this is a relatively rare occurrence. The lowest number of sites investigated per country was 30 by researchers in Spain and the highest was 35 by researchers in Belgium with an average of over 32 sites investigated per country during the research. Where the analysis below discusses country-specific findings (for example: 'in the UK...') this should be taken to mean that the researcher(s) was based in the UK and the fieldwork was undertaken from this country although some research sites operate across national boundaries (such as multi-national organisations like Facebook and Amazon).

In order to explore the experiences of data subjects in attempting to locate data controllers, researchers were asked to place themselves in the shoes of a lay person – a role of 'citizen researchers'. In many cases, researchers had conducted previous research regarding data protection, privacy and access to personal data. Indeed, some researchers had conducted or were aware of previous research regarding specific sites within this study (such as Facebook[16]). With this in mind, in most cases researchers could therefore use their expertise in data protection matters to locate data controllers with relative ease. However, this would not reflect the experiences of the lay person who may need to browse a website for several minutes before finding the relevant content. Similarly, an expert researcher may instinctively know where CCTV signage is likely to be located but a lay person may need to spend several minutes searching for such signage. The results below therefore reflect as best as possible the experiences of the lay person although it of course impossible to remove all trace of the individual researcher's inherent expertise and experience of previous study in this field.

Linked to the notion of 'citizen researchers', the methodology also guided researchers to pursue whichever method of locating data controllers (online, via telephone or in person) they preferred. Where one (or more) methods failed, researchers would need to pursue an alternative method until all avenues were exhausted. It was envisaged that such a methodology would allow researchers to tailor their approaches in tune with country-specific cultural nuances and conventions.[17]

---

[14] For example, content on such websites was often offered only in English. As such, a researcher from an English-speaking country is likely to find it easier to locate data controller contact details than a researcher from a non-English speaking country.

[15] All 50 of these cases concern CCTV sites.

[16] See for example the campaign entitled Europe v Facebook which seeks to challenge Facebook over its privacy practices and in particular its failure to disclose personal data when requested to do so by citizens. http://europe-v-facebook.org/EN/en.html . This initiative led to the Irish High Court referring the case to the European Court of Justice in June 2014 (Maximillan Schrems v Data Protection Commissioner [2013 No. 765JR]). Most recently, the campaign has filed a class action against Facebook which is set to be heard in Austria in April 2015.

[17] Finally, researchers were also tasked with providing ratings for certain indicators of online, telephone and face to face interactions. The rating levels (poor; adequate; good) were to be determined based on an objective

3. Overall findings: is it possible to locate data controllers?[18]

The overall average success rate of locating information about data controllers was 80% across the entire study, as per Table 2 (*Success rate in locating data controllers*). Conversely, in around a fifth of instances, it was not possible to locate the contact details of the data controller. This suggests that in a substantial minority of cases, unless citizens are prepared to submit a formal complaint to the relevant DPA, it is simply not possible for them to locate a data controller or their contact details in order to proceed with a subject access request. Data subjects are effectively disenfranchised in being able to make clear and informed decisions about their involvement in surveillance/data collection practices.

Of all the cases where data controllers were successfully located, Table 3 (*How were data controllers' details located?*) shows that the majority (63%) of these were located online. Using the telephone and visiting physical locations of surveillance (i.e.: sites in which CCTV cameras are located) in person accounts for just over one third of all cases in which researchers were able to locate data controller details. This indicates that access to the internet and to organisations' websites is important if one wishes to successfully identify data controllers. This also means that those people with limited or no internet access or those with little or no computer literacy are at a significant disadvantage. As such, elderly and low-income persons are most likely to be disadvantaged given their potential lack of computer literacy or their limited access to the internet. This potential drawback is arguably especially pronounced in the UK, where 86% of successful cases involved the use of online methods. Similarly, 81% of data controller details were located online in Germany and 76% in Slovakia.

While online and telephone enquiries were successful in over two-thirds of cases overall, this was not true of in-person enquires. This disparity was particularly evident for researchers in Austria, Hungary and the UK, where only a single query in each country made in person resulted in a positive outcome. For researchers in Luxembourg it was not possible to locate data controller contact details by visiting the physical location in person (i.e.: where CCTV cameras are physically located) in any case at all.

Table 4 (*Success and failure rates of locating data controllers according to method used*) shows that in less than half of all cases where a physical location was visited in person were researchers able to locate a person or office to contact within a data controller's organisation (43%). This represents the highest 'failure rate' of any of the methods utilised in this study. In total, only 26 out of 262 data controller details were located by attending a location in person. This indicates several things. Firstly, the level of knowledge and expertise of representatives of data controllers to whom researchers spoke when attending physical locations in person is low. Their inability to answer questions about the data controller and subject access procedures meant that researchers were either unsuccessful or sought alternative methods to locate the required information. It also shows that in some cases, representatives of data controllers were simply unwilling to divulge the required information to data subjects and undertook strategies of avoidance and denial in order to re-direct the query. In the UK for example, members of staff frequently (and incorrectly) informed researchers that the

---

list of context-specific considerations dependent on the type of interaction involved. These indicators are outlined in greater detail below. However, alongside these objective guidelines, researchers were also expected to consider their subjective experiences given the auto-ethnographic nature of the research methodology and the above-described 'lay citizen' persona researchers were asked to act out. With this in mind, the rating findings outlined below should be considered as a conflation of both objective and subjective considerations.

[18] All numerical data is rounded up to the nearest whole number.

organisation in question never disclosed the type of data (i.e.: CCTV footage) requested. Elsewhere, in Norway members of staff incorrectly repeatedly argued that only certain authorities (such as the police) could obtain access to certain types of data.

In the remainder of this paper we are going to spell out our key recommendations as to what Data Protection Officers and organisations in general can do to ensure that data subjects are facilitated in exercising their right to submit a subject access request. Although these recommendations may seem to be obvious, and plain common sense, as we will illustrate with the findings from our research, good practice is often times elusive.

4. Key Recommendations

4.1 Data protection and privacy links should be clearly visible and easily accessible on organisations' homepages

The main method of locating a person or office within an organisation whose responsibility is to respond to access requests during the research was by visiting official websites and analysing the privacy policies or data protection content of individual organisations. This is an inevitable consequence in the globalised world of contemporary social and non-social interactions which increasingly take place in a virtual rather than embodied world.[19] In some cases, such as Facebook, Amazon and Google, which offer their services entirely via an online platform, it would seem unnatural to seek out information about such organisations in any way other than via their online presence.

Organisations can hinder or facilitate data subjects' attempts to find and view privacy policies and associated details about how to request their subject access rights. By creating well designed web-pages which are easy to navigate, relevant content can be quickly located and accessed. However, the poor design of online platforms can also lead to information being 'buried' amongst masses of irrelevant content, rendering users' navigation lengthy, confusing and often circular. In order to effectively analyse how data controllers disseminate their data protection/privacy content online, researchers in this phase of the research were tasked with documenting several indicators which, taken together, indicate the ease or difficulty of locating data controller information.

One indicator of the ease/difficulty of locating data controller details online is the length of time this process takes. In simple terms, the longer one must browse a website, the poorer the design of the website and the poorer the visibility and prominence of the relevant privacy links are.

Where the data controller contact details were sought on organisations' websites, as Table 5 (*How long (in minutes) did it take to locate data controller details on organisations' websites?*) shows, in only 34% of all cases was this located within 1-2 minutes. In direct contrast, in 39% of instances, it was necessary to browse a website for 5 minutes or longer before finding data controller details. This perhaps raises questions regarding the visibility of privacy-related links on websites as well as the quality of the content available. Linked to this is the possibility that data controller information is 'buried' amongst content within organisations' privacy policies. Some country-specific findings are particularly poor in this context. In the UK, not a single case was evidenced in which it was possible to locate data controller information within 1-2 minutes. Meanwhile, in 71% of cases it was necessary to browse a website for 5 minutes or more in order to locate data controller information. Worse

[19] Lyon, D. (2001) Surveillance society: monitoring everyday life. Buckinghamshire: Open University Press

still, in Italy, researchers spent 5 minutes or more locating data controller information in 93% of cases. This means that well over two thirds of organisations investigated in the UK and Italy demonstrated what may be termed as bad practice in terms of website design and navigation. The results in Austria offer a stark contrast to this picture however. Here, a significant majority (83%) of data controller details were located within 1-2 minutes of browsing a website. This indicates very good practice in the design and content of the websites visited.

Similarly, the number of 'clicks' required to successfully locate data controller information is also indicative of the ease or difficulty of navigating an organisation's website before accessing the desired content. Put simply, the fewer the number of clicks, the easier the content is to access. A (deliberately or otherwise) poorly designed website may 'hide' content behind several pages and contain links to irrelevant data. Although challenged by some commentators[20], the 'three-click rule' requires that users should always be able to locate the desired information within three click completions[21]. As such, if data controller details are only available after four or more clicks, this suggests that an organisation is actively trying to discourage citizens in exercising their rights.

As per Table 6 (*Number of 'clicks' required to reach privacy/data protection/subject access content on organisations' website*), in over a fifth of cases (22%), researchers were able to locate data controller information in just a single click. This can be considered to be best practice. Meanwhile, in just over half of all cases, the details of a data controller can be found within 2-3 clicks (53% of cases). This can be taken to represent good (if not best) practice. However, in the remaining 25% of cases, it is necessary to complete at least four clicks in order to locate such content. Indeed, in 11% of cases, it takes more than 6 clicks to locate this information. Overall, this means that in a quarter of all cases, it is highly questionable whether the average data subject would be able to locate crucial information concerning privacy and data protection policies. Even if they did locate this content, great time and effort would need to be expended in order to do so.

This poor practice indicates that in a significant minority of cases, privacy-related content is given little prominence on organisations' websites which effectively forces users to pro-actively 'dig out' this information, a task which may be time consuming and reliant upon the individual user's level of computer literacy.

Researchers were also tasked with rating the visibility of data protection/privacy links on organisations' websites. While researchers made an individual overall judgement of their own experiences, these judgements were objective to the extent that they were based on detailed protocols to determine how a page should be ranked[22]. In the case of rating the visibility of data protection/privacy links, researchers were asked to consider where is the link located on the webpage; whether the link is located where one might reasonably expect it to be (i.e.: at the bottom of the page with the other 'small print' and legal information); and the size colour of the font (i.e.: does the link fade into the background of the other colours on the webpage).

---

[20] See for example Hammill, D. (2009) 'Stop counting clicks' available online at http://www.uxbooth.com/articles/stop-counting-clicks/

[21] Zeldman, J. (2001) *Taking your talent to the Web: A guide for the transitioning designer*. Indianapolis, IN: New Riders

[22] Further details on the methodological protocol of the research can be found here: http://irissproject.eu/?page_id=9

The overall trend shows that the visibility of data protection/privacy content links on websites is most commonly rated as 'adequate' and this was the case just under half the time (46%), according to Table 7 (*Rating given to the visibility of the data protection/privacy link on organisations' website*). This usually meant that whilst privacy links were given little prominence in the design of websites and were located at the bottom of web pages in relatively small font, this was also where users can generally expect to find such links given the expectation that, generally speaking, this is where 'small print' is usually located in most website designs.

Over a third of all links (37%) were also rated as having 'poor' visibility which contrasts to just one in five links rated as having 'good' visibility. Poor visibility restricts data subjects' ability to exercise their rights insofar as it 'hides' the information required to actually go ahead and practically exercise informational rights. While the UK found less instances of 'poor' ratings (18% in the UK compared to 37% overall), significantly fewer instances of 'good' ratings were evidenced (only 6% in the UK compared to 18% overall). So poor was the visibility of privacy links in some countries (i.e.: Slovakia) that researchers could not find a single example of 'good' visibility while in Spain, Italy and Belgium only one example of good 'visibility' was found in each country.

4.2 Organisations' websites should include information on what type of data is collected and stored

For data subjects to exercise their right of informational self-determination, they need to be aware of what type of data is collected, stored and processed about them. Without such information, citizens are arguably unable to determine whether they should make an access request simply because they do not know what type of data may have been collected[23]. This information is not only basic but it is also important in notifying data subjects of the extent of the personal data processing practices to which they are subject when they enter into an agreement with a particular organisation. Overall, only half of organisations' websites informed citizens as to what data was collected about them how it was then stored and processed. Without this information it is not possible for citizens to decide as to whether they want to demand full disclosure by submitting a subject access request. They simply do not have enough information.

In Germany, Hungary and the UK, the vast majority of websites visited did in fact provide such information (94%, 90% and 88% of websites respectively). This is in stark contrast to their European neighbours such as Luxemburg, where only a quarter of organisations provided such information (25%), and most significantly of all, Belgium, where not a single case was found in which such basic information was provided.

4.3 Privacy policies should include a template via which to submit a subject access request

A good template facilitates a subject access request. Templates can provide the data subject with a recognisable format through which to make a request; provide procedural information such as the type of documentation to accompany a request and; indicate the costs of making a request and how to pay these costs. The provision of a template therefore generally represents good practice both administratively and in light of compliance with data protection

[23] It may also be argued that a proportion of potential requesters would be satisfied if they were made aware, via an organisation's privacy policy, what type of data was (and was not) collected and consequently would discontinue their interest in requesting their personal data.

legislation. The provision of templates may also illustrate an organisation's good procedural practice insofar as ensuring that access requests are received in a uniform, recognisable format, making the processing of such requests easier for data controllers themselves.

Despite the value of templates in facilitating access requests, they are only available 18% of the time. While neither European nor national legislation concerning data protection make the use of templates compulsory, several national DPAs' guidance to data controllers includes the suggestion that the provision of templates demonstrates good practice and an open and pro-active approach to enabling data subjects' access to their personal data[24]. As a result, the unavailability of such templates in 4 out of 5 cases is a significantly negative finding. In Hungary and the UK, researchers found that templates were available in 44% and 41% of cases respectively. While these are the best results across the study, they still represent less than half of the sites visited. Moreover, while no country found zero sites providing templates, several countries found only a single site which provided a template through which to make an access request (Belgium, Luxemburg and Spain).

4.4 Privacy policies should never be made available only *after* a user has signed in to a registered members section

If data controller information is only available once users have registered with a website, their ability to exercise informational self-determination is compromised. Put simply, data subjects must be able to access information about data processing practices *before* giving their personal data by registering for a service. Making this type of information available to users only *after* they have already provided their personal data renders data subjects' right to make informed choices about their data obsolete.

The research showed that privacy-related information was available without having to register and log-in to a 'members only' portal in 95% of cases. But in 7 cases (5%) the details of an organisation's privacy policy and how to make a subject access request was only available behind a 'members only' section. This prevents citizens form making informed choices prior to submitting their personal data to an organisation.

4.5 Privacy policies should include full details of how to make a subject access request including how to make an access request and whom to address it to

The quality of information available on organisations' websites obviously affects data subjects' ability to exercise their access rights. A website providing clear and unambiguous guidance regarding what access rights are and how they can be exercised will invariably lead to greater ease for users in their attempts to enact these rights. In contrast, online content lacking such guidance or providing only general and/or highly complex information is likely to obstruct data subjects' attempts to exercise their rights. During the research, researchers were tasked with rating the information located online in order to determine whether this content could be deemed as helping data subject to arm themselves with sufficient information in order to exercise their right of access. In assigning ratings to the quality of the information provided online, researchers considered whether there is any mention of specific national or European legislation; whether there is any mention of time limits or other data controller obligations; whether there is any mention of the financial cost of making a request; and whether there is any mention of the format of making a request (i.e.: in writing/verbal?);

---

[24] See Information Commissioner's Office (2013) 'Subject Access Code of Practice' available at http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.pdf

whether any information is included regarding the right to appeal against a decision made by the organisation regarding accessing one's personal data.

As Table 8 (*Rating given to the quality of information given in the data protection/privacy section of organisations' websites*) shows, in only a fifth of cases did researchers judge the quality of information to be 'good' (20%). In around half of the cases, it was deemed to be 'adequate' (48%) but in nearly a third of all cases, the content of privacy policies was rated as being 'poor' (31%). In Germany, not a single instance of 'poor' information was found by researchers and indeed, almost half of all sites were rated as providing 'good' levels of information (47%). In the UK meanwhile, 47% of online content was rated as 'good' (compared to 20% overall). Moreover, only 18% of content was rated as 'poor' (compared to 31% overall). Whilst far from perfect, these results compare favourably to those gathered in Italy, Slovakia and Spain, where researchers could not find a single example of a 'good' level of information being available on an organisation's website. In Luxemburg and Belgium, researchers found only one such example and indeed, Belgium found that the vast majority of websites gave 'poor' quality information (84%).

4.6 If organisations choose to direct data subjects to telephone numbers for data controller information, this should be a simple process and only involve speaking to one person

In several instances, it was necessary to contact data controllers via telephone. Across the entire study, this was the case in more than a quarter of all successful attempts to locate data controller information (26%). As with online-based searches, the amount of time taken to locate a data controller when speaking on the telephone is indicative of the ease or difficulty with which this information is available. Theoretically, the shorter the time one spends on the phone before obtaining the requested information, the easier it is to access. Conversely, those spending a lengthy amount of time before receiving the information may find that their request was harder to fulfil and the several minutes on the phone may have been spent speaking to several people and attempting to negotiate access to the relevant information.

On average, Table 9 (*How long (in minutes) did it take to locate data controller details when enquiring on the phone?*) shows that data subjects receive the requested information when speaking to people on the phone within 5 minutes almost half the time (46%). While this may indicate that locating data controller details on the phone was relatively easy, the results also show that individuals are likely to have to spend more than 10 minutes on the phone in more than one in five cases (21%). Taking this and the results of the 6-10 minutes category together, data subjects are also likely to spend over 5 minutes on the phone in more than half of all instances (54%). This has particular significance when considered in light of the cost of premium telephone numbers as well as the more abstract argument of how deeply a data subject should have to 'dig' in order to obtain the level of information required in order to exercise their citizen rights. As argued above, data controller contact details and information about how one may submit a subject access request should be easily accessible information. For data subjects to spend more than five minutes on the telephone (bearing in mind that they may have already browsed an organisation's website or visited a physical location in person) is a significant burden placed upon the individual.

Some country-specific results are noticeably poor in this context. The UK was particularly bad: not a single successful case was concluded on the telephone within 1-5 minutes. So too was Norway, where the requested information was available within 5 minutes in only 20% of cases and researchers had to wait over 5 minutes in 45% of cases and over 10 minutes 35% of

the time. The UK also totalled the second highest mean average amount of time spent on the telephone, illustrating the poor performance of UK and Norwegian-based organisations compared to their European contemporaries. For example, in Germany, Italy and Slovakia, the requested information was received within 5 minutes in every instance.

4.7 Telephone numbers provided for data protection and privacy queries should be directed to a member of staff with requisite knowledge and expertise to answer queries of this nature

One way to ensure that time spent on the telephone is conducive to citizens exercising their rights is to ensure that telephone numbers are directed to members of staff with the requisite levels of expertise to be able to answer data protection and privacy-related queries. If, however, one needs to speak to several respondents before finally obtaining the correct information, this is indicative of not only a lack of knowledge and expertise on behalf of the first (and perhaps several more) respondent(s), but also that the data controller has directed data subject queries towards a respondent who is unable to answer these queries, thereby demonstrating poor organisational practice.

At a pan-European level, it was only possible to obtain the relevant information by speaking to a single respondent on the phone in half of all cases (50%). However this hides considerable variation at the nation level. In Slovakia for example, researchers were able in 100% of cases to locate information by speaking to only one person. Moreover, in 4 of the 10 countries, it was *never* necessary to speak to 3+ people and indeed this only occurred in a single case in the UK, Austria and Belgium respectively.

Researchers were also tasked with rating the quality of information they received when making telephone queries. This in part enabled them to determine whether the respondents had received the required level of training to correctly and accurately provide advice regarding data protection and privacy queries. In order to assess the quality of guidance received when contacting organisations on the phone, researchers were asked to consider the following guidance: whether the phone respondent had data controller contact details; whether researchers were advised on time limits or other data controller obligations; whether researchers were advised about the cost of making a subject access request; and whether researchers were advised about the preferred format of making a request (i.e.: in writing/verbal).

Despite the fact, as outlined above, that some researchers spoke to several different respondents before obtaining the desired information on the telephone, Table 10 (*Rating given to quality of information about data protection, privacy and subject access received on the phone from organisations' representative(s)*) indicates that generally speaking, the level of information received was often 'good' (this was the case in 34% of instances). Elsewhere, advice received on the phone was of 'adequate' quality in 39% of cases. This means that in the vast majority of cases (73%), data subjects will receive information of a sufficient quality to enable them to exercise their rights. However, it also means that in over a quarter of cases (27%), data subjects receive a 'poor' level of information which compromises their ability to exercise their informational rights.

Some countries demonstrated particularly positive findings here. In Austria and Germany, it was found that researchers received 'good' quality information 80% and 100% of the time (respectively), demonstrating a high level of data protection and privacy expertise on behalf of telephone respondents. In the UK, two thirds of cases showed 'good' levels of information were received and indeed researchers in the UK did not experience any 'poor' examples of

the level of information provided. In contrast, in Slovakia, Spain and Belgium, not a single example of 'good' levels of information was received.

4.8 Signage should always be displayed to advise citizens that CCTV surveillance is in operation

In order to locate the data controller of CCTV systems, researchers visited areas which had CCTV systems in operation. This in part enabled the researchers to assess whether such systems were compliant with legislation and guidance concerning the presence, purpose and content of CCTV signage. In particular, one should be mindful of legal requirements in *all* of the countries within this research which demand that signage is displayed in sites where CCTV systems are in operation. It is also a legal requirement in a number of countries to identify the data controller within such signage, as well as provide contact details for queries from members of the public.

One may begin by asking whether CCTV signage was in fact present at all. Signage indicating the presence of CCTV and who it is operated by is a crucial mechanism by which to empower data subjects to exercise informational self-determination. There are also, of course, issues of consent insofar as informing citizens about the presence of surveillance measures (i.e.: CCTV cameras) and (theoretically) enabling them to decide whether to submit themselves to such surveillance or not. In many countries, signage is also a legal requirement, so the presence/absence of signage is an important marker to determine to what extent data subjects' ability to exercise their democratic rights are being denied or facilitated.

Researchers were able to locate CCTV signage on site on average in over four fifths of cases (82%), according to Table 11 (*Was signage present at location of CCTV?*). This effectively means that approximately 1 in 5 of CCTV systems do not display signage. This is not just poor data protection practice by organisations operating these systems but is also a breach of national legislation which in most countries makes it a legal requirement to display signage indicating (at an absolute minimum) the presence of CCTV. In the UK, signage was present in every site visited (100%). This high level of data protection legal compliance was reflected in Italy, Luxembourg and Slovakia. The remaining six countries in the research (Austria, Belgium, Germany, Hungary, Norway and Spain) evidenced some instances in which signage was not displayed at all.

4.9 CCTV signage should include contact details for the CCTV operator/data controller

In cases where CCTV signage *was* displayed, one may consider whether contact details for data controllers were available on the signage itself. Although the presence of signs may appear to indicate good practice, the content of this signage must be assessed with regards to whether it is fit for – and fulfils – its purpose. In other words, the mere presence of signage only fulfils one requirement: alerting citizens that they are under surveillance. This signage should also enable data subjects to exercise their democratic rights in an informed manner by alerting them of who to contact to gain more information as to the operation of the CCTV surveillance system.

On average, Table 12 (*Where CCTV signage was present, did this signage contain contact details in order to contact the operator of the CCTV/data controller for the CCTV system?*) shows that researchers found that contact details on signage are only available in just under a third of cases (32.5%). This means that in two thirds of all sites where researchers were able to locate signage, this signage is not fit for purpose aside from merely announcing the presence of CCTV. The UK's findings are significantly better than the cross-European

average. Whilst not flawless, CCTV sites visited by researchers in the UK contained signage with data controller contact details in 80% of cases. This is in clear contrast with a number of countries in the research, including Austria, Hungary and Norway where contact details on signage were *never* found.

4.10 CCTV signage should be displayed prominently and the content should ensure that data subjects are able to identify who operates the cameras

In the cases where signage was displayed, researchers were tasked with rating such signage with the following guidance in mind: the location/prominence of the signage (i.e.: in relation to the size of the location); the condition of the signage (i.e.: is content clearly visible?); and the content of the signage (i.e.: what information is included bearing in mind only limited content can be included in a sign?).

The overall findings show that it is most likely that signage will be rated as 'poor' (42.5%) or 'adequate', (42.5%), according to Table 13 (*Rating given to the visibility and the quality of content of CCTV signage in cases where signage was present*). Meanwhile, only 15% of signage was rated as 'good' which means that in total, in 85% of instances, signage will never be considered as showing good/best practice and will only be considered 'adequate' at best (and indeed is equally likely to be 'poor'). Moreover, in 6 out of 10 countries, researchers could not find a single example of 'good' signage and in Norway, all the signage located was considered to be 'poor'. In contrast however, UK results show that 'poor' signage is less likely to be encountered than in the rest of Europe (20% in the UK compared to 42.5% across Europe).

4.11 Organisations should send holding/acknowledgement letters once a request has been submitted

Receiving a holding letter from a data controller once a request has been submitted can be seen as evidence of good practice. Holding letters not only confirm to the data subject that the request has been received, but also offers the opportunity for data controllers to either seek further information about the request or simply indicate to the requester when he/she should expect a response. This in turn may demonstrate practices of transparency and accountability, managing data subjects' expectations by making them aware of legislative guidelines around response times. Generally speaking, holding letters demonstrate a commitment to opening clear and ongoing lines of communication between the data controller and the data subject, ensuring that the requester is aware of the progress of his/her request at every step along the way. Perhaps most importantly of all, the failure to receive an acknowledgement of a request leaves the requester unsure as to whether the request has been received, whether it is being processed, when a response may be received and indeed whether he/she can expect to receive a response at all[25]. These uncertainties dis-empower data subjects and may lead to frustration, disillusionment and ultimately disengagement in the process. However, on average holding letters were only received in a third (34%) of all cases in the research. Indeed, in some countries the sending of holding letters was a very rare or even non-existing practice amongst the data controllers in the sample. In Austria, a holding letter was never received while in Slovakia, only two data controllers (11%) out of 19 sent such letters.

[25] It is worth noting here that 'holding letters' in this context refers to more than simply automated responses offering little more than generalised content. A holding letter showing good practice *can* be automated but should seek to include, as a minimum, an estimated date by which a requester may expect a response from the data controller as well as contact details should requesters have further queries.

At the other end of the scale however, in the UK (71%) and Germany (69%) in the majority of cases data controllers issued holding letters. In these countries therefore, the researchers were generally kept well informed of the access request process and were given a clear indication of when they may expect to receive a reply to their requests.

4.12 Organisations should ensure that they respond to subject access requests according to the legally-stipulated response times in different countries

Different countries in the EU stipulate specific deadlines by which data controllers should respond to subject access requests. In the UK, data controllers must respond within 40 days of receiving a request[26]. In Austria, the response time may be as long as 56 days[27] whilst in Italy, the response time is considerably shorter – 15 days[28]. In some countries, such as Luxembourg, national legislation does not stipulate a specific response time. Ensuring that access requests are responded to within the legal timeframe achieves a number of goals, all of which are indicative of good practice. Most obviously, such protocols ensure legal compliance. Elsewhere, respecting legal timelines eliminates uncertainty on behalf of data subjects. Promising and ensuring that a response will be received within a certain time means that data subjects' expectations can be managed and generate feelings of trust and satisfaction. This plays an important part in the social dynamics of exercising one's democratic rights and indeed, several researchers expressed frustration and exasperation during the course of the research due to the lengthy delays experienced in obtaining responses from data controllers. In Italy, only one of 18 requests was responded to within the legal timeframe. This means, quite simply, that the vast majority of organisations to whom a subject access request was submitted acted in a non-legally compliant manner. Elsewhere, a request made in the UK to a large multi-national corporation was responded to only after five months of complete silence. A request to a local authority in Norway took four months to resolve and a request made in Luxembourg for vehicle licensing records took three months to conclude. These examples of lengthy delays serve only to create frustration and disillusionment amongst data subjects and are likely, in a non-academic research setting, to lead to the abandonment of requests and the obstruction of data subjects' ability to exercise their democratic right of access to personal data.

5. Conclusions

The results above paint a picture of widespread ineffectual and poor practices with regards to administrative and organisational efficiency and transparency, but more worryingly in terms of compliance with data protection and privacy legislation. In around a fifth of all cases, the researchers, exercising their rights as data subjects, were not able to locate data controller information at all. This effectively terminated their chance of exercising their right to informational self-determination before it has even begun. One may argue that in such circumstances, data subjects can make complaints to the relevant authorities, but it is a sorry state of affairs where to begin the process of exercising one's rights, one has to launch an official complaint at the outset.

Even where organisations did not outright deny our attempts to access our personal data, they did many things to discourage them. The reliance on online platforms via which organisations make available their privacy-related content (in 63% of all successful cases), places a duty on organisations to ensure accessibility, ease of navigation and efficiency of design of their

[26] Section 7(10) Data Protection Act 1998
[27] Article 26(4) Data Protection Act 2000
[28] Article 146.2 Data Protection Code 2003

websites in order to enable citizens, in their role as data subjects, to locate relevant information. Our researchers were expert users of the internet, but that is not true of the majority of European citizens. So problems naturally arise here in light of the existence of the so-called digital divide[29] meaning that those with access to information communication technology are more easily able to exercise their access rights than those without. Moreover, the ability to exercise one's right becomes at least partially determined by one's computer and/or internet literacy.

The above findings with regards to online interactions with data controllers showed transparent and pro-active practices in most cases but also demonstrated poor practice in a significant minority. This includes the 25% of instances in which 4 or more 'clicks' were required in order to reach the relevant content as well as the 39% of cases in which it took 5 minutes or more to locate data controller information on organisations' websites. The availability of templates in less than a fifth of cases indicates poor levels of content within websites. Indeed, the quality of online content regarding privacy and data protection was rated as 'good' by researchers in only 1 in 5 cases. Most damning of all, only half of websites included information about what type of data is routinely collected and stored by data controllers, a fundamentally basic facet of information allowing data subjects to make informed choices regarding whom to give their personal data to. This is a violation of the principle of self-determination and severely undermines the concept of notification, a facet of surveillance regulation which is said to be growing in importance in the context of data controller transparency and accountability[30].

Contacting data controllers via the telephone did not prove significantly easier or more efficient (with some minor exceptions). Data controller information was successfully obtained in under 5 minutes in less than half (46%) of all cases, necessitating data subjects to enter into an often lengthy negotiation process with more than one respondent (2 people or more in 50% of cases). Moreover, the quality of the advice received from respondents on the phone was considered 'poor' in 1 in 4 of cases, meaning that researchers were obtaining inadequate information a quarter of the time.

Finally, the poorest results are found in the experiences of researchers attempting to locate data controller information when visiting physical locations in person. In over two thirds of all cases, it was not possible to successfully identify a data controller only by visiting a location in person, necessitating researchers to carry out further investigations either online or via telephone before being able to locate basic data controller information. Moreover, CCTV signage was absent on average in just under 1 in 5 of all sites and this, of course, is a violation of the law in many countries. Where CCTV signage was displayed, this was often insufficient and in two thirds of cases, failed to provide contact details for the CCTV operator/controller. As such, operators of these CCTV systems are most likely in breach of their national legislations.

The findings suggest that a number of key recommendations would help to ensure that data subjects, whether acting as citizens, consumers or otherwise, received best practice and are able to exercise their informational rights in an informed manner. These are outlined in the structure of this paper but it is worth reminding ourselves of these once again here:

---

[29] See Norris, P. (2003) *Digital Divide: Civic engagement, information poverty and the Internet worldwide*. Cambridge, UK: Cambridge University Press.

[30] See Boehm, F. and de Hert, P. (2012) 'Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law', *European Journal of Law and Technology*, 3(3)

- Data protection and privacy links should be clearly visible and easily accessible on organisations' homepages
- Organisations' websites should include information on what type of data is collected and stored
- Privacy policies should include a template via which to submit a subject access request
- Privacy policies should never be made available only after a user has signed in to a registered members section
- Privacy policies should include full details of how to make a subject access request including how to make an access request and whom to address it to
- If organisations choose to direct data subjects to telephone numbers for data controller information, this should be a simple process and only involve speaking to one person
- Telephone numbers provided for data protection and privacy queries should be directed to a member of staff with requisite knowledge and expertise to answer queries of this nature
- Signage should always be displayed to advise citizens that CCTV is in operation
- CCTV signage should include contact details for the CCTV operator/data controller
- CCTV signage should be displayed prominently and the content should ensure that data subjects are able to identify who operates the cameras
- Organisations should send holding/acknowledgement letters once a request has been submitted
- Organisations should ensure that they respond to subject access requests according to the legally-stipulated response times in different countries

These recommendations can be taken as a list of guiding principles for data controllers and data protection officers within organisations to follow in order to ensure that they not only fully compliant with data protection law but indeed they demonstrate best practice in enabling data subjects to fully exercise their right of access.

Considering the overall results, the generally negative findings in this research affect not only the ability of data subjects to access their personal data but also, as explained in the introduction, naturally restricts the potential for citizens to exercise the remainder of their ARCO rights. Further still, the findings outlined above raise questions about data controllers' practices insofar as fulfilling their duties of transparency and notification which, naturally, have a consequent impact upon the ubiquitous notion of citizens' consent to the wide range of surveillance activities to which they are subject as they go about their everyday lives. Perhaps most concerning of all is that many of the findings detailed above, such as the high occurrences of absence of CCTV signage, demonstrate practices which are in contravention of both the spirit and, more tangibly, the letter of European and national legislation. The key recommendations outlined in this paper may help to remedy these problems.

Tables

Table 1 – Domains and sub-categories included in sample

Domain	Sub-category
Health	National-held patient records Locally-held patient records
Transport	Vehicle registration records Border control Passport issuing records

	ANPR Identification card records CCTV in a transport setting
Employment	Human resources records Entry/exit monitoring system at place of work
Education	Primary school records Secondary school records
Finance	Banking and credit card records Credit rating Insurance provider records CCTV in a bank
Leisure	Membership to leisure/sports club Facebook Online gaming
Consumerism	Loyalty card for a supermarket/department store Loyalty card for a food and/or drinks retailer CCTV in a department store CCTV in a small independent store
Communication	Internet service provider Email records Mobile phone records Search engine data
Civic Engagement	Membership to national charity Membership to an NGO Membership to a political party Membership to a trade union Electoral register records
Security and Criminal Justice	Interpol/Europol records Police records CCTV in a public space/open street

Table 2 – Success rate in locating data controllers

Country	Success rate	Success rate %	Total
Total (average)	262/327	80%	327

Table 3 – How were data controllers' details located?

Country	Online[31]	Telephone	In person	Total
Total	166 (63%)	70 (27%)	26 (10%)	262 (100%)

Table 4 – Success and failure rates of locating data controllers according to method used[32]

[31] The online method includes successfully locating data controller information via email.

Online Success	Online Failure	Phone Success	Phone Failure	In person Success	In Person Failure	Total Success	Total Failure
166 (70%)	70 (30%)	70 (77%)	21 (23%)	26 (43%)	34 (57%)	262 (68%)	125 (32%)

Table 5 – How long (in minutes) did it take to locate data controller details on organisations' websites?

Countries	1-2 minutes (%)	3 - 4 minutes (%)	5+ minutes (%)	Total (%)	Mean Average Minutes
Total	50 (34%)	40 (27%)	57 (39%)	147 (100%)	4.5

Table 6 – Number of 'clicks' required to reach privacy/data protection/subject access content on organisations' website

Countries	1 click (%)	2-3 clicks (%)	4-5 clicks (%)	6+ clicks (%)	Total
Total	32 (22%)	78 (53%)	21 (14%)	16 (11%)	147 (100%)

Table 7 – Rating given to the visibility of the data protection/privacy link on organisations' website

Countries	Rating – 1 = Poor (%)	Rating 2 = Adequate (%)	Rating 3 = Good (%)	Total (%)
Total	54 (37%)	67 (46%)	26 (18%)	147 (101%)

Table 8 – Rating given to the quality of information given in the data protection/privacy section of organisations' websites

Countries	Rating – 1 = Poor (%)	Rating 2 = Adequate (%)	Rating 3 = Good (%)	Total (%)
Total	46 (31%)	71 (48%)	30 (20%)	147 (99%)

Table 9 – How long (in minutes) did it take to locate data controller details when enquiring on the phone?[33]

Countries	1-5 minutes (%)	6-10 minutes (%)	11+ minutes (%)	Total (%)	Mean Average Minutes
Total	32 (46%)	23 (33%)	15 (21%)	70 (100%)	7.7

[32] Several sites are double-counted in this table as researchers will have 'failed' using one method and as such will have tried again using a different method(s). As such, one site may be counted as many as three times in this table.

[33] It should be noted that number of cases per country is very low. In several countries (UK, Slovakia, Germany) it was as low as just three cases. So there may be some limitation to the significance of the findings. However, the number of cases is as high as 24 cases for Norway, 12 for Hungary and 8 for Spain.

Table 10 – Rating given to quality of information about data protection, privacy and subject access received on the phone from organisations' representative(s)

Countries	Rating – 1 = Poor (%)	Rating 2 = Adequate (%)	Rating 3 = Good (%)	Total (%)
Total	19 (27%)	27 (39%)	24 (34%)	70 (100%)

Table 11 – Was signage present at location of CCTV?

Countries	Yes	No	Total
Total	40 (82%)	9 (18%)	49 (100%)

Table 12 – Where CCTV signage was present, did this signage contain contact details in order to contact the operator of the CCTV/data controller for the CCTV system?

Countries	Yes	No	Total
Total	13 (32.5%)	27 (67.5%)	40 (100%)

Table 13 – Rating given to the visibility and the quality of content of CCTV signage in cases where signage was present

Countries	Rating – 1 = Poor (%)	Rating 2 = Adequate (%)	Rating 3 = Good (%)	Total (%)
Total	17 (42.5%)	17 (42.5%)	6 (15%)	40 (100%)