Mapping the Legal and Administrative Frameworks of Access Rights in Europe – A Cross-European Comparative Analysis[1]

Antonella Galetta, Professor Paul de Hert, Dr Xavier L'Hoiry & Professor Clive Norris

Introduction

This report develops a comparative legal analysis of laws and practices on access rights that can be found in the selected countries that we analysed in this research (Austria, Belgium, Germany, Hungary, Italy, Luxembourg, Norway, Slovakia, Spain and the United Kingdom). Although the right of access to personal data is protected and enforced in all these countries (in compliance with Directive 95/46/EC), many differences can be observed.

This report will focus on data protection and in particular on four key aspects that emerge in the exercise of access rights, namely: access to personal data; relevant case law at European and national levels; access to CCTV footage; and the role of DPAs. Finally, this comparative analysis will allow us to draw conclusions while emphasising how the European legal framework on access rights could be further strengthened.

Data protection

Access rights are framed within the broader data protection legislation and their implementation depends upon the legal provisions that govern data protection. The key regulatory framework at the European level is represented by Directive 95/46/EC. However, one cannot define an individual country's national legal framework that concerns data protection on the basis of the Directive. In fact, if one looks closer at national laws on data protection, peculiarities and nuances emerge. National differences about the way data protection laws are implemented depend upon historical and legal traditions. They, in turn, determine and define the way access rights are enforced at national level.

There is not space here to elaborate upon the historical and legal traditions that lay at the basis of data protection laws across Europe. Yet, it is important to highlight how the exercise of access rights depends upon certain historical and legal traditions. Norms about the legal protection of personal data found their way in Europe since 1970 with concrete initiatives promoted by the German state of Hesse and by northern European countries like Sweden and Norway. However, data protection norms and principles had a different appeal within Europe and across countries. This difference is partly attributable to the divide between common law and civil law legal systems. In Germany and Hungary the legal protection of personal data was affirmed through the principle of informational autonomy and self-determination. The two principles took root in the German legal system following the census case of 1983, which, more broadly, can be considered as a landmark decision for data protection legislation in Europe.[2] Indeed, the decision is reflected in other European countries like Hungary, Slovakia and Estonia. The principle of informational self-determination refers to the idea that the freedom of individuals is at stake when they are not made aware about what is known about them and which data are being processed. As a consequence, in order to avoid becoming the object of illegitimate data processing which may infringe upon their private

[1] This version of the report is a draft. It is yet to be formally approved by the European Commission.

[2] Hannah, Matthew, *Dark Territories in the Information Age. Learning from the West German Census Controversies of the 1980s*, Farnham, Ashgate, 2010.

lives - and dignity - data processing has to comply with certain principles (i.e. lawfulness and purpose limitation) and be balanced with data subjects' rights (i.e. access and correction). In addition to that, independent authorities must make sure that data are handled in accordance with the law.

Formally speaking, data protection is not a constitutional right in European Member States as it developed as of 1970, when the transition to modern constitutional states had already occurred. Instead, data protection arose from the information society and the computer revolution which knocked at the doors of Europe in the late twentieth century.[3] In certain cases it crept in national constitutional traditions through the principle of informational self-determination (such as in the case of Germany). In other cases, data protection answered the need to set rules to the informatisation of society (such as in Sweden and Norway). Lastly, in the UK data protection had mainly a trade-oriented approach whose purpose was essentially to allow for the free movement of data. Nonetheless, this latter approach can be partly found in Directive 95/46/EC.

For the purpose of this report it also important to note that the word 'surveillance' is not explicitly mentioned in almost any of the constitutional bills of the Member States we looked at. The only remarkable exception to this is represented by Germany.[4] This confirms that the legal systems of countries which experienced dictatorships and human rights violations are perhaps more sensitive to forms of control exercised by state powers. In turn, this shows how the legal tradition set at national level is influenced by broad historical and cultural factors and specific events. However, legal systems do not necessarily reflect the peculiar political and social climate of a country. Although Hungary has implemented Directive 95/46/EC and data protection is recognised as a human right according to national legislation, the government has recently taken several initiatives which have somehow undermined the right to data protection. Thus, in this case there is a mismatch or tension emerges between the state of law and governmental decisions, between laws and practices.[5]

Data access

Although misconceived and overlooked, the right of access to personal data has an important role within the broad legal framework of data protection. This consideration can be drawn not only from an analysis of the provisions that regulate data protection across Europe, but also going back to the origins of data protection. Born as a legislative tool to regulate power conflicts, the Hesse Act marked the breakthrough of access rights into data protection legislation. It gave data subjects the possibility to exercise access rights and correction rights and to obtain an injunction and remedies in case of unlawful data processing. Remarkably, according to the Hesse Act data subjects did not need to show any reason as to why they

[3] Burkert, Herbert, "Privacy- Data Protection – A German/European Perspective", in Engel, Christoph; Keller, Kenneth H. (eds.), *Governance of Global Networks in the Light of Differing Local Values*, Baden-Baden 2000, pp. 43-70.

[4] As Article 13 (3) of the Grundgesetz says (English translation) "If particular facts justify the suspicion that any person has committed an especially serious crime specifically defined by a law, technical means of acoustical surveillance of any home in which the suspect is supposedly staying may be employed pursuant to judicial order for the purpose of prosecuting the offence, provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive. The authorisation shall be for a limited time. The order shall be issued by a panel composed of three judges. When time is of the essence, it may also be issued by a single judge"

[5] See the Hungary country report at Appendix 1.

wanted to gain access to personal data. Accordingly, since the Hesse Act data access constituted one of the main rights of data subjects mainly *against* the state. [6]

In spite of the fact that data protection is not formally recognised as a constitutional right at national level, it is safeguarded by primary legislation. All the selected countries have data protection laws or bills in place on which basis data protection and access rights are enforced. The right to access personal data is enshrined in those laws or bills. However, further distinctions should be made in this regard. Generally speaking, the right to have access to personal data represents an ancillary right with respect to other rights of the data subject such as rectification, erasure, cancellation, objection and opposition. If we then look closer at the national level, we see that further differences can be found. In Spain for example, access rights are more often associated with rectification, cancellation and opposition rights (from where the acronym of ARCO rights is frequently used). An additional distinction which can be found across the concerned countries regards the identification of the data subject. In the bulk of the selected countries data subjects can be physical (or natural) persons only. By contrast, in other countries such as Italy, Austria and Luxembourg data subjects can also be legal persons - that is any organisation, association or group of people which by law are capable of having legal rights and duties.[7] Although this distinction might seem to be irrelevant, this is not the case. The fact that legal persons can exercise access rights implies that their company's or organisation's data are given a certain protection at national level and deserve it according to national law. As a consequence, in Italy, Austria and Luxembourg legal persons are entitled to exercise access rights like any physical person would do. This means that in these countries private companies are given for instance the right to claim access to those corporate data which reveal their own identity on the market (such as the business name) which may be processed by other organisations or entities.

The right of access to personal data is essentially about transparency, accountability and confidentiality. The key principle that lies at the basis of access rights is transparency. In fact, on the one hand access rights requests can be seen as a way for data subjects to ask for a transparent processing of personal data. On the other, by exercising access rights data subjects make sure that their data are not disclosed to third parties unlawfully and that confidential practices in the processing of personal data are in place. While doing so, the data subject calls the data controller to ensure responsible data processing procedures, making him accountable for certain data protection practices and policies. However, transparency, accountability and confidentiality requirements vary across Member States significantly. The level of transparency, accountability and confidentiality depends upon the specific legislation on access rights, as well as on practices set at national level and within companies and organisations.

Substantial differences at national level exist as to how access rights can be exercised. In general, access rights requests are introduced in writing to data controllers, but a few exceptions to this general rule can be found. It is necessary to address access requests in writing in Belgium, Hungary, Slovakia and the United Kingdom. However, in some countries it is possible to file access requests also in less formal ways. According to the Italian legislation, for example, access requests are introduced "without any particular formality".[8] In Austria access requests are usually made in writing to the data controller. Nevertheless,

[6] Burkert, Herbert, "Privacy- Data Protection – A German/European Perspective", ibid., pp. 45-46.
[7] See for example Nijman, Janne Elisabeth, *The concept of international legal personality. An enquiry into the history and theory of international law*, T.M.C. Asser Press, 2004.
[8] Art. 8.1 D. Lgs. 30 June 2003 n. 196 (Data Protection Code).

Art. 26 of the national Data Protection Act stipulates that the request can be made orally, subject to the agreement of the data controller.[9] In other countries like Norway legislation is vaguer on this point and allows the data subject and data controller the possibility to decide on the form of the request. Hence, information *may* be requested in writing and data controllers *may* also require a written, signed request.[10] A certain flexibility is also contemplated under the Spanish law. Here access is granted either by requesting the concerned information in writing or by simply displaying the data for consultation.[11]

Once an access request is introduced, data controllers normally handle it within a specified time frame. It backdates from the moment in which the request (usually together with the requirement identification documents) is received by the data controller and varies substantially in the selected countries. The shortest lapse which is required for a data controller to react to an access request is 15 days in Italy (standard time limit). By contrast, longer time frames are allowed in Belgium (45 days maximum) and Austria (56 days maximum). Even though the standard timing is 15 days in Italy, data controllers or processors can postpone their replies to the data subject in complex cases. In these circumstances the time frame is shifted to 30 days. In any case, the data controller or processor has to inform the data subject about the reasons why a longer lapse is needed.[12] Similarly, the Norwegian Personal Data Act fixes an 'ordinary' time limit of 30 days from the receipt of the request, which can be postponed because of 'extraordinary' circumstances.[13] It is noteworthy that the law in Luxembourg and Germany does not fix any specific time limit within which data controllers have to provide feedback to the data subject. This vague provision gives data controllers a substantial discretionary power against data subjects and jeopardises the exercise of access rights.

The following table illustrates clearly differences among Member States as regards the time limit granted to data controllers to process an access request.

[9] Art. 26 (1).
[10] Sections 17 and 24 of the Personal Data Act.
[11] Art. 15 (2) of the Personal Data Protection Act.
[12] Art. 146 (3) D. Lgs. 30 June 2003 n. 196 (Data Protection Code).
[13] Section 16 of the Personal Data Act.

Country	Time frame	Legal provision
Austria	within 56 days	Article 26 (4), Data Protection Act, 2000
Belgium	within 45 days	Article 10, Privacy Act, 1992
Germany	no specific time limit	/
Hungary	within 30 days	Article 14 (4), Data Protection Act, 2011
Italy	within 15 days (short term); within 30 days (long term)	Article 146.2, Data Protection Code, 2003
Luxembourg	no specific time limit	/
Norway	within 30 days	Article 16, Personal Data Act
Slovakia	within 30 days	Section 21 (3), General Data Protection Law, 2002
Spain	within 30 days	Article 15, Personal Data Protection Act, 1999
UK	within 40 days	Section 7 (10), Data Protection Act, 1998

These differences across European countries have a significant impact on the exercise of access rights. A longer time frame gives data controllers more discretion as to when a data request should be processed. As such, data subjects in different countries may have a longer wait than in other Member States before receiving a response to their requests. Perhaps of even more importance are those countries in which there are no legal stipulations as to response times for data controllers, as in the cases of Germany and Luxembourg. Data subjects in these Member States may therefore suffer from uncertainty as to when their requests will be dealt with and the danger exists that data controllers are given too much discretion in how (and specifically how quickly) organisations reply to access requests. As we will highlight in the following section, provisions related to timing play a crucial role especially in the case of access to CCTV footage.

The idea that individuals need to pay in order to exercise a certain right is somehow alien to the civil law tradition.[14] However, continental Europe is not completely immune to this kind of logic when it comes to access rights. In general, access to personal data is free of charge for the data subject, no matter how many times the data controller is asked to handle a certain

[14] René Seerden, *Administrative law of the European Union, its member states and the United States: a comparative analysis*, Antwerp, Intersentia, 2007.

access request. This is the case of Belgium, Germany, Luxembourg and Spain.[15] In these countries access to data is also free of charge when a request is submitted to the DPA, both in cases of mediation and/or indirect access. In other countries data access is free of charge if the data controller receives one request per year, whereas it is necessary to pay a fee in case more than one request is submitted to the same data controller for the same purposes within one year. In Austria for example data subjects are asked to pay a flat rate compensation of 18,89 EUR in this latter circumstance.[16] The Hungarian legislation follows the same pattern. Interestingly, in this country the amount of the fee is not established by the legislation itself but is fixed upon agreement between the data subject and the data controller. In Slovakia, meanwhile, access request are free of charge for the data subject. However, a small fee has to be paid by the claimant to cover material costs accrued in connection with the making of copies and sending information to him.[17] A peculiar regulatory framework is in place in Italy. Data subjects do not have to pay any fee or compensation when they ask data controllers for access to their personal data. By contrast, if they want to introduce a formal complaint to the national DPA a fee of 150 EUR has to be paid. The Italian Data Protection Act also gives data subjects the possibility to ask the DPA to check the compliance of the data controller's reply to an access request with national data protection legislation, by introducing a report. In this case no fee is needed.[18] However, it raises the possibility that the most robust complaint procedures in Italy are the preserve of only those able to pay significant sums to access these redress mechanisms. In the UK the submission of access requests is not free for the data subject who has to pay £10 per request (£2 for requests concerning credit rating).[19] In any case, in those countries in which data access is not always free, data subjects are refunded if their data were used illegally or the request led to a correction.

In all selected Member States data subjects are allowed to introduce a complaint to national DPAs when data controllers do not provide any feedback to an access request or their reply does not satisfy the claimant. In this case DPAs mediate between data controllers and data subjects making sure that the access request is handled in accordance with national data protection laws. In general, Member States' legislation does not set any time limit within which the national DPA has to process the data subject's request for mediation. However, in other countries a specific time limit is in place, such as in Italy, where the national DPA has to begin processing the data subject's complaint within three days from the notification of the request.[20]

There are also disparities between the Member States in this study with regards to the legal requirements at national levels for the appointment of a Data Protection Officer (DPO) by data controllers. While the Directive does not proscribe any legal measures on when data controllers should appoint DPOs, a number of Member States have enacted legislation requiring data controllers to appoint such officers in certain circumstances. It may be argued that the enshrinement in national legislation of such measures demonstrates a commitment by the legislature of those countries to ensure some degree of accountability amongst data controllers and implement safeguards in their organisational structures to guarantee transparent practices and procedures. In Germany, the requirements of appointing DPOs are

[15] Although the exercise of access rights is free in Spain, access can be claimed no more than once a year, unless the data subject can prove a legitimate interest in doing so (Art. 15 of the Personal Data Protection Act).
[16] Art. 26 (6).
[17] Section 21 (2) of the General Data Protection Law.
[18] Art. 141 (1)b, D. Lgs. 30 June 2003 n. 196 (Data Protection Code).
[19] Section 7 of the Data Protection Act.
[20] Art. 149 (1) D. Lgs. 30 June 2003 n. 196 (Data Protection Code).

stringent, particularly where organisations use automated decision making processes. In Hungary, the requirement to appoint a DPO applies to certain types of organisations including financial institutions, telecommunication and public utility companies and those data controllers processing personal data in nationwide databases. Perhaps most stringent of all, in Slovakia data controllers must appoint a DPO if they employ more than five persons. At the other end of the scale, Austria, Italy, Norway and the UK have no legal requirement to appoint DPOs[21] while in Luxemburg, the appointment of DPOs is recommended but takes place on a voluntary basis. Finally, in Belgium and Spain, no general legal requirements exist to determine the appointment of DPOs but national guidelines advise in favour of this in certain circumstances such as the type of data processed and the level of data security risk[22]. The legal obligation to appoint DPOs is established at EU level only by the European Regulation 45/2001 on the processing of personal data by the EU institutions and its bodies.[23] In fact, Art. 24 of this law states that each institution and body of the European Union "shall appoint at least one person as data protection officer".[24] No provision of such kind is established at European level. However, the ongoing data protection reform might set specific obligations on data controllers to appoint DPOs. Whereas Directive 95/46/EC does not deal with DPOs, Section 4 (Articles 35-37) of the proposed data protection Regulation focuses precisely on its appointment, role and tasks.[25] Art. 35 of the proposed Regulation holds that the controller and the processor "shall designate" a data protection officer where:

> "(a) the processing is carried out by a public authority or body; or
> (b) the processing is carried out by an enterprise employing 250 persons or more; or
> (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects".[26]

National data protection laws do not always set significant guarantees for the data subject in case of unlawful data processing or data access denial. In this first circumstance data subjects get reimbursed for the cost of the fee or compensation they were asked to pay to have their request processed by the data controller, if applicable. Legislation guarantees the data subjects' rights of rectification, cancellation, erasure or opposition which therefore represent legal remedies to counter illegal or illegitimate data processing practices. However, national data protection laws do not usually establish automatic mechanisms to sanction data controllers which processed personal data unlawfully. Of course, data subjects might invoke forms of sanctions by appealing to the judicial authority. As said earlier, if the data controller ignores an access request the data subject can submit a formal complaint before the national DPA. However, again the data subject does not have substantial legal guarantees against

[21] It should be noted that despite the absence of legal requirements in national legislation, some data controllers nevertheless pro-actively appoint DPOs.
[22] DLA Piper (2013) Data Protection Law of the World, available online at http://www.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf
[23] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L 8/01.
[24] Art. 24.1 of Regulation 45/2001.
[25] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigations, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (General Data Protection Directive), COM(2012) 10 final, Brussels, 25 January 2012.
[26] Ibid, Art. 35.

access denial. In spite of the DPA's mediation, data controllers can keep ignoring the access request without any major legal consequence or risk. In the majority of selected countries, guarantees of this sort were missing. However, there were a few exceptions. In Norway, for example, the national DPA can decide about possible fines for data controllers in cases where access requests are disregarded. Remarkably, in Luxembourg if data controllers obstruct data subjects' access to data a prison sentence (between 8 days and 1 year imprisonment) and/or a fine (between 251 and 125,000 EUR) may be applied.[27]

Apart from access rights, there are also additional guarantees established by law that enhance transparency, accountability and confidentiality between data controllers and data subjects which seek to strengthen the position of the latter against the former. In most of the Member States studied, data controllers have the legal obligation to inform data subjects about whether personal data about them are being processed. However, in Austria and Germany this obligation is not explicitly stipulated but is somehow implicit in the right of access.

Important distinctions emerge also from the comparison of legal exceptions to the right to access personal data set at national level. Generally speaking the exceptions established in each of the selected countries comply with Directive 95/46/EC which all the concerned countries have implemented so far. Accordingly, national exceptions to the right to access personal data recall Art. 13 of the Directive and are set in case it is necessary to: safeguard national security; defence and public security; for the prevention, investigation and detection of crime; for protecting economic or financial interests of a Member State; for protecting the data subject or the rights and freedoms of others; and for scientific or statistical purposes. Article 13 encompasses several different situations in which data protection violations are made basically legitimate by law. The content of expressions such as national security or public safety is open to interpretations and left to the discretion of Member States. Indeed, from the perspective of Member States, Art. 13 can be seen as a sort of squeeze-box which is tailored and adjusted on the basis of national politics. The recent PRISM scandal is emblematic of how the illegitimate processing of personal data was carried out in the name of national security, by the National Security Agency (NSA).

Although national laws are compliant with the provisions of the Directive, in almost all of the selected countries there are additional exceptions to the general provisions of the Directive. In Italy for instance, the right of data subjects to have access to personal data is further limited in the framework of the implementation of legislation on victims of extortion (Art. 8 of the Data Protection Code). In Belgium, data access is restricted when it is necessary to implement money laundering legislation (Art. 3, Para. 5 of the Belgian Privacy Act). Lastly, in Norway data access is denied when secrecy has to be guaranteed (Section 23 of the Personal Data Act).

Our comparative analysis shows that distinctions across Europe can be found also with regards to the automated processing of personal data. According to Art. 15 of Directive 95/46/EC data subjects can oppose automated decisions data controllers might take against them which have the purpose of evaluating certain personal aspects such as creditworthiness, performance at work, reliability, conduct, etc. Although this provision is part of the data protection framework established in each of the selected countries, some of the concerned Member States have set additional safeguards against automated decision-making. This is the case in Norway for example, which not only prohibits automated profiling but also gives data

[27] Art. 28 of the Data Protection Act.

subjects the right to obtain information from data controllers as to the rules incorporated in the computer software which formed the basis of the decision (Section 22 of the Norwegian Personal Data Act). Hence, the highly detailed Norwegian provision gives data subjects a substantial power to counter automated decisions made by data controllers. This provision confirms the increased importance given to data security by the Norwegian legal system, in line with the Scandinavian legal tradition. At the same time, differences in the way automated processing is regulated across Europe recall the questions of whether and to what extent it is possible to harmonise European data protection legislation at European level. This would be possible if data protection standards be kept high in countries like Norway and if more Member States would follow best practices in the implementation and enforcement of data protection norms.

Case law

Although analyses of case law should bear in mind the context-specific nuances of individual cases, one may argue that emerging trends can be discerned by considering the evolution of case law at national and supra-national levels. Specifically for the purposes of this study, one may look at the way European and national provisions on data protection have been interpreted and applied, with special regard at the way data subjects' and data controllers' rights have been balanced. This section does not seek to repeat the individual details of the case law discussed in the country reports below but rather to highlight general trends and thus determine if any socio-legal patterns emerge from one Member State to another.

Before one considers any possible trends in national and European court judgements, it is equally noteworthy that in a number of the countries involved in this study, relevant case law was hard to find. Although one can find some interesting case law on data protection in Austria and Luxembourg, case law specifically on access rights is sparse (national DPA decisions notwithstanding) in these countries. In Norway too, high-level court judgements are rare (although some noteworthy decisions have been made at lower-level administrative courts). This may point to a number of inferences including the proposed assertion that informational rights (and in particular the right of access) are not commonly exercised by citizens in some countries. Moreover, one may argue that a general lack of awareness exists in many European countries as to the redress mechanisms, including the possibility of bringing cases to court, where data breaches have taken place. Recent research by the EU Agency for Fundamental Rights (FRA)[28] strongly reinforces such claims and indeed extends these conclusions to include a lack of knowledge and expertise on behalf of lawyers and judges, further undermining the use of courts as a medium through which to resolve data protection disputes.

At a supra-national level, the European Court of Human Rights (ECtHR) and the European Court of Justice (ECJ) appear to have ruled broadly in favour of individual data subjects in recent years during disputes with data controllers and/or Member States which have escalated to the levels of European courts. While in *Leander v Sweden*[29] the ECtHR backed the Swedish government's refusal to grant the plaintiff access to sensitive data based in part to the presence of an impartial and independent body at a national level who had decided on the denial, the court has shown in subsequent cases that the absence of such safeguards of

[28] European Union Agency for Fundamental Rights (FRA) *Access to Justice in Europe: an overview of challenges and opportunities,* 2011 and *Access to data protection remedies in EU member states,* 2013.
[29] ECtHR, *Leander v. Sweden*, application no. 9248/81, judgment of 26 March 1987.

impartiality is not acceptable. In both *Gaskin v UK*[30] and *M.G. v UK*[31], the court found the absence of an independent authority to decide on whether access should have been granted to the applicants was a failure on the part of the British government. While the plaintiff's case was unsuccessful in *Odièvre v. France*[32], the court once again reasserted the importance of the presence of an impartial body to make judgements on data access, once more imposing a strict regime upon data controllers and national governments in order to ensure neutrality and fairness.

The ECJ meanwhile has similarly taken a broad interpretation of some principles of the Directive via its judicial decisions resulting in ruling which have broadly favoured individual data subjects. In *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*[33] for example, the court took a narrow reading of the concept of disproportionate burden upon data controllers in finding that the plaintiff should fulfil an access request for two years worth of data rather than the one year limitation the data controller had restricted its disclosure to. In *Commission v Germany*[34] meanwhile, the ECJ took a wide reading of the concept of DPAs' independence and thus ruled that both public and non-public interferences should be avoided in order to safeguard the neutrality of DPAs as their undertake their duties.

At national levels, courts in different countries have taken significantly conflicting decisions, showing little consistency from one Member State to another in their interpretations of European and national legislation. German case law appears to have had a particularly influential role in the notion of enhancing individual citizen's privacy and data protection rights and indeed the landmark census case of 1983 effectively gave birth to the concept of informational self-determination[35]. Since then, case law in Germany's constitutional and federal courts has tended to demonstrate the importance attached to data subjects' informational rights and the courts' reading of legislation has broadly reflected a desire to prioritise the concept of informational self-determination over the interests of data controllers (even in those cases when the data subjects' complaints were dismissed). However, the most recent high profile ruling concerning access rights in the context of credit scoring appears to show something of a difficult balancing exercise for the German Federal Court of Justice, who issued the judgement. While the court emphasized the ongoing importance of protecting data subjects' right of access, the judgement also sought to protect the trade secrets around the scoring systems used to calculate credit ratings.

Hungarian data protection discourse was heavily influenced by the German census case and indeed case law in Hungary shows a similar reliance upon a landmark finding of the Constitutional Court in 1991. In its judgement, the court abolished the use of personal identification numbers since these were deemed to impinge upon the right of informational self-determination of data subjects as well as threaten the notion of protecting personal data[36]. Since then however, Hungarian case law, particularly in the context of access rights, has been inconsistent. For example, the Metropolitan Court ruled in favour of the data subject in a case involving an insurance company's refusal to grant access to personal data and reinforced the DPA's judgement that insurance data represented particularly sensitive data. However, a later

[30] ECtHR, *Gaskin v. the United Kingdom*, application no. 10454/83, judgment of 7 July 1989.
[31] ECtHR, *M.G. v. the United Kingdom*, application no. 39393/98, judgment of 24/12/2002.
[32] ECtHR, *Odièvre v. France*, application no. 42326/98, judgment of 13 February 2003.
[33] ECJ, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, case C-553/07, 7 May 2009.
[34] ECJ, *European Commission v. Federal Republic of Germany*, case C-518/07, 9 March 2010.
[35] Bundesverfassungsgericht, decisions volume 65, p. 1 ff.
[36] Decisions No. 24/1998. (VI. 9.) AB and No. 44/2004. (XI. 23.) AB.

case failed to award damages to a data subject who had incorrectly been refused access to his personal data since the court found that no damages could be proved as a result of a data protection breach[37].

Italian jurisprudence meanwhile, appears to have consistently supported the right of access, even in cases where this primary right has been in direct conflict with another, that of the right to data protection in the context of disclosing personal data of third parties. In such cases, Italian courts have advised that data should be censored and then disclosed, allowing for the protection of third parties' sensitive data whilst nevertheless fulfilling the request of applicants. Elsewhere, the Italian Supreme Court has taken a wide interpretation of the responsibilities of 'natural persons' in handling personal data as well as highlighting that data breaches may be more serious depending on the context in which the data has been breached (i.e.: disclosure of data on the internet is potentially more harmful than in other domains)[38]. Moreover, in another case, the Supreme Court ruled that the duties and obligations upon data controllers outlined in Italian legislation should be strictly followed to ensure accountability and the protection of data subjects' interests[39]. As such, the general trend in Italian case law appears to demonstrate a commitment to enhance, as much as possible, the ability of data subjects to exercise their access rights while also ensuring that data controllers fulfil their legal responsibilities.

In Slovakia meanwhile, while case law appears to be silent on the issue of access rights, existing judgements concerning data protection in a more general sense have tended to protect the interest of data subjects and prioritise their informational rights. For example, the DPA's powers to end the use of national identification numbers have been backed by the Supreme Court despite a challenge by the Slovak Ministry of Justice[40]. Elsewhere, the Constitutional Court has appeared to prioritise the right to information ahead of the right to privacy in a number of contexts. In one case, the court allowed protesters to film police officers without the latter's consent[41] while in another, the court found that politicians could not object to having their photographs taken during a particularly controversial vote in parliament[42]. Finally, the court ruled against the Ministry of Justice who had unsuccessfully sought to contest a legal amendment which allowed access to information concerning public officials' salaries and other similar data[43].

In Belgium, court judgements have highlighted the sanctity of the right of privacy as well as emphasizing the importance of accountability and transparency by ordering data controllers to ensure data subjects are properly informed as to their data processing practices. With regards to access rights, the court's judgement in the case of *C.F.X.S (Financieel studiecentrum Xavier Serwy) v* the *Union royale professionnelle du crédit*[44] reminded data

[37] Metropolitan Court 26.K.32.704/2012/5.
[38] Tribunale di Milano, Sent. 04.02.2009 and Corte d'Appello di Milano, Sent. 11.05.2010
[39] Cass. Civile, Sez. I, 09.01.2013, Sent. n. 349, in www.ilsole24ore.com/pdf2010/SoleOnLine5/Oggetti_correlati/Documenti/Norme%20e%20Tributi/2013/01/corte-cassazione-sentenza-349-2013.pdf
[40] Article 29 Working Party, 11th Annual Report of the Article 29 Working Party on Data Protection, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf
[41] IV. ÚS 44/00, The Constitutional Court of Slovakia. The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2001a/10_01a.pdf
[42] IV. ÚS 40/03, The Constitutional Court of Slovakia, The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2003a/190_03a.pdf
[43] PL. ÚS 1/09, The Constitutional Court of Slovakia, The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2011a/1_11a.pdf
[44] Tribunal de Première Instance de Bruxelles, Civ. Bruxelles, op. cit

controllers of their duty to act prudently in processing personal data due to the (potentially negative) consequences of such activities and reinforced the notion that the right of information should be considered as a fundamental right for citizens.

Despite the absence of a body of case law in Luxembourg, the most significant court judgement on data protection matters resulted in a ruling which emphasized the importance of acquiring data legally in order to protect the right to a fair trial[45]. In doing so, the court effectively prioritised this over the possibility of prosecuting an offender of a serious offence based on illegally obtained CCTV footage. Similarly in Norway, lower-level administrative courts have shown instances of protecting data subjects' interests and emphasizing the priority of transparency by granting access to personal data. Indeed, these judgements even overturned previous decisions by Norway's DPA to support data controllers' denial of access to applicants[46].

In a marked contrast however, British courts have taken perhaps the narrowest interpretations of national legislation and in so doing appear to have restricted the ability of individuals to exercise their access rights, concurrently relieving data controllers of considerable burden in the context of responding to access requests. In the landmark case of *Durant v Financial Service Authority*[47], the Court of Appeal took exceptionally narrow readings of terms such as 'personal data' and 'relevant filing system', seemingly freeing data controllers from many obligations when responding to access requests. The ruling was reinforced in subsequent case law which once more interpreted the terms of the national legislation in a restrictive manner, undermining the applicants' attempts to access their personal data. Finally, the High Court in *Ezsias v Welsh Ministers*[48] further lifted the burden upon data controllers by finding that a request for 'all' personal data by the applicant represented disproportionate effort on behalf of the data controller. Indeed, while the court acknowledged that the data controller had failed to respond within the legal time limits, this breach was deemed to be 'of little importance'[49], further undermining the importance attached to the rights of data subjects.

General trends across the EU are thus difficult to locate in terms of case law, particularly due to the exceptionally narrow interpretations taken by British courts. However, some country-specific conclusions can perhaps be drawn. At a supra-national level, European courts have emphasized the importance of independence, impartiality, transparency and neutrality in matters concerning the granting or denial of access to personal data. Even when data subjects' cases were dismissed by the courts, the judgements still sought to ensure that the correct procedures were followed in order to safeguard accountability and impartiality. In Germany, Slovakia, Hungary and Italy, courts at various levels have tended to emphasize the importance of informational rights of those seeking to access personal data, even in instances when such rights conflict with others such as the right to privacy (particularly the privacy of third parties). In other Member States, court judgements are somewhat inconsistent, such as in Norway where lower-level courts have protected the interests of individual data subjects but the Supreme Court did not penalise the use of illegally obtained data. However in the UK, case law seems to have sided firmly with data controllers, consistently taking restrictive

[45] Arrêt de la cour de cassation n°57/2007 pénal. du 22.11.2007

[46] KLAGESAK 2005-02: Klage på Datatilsynets vedtak om å avvise sak med krav om innsyn i innbetalt forsikringspremie Personvernnemndas avgjørelse av 9.8.2005 ; available at: http://www.personvernnemnda.no/vedtak/2005_2.htm.

[47] *Durant v Financial Services Authority* [2003] EWCA Civ 1746

[48] *Ezsias v Welsh Ministers* [2007] All ER (D) 65 (Dec)

[49] *Ezsias v Welsh Ministers*, ibid. para 106.

interpretations of legislative terms and significantly easing the burdens faced by data controllers when responding to access requests.

Perhaps more significant than specific findings in individual cases is the more general lack of case law on data protection issues and specifically access rights in courts across the EU. While the lack of clear harmonization in courts' approaches to informational rights disputes across Europe may serve to undermine the exercise of such rights by data subjects, one may argue that a far more deep-seated problem lies in the fact that low levels of engagement with the court system belies a number of difficult issues mentioned above and highlighted in more depth in FRA's recent reports[50]. These include a systematic lack of awareness of informational (and specifically access) rights amongst data subjects, particularly regarding potential redress mechanisms such as courts, coupled with low levels of expertise regarding data protection matters on behalf of criminal justice professionals extending as far as judges.

Access to CCTV footage

The right to have access to CCTV footage is considered as a sort of corollary to the right to have access to personal data in all the concerned countries. Accordingly, access to CCTV images is normally regulated by data protection acts established at national level. While carrying out this analysis we noticed that in a few European countries the use of CCTV cameras is regulated on the basis of specific provisions on CCTV cameras. This is the case of Belgium for example which passed in 2007 a specific law on the use of CCTV cameras, the Belgian Camera Act.[51] In Austria, recent amendments to the Data Protection Act introduced special provisions to regulate the use of CCTV cameras. Apart from these sporadic cases, the use of CCTV cameras is not regulated by any sector-specific legislation in the selected countries and access to CCTV footage is compliant with national provisions on access to personal data. This is also the case of the UK for instance. Despite the fact that over 4 million CCTV cameras may be in operation in the UK,[52] no specific legislation on CCTV is in place. Accordingly, access to CCTV footage follows the same rules which apply to access to personal data, as stated in the Data Protection Act 1998. Since legislation is often silent about how to regulate the use of CCTV systems, guidelines and codes of practice are often formulated by national DPAs. In Italy for example, the national DPA issued in 2010 a provision on video surveillance which makes clear, among other things, how controllers of CCTV images should handle an access request. More recently, in 2013 the UK Home Office and DPA released a code of practice on the use of CCTV. It is important to note that initiatives of this sort have also been promoted by the private sector and associations of professional groups. This is the case in Hungary for example, where specific legal provisions on the use of CCTV cameras can be found in the Security Services Act and the Condominium Act.

Substantial differences among Member States can be found as regards the maximum storage period of CCTV images. In almost all the Member States we analysed time limits for the storage of CCTV footage were set in national legislation, in cases where the CCTV recording

[50] European Union Agency for Fundamental Rights (FRA) *Access to Justice in Europe: an overview of challenges and opportunities,* 2011 and *Access to data protection remedies in EU member states,* 2013.
[51] Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007, M.B. 31 May 2007.
[52] McCahill, Mike and Clive Norris, "Estimating the extent, sophistication and legality of CCTV in London", in Gill, Martin (eds.), *CCTV*, Leicester, Perpetuity Press, 2003. Gras, Marianne L., "The legal regulation of CCTV in Europe", *Surveillance & Society*, Vol. 2, 2004, pp. 216-229.

was not used as evidence in any criminal proceeding or investigation. However, storage limits vary across Member States. In Austria CCTV footage can be kept for 72 hours maximum. In Belgium and Spain the maximum storage period is of 30 days. In Slovakia CCTV images can be kept for 7 days at most from the day of the recording. According to the 2010 provision on video surveillance issued by the Italian DPA CCTV images should be stored for 24 hours maximum (ordinary storage period). However, a longer storage period of 7 days is allowed when specific security needs arise (such as in the case of a bank) in occasion of public holidays.[53]

Provisions that limit the storage period of CCTV images fulfil certainly the need to protect personal data, in compliance with the principles of purpose limitation and proportionality. In a general sense, the erasure of data is preferable in principle, given that the absence of such measures could lead to the permanent retention of data. However, it is important to note that this time limit does sometimes represent an obstacle to the exercise of access rights. If the storage period is lower than the amount of time given to the data controller to reply to an access request, it is very likely the data subject will not get access to the concerned CCTV images because they will have been erased by the data controller. In this case, there is no way for the data subject to tangibly have access to the footage. It is also important to note that in addition to this material difficulty in exercising access rights, for data subject is often harder to have access to CCTV images than other types of personal data because of additional legal requirements. In Belgium for example, data subjects should be given access to CCTV footage as long as they introduce a written and motivated request to the data controller.[54]

Role of DPAs

DPAs play a crucial role in promoting access rights. They mediate between data controllers and data subjects whenever the former ignore data access requests or do not provide data subjects with the required information. Although in all the concerned Member States DPAs are called to play a key role in ensuring data subjects' access to personal data, their activity is highly influenced by the way they operate in protecting personal data. Differences in this regard can be found across Europe and they relate in particular to the level of engagement, autonomy and independence of national DPAs. Because of the recent implementation of European data protection laws, one could think that the activity of DPAs in Eastern European countries is more problematic than in Western European countries. However, this is not the case. All European DPAs are confronted with the same issues nowadays, which we can illustrate here as follows.

Article 28 (1) (2) of Directive 94/46/EC requires Member States to ensure that their national DPAs act in complete independence. However, this provision is problematic for several European Member States. Recent jurisprudential cases of the European Court of Justice have demonstrated that the Austrian and the German DPAs lack autonomy and independence.[55] As the Court highlighted, procedures established in these Member States to elect DPA are faulty and inappropriate to safeguard standards of independence. Hungary is coping with similar problems. The Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information has been recently dismissed by the government and replaced with a

[53] Art. 3.4 of the DPA provision on video surveillance, 2010.
[54] Art. 12 of the Camera Act. The empirical phase of WP5 illustrates clearly how this requirement limits the exercise of access rights.
[55] ECJ, *European Commission v. Federal Republic of Germany*, case C-518/07, 9 March 2010. ECJ, *European Commission v. Republic of Austria*, case C-614/10, 16 October 2012.

governmental authority whose independence is highly questionable. Moreover, upon the initiative of the European Commission, a formal proceeding against Hungary has been started before the European Court of Justice. In recent times, the Slovak DPA has also been criticised for its lack of independence from the national government. Although in 2002 an independent Data Protection Officer was appointed, until recently the European Commission had expressed its doubts about the role of the Slovak DPA.

The activity of some DPAs in Europe is highly affected by lack of material and human resources, which limit or invalidate data protection initiatives. The Slovak and Hungarian DPAs are not particularly involved in promoting access rights and in awareness-raising initiatives. The same trend can be found in Austria where the DPA does not engage in compliance initiatives. By contrast, other DPAs in Europe seem more active in promoting access rights and in promoting data protection rights, such as DPAs in Belgium, Luxembourg, the UK and Italy.

All DPAs we looked at provide information on their websites about how data subjects can access their personal data, as well as about data subjects' rights in general. However, only some of them offer detailed guidance and substantial assistance in this respect. Apart from explaining how data subjects can exercise access rights, DPAs in Belgium, Spain and Austria provide template letters on their websites which can be used by data subjects to introduce access requests. In addition, DPAs in these countries put at disposal of data subjects also template letters which can be used to introduce requests for mediation to the DPA itself. In Luxembourg it is not possible to find on the website of the DPA a template latter to file access requests to data controllers. However, data subjects can fill in online forms to ask for mediation and send them to the DPA electronically. For the moment being, this form is available in French only. Similarly, the British ICO has set up an online complaint resolution service which allows data subjects to file complaints to the DPA in a few clicks. A lower level of interaction between DPAs and data subjects can be found in other European Member States. It is not possible for instance to find on the website of the Slovak DPA any template letter that citizens can download or complete in order to submit a complaint either to data controllers or to the DPA.

Nevertheless, concerns about the role and function of European DPAs were expressed in the recent report of the EU Fundamental Rights Agency (FRA) on data protection in Europe.[56] It identified a number of deficiencies in data protection law, namely: weaknesses in the role of DPAs (1); compliance problems (2); lack of sanctions, compensation and legal consequences (3) and rights awareness (4). Similarly, the report spotted three problematic areas regarding data protection, namely: data protection in relation to data security (1); data protection relating to an individual's health (2); and data protection in relation to video surveillance (3).[57] The comparative analysis about the exercise of access rights in Europe developed in this report touches upon all the problematic aspects and concerns raised by the FRA.

Conclusion

The right to have access to personal data constitutes the main right data subjects have against data controllers. In spite of this, it seems to be the least catchy of ARCO rights from the point of view of the data subject as it is seldom claimed. This can be partly explained by the

[56] European Union Agency for Fundamental Rights (FRA), *Data protection in the European Union: the role of national Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, 2010.
[57] FRA, ibid., pp. 42-46.

resistance of data controllers in providing data subjects access to personal data. In addition, as it has been pointed out, "there is some lack of clarity" about the general scope of access rights.[58] It is said that if not meant to rectify, cancel or oppose the treatment of personal data one is confronted with a certain difficulty in explaining the content of this right and its true value. Although this difficulty is understandable, it cannot be put forward as an argument to limit data subjects' rights and hence undermine the notion of data protection. If so, this would imply the end of the data subject's right of informational self-determination.

Although all the Member States we looked at implemented Directive 95/46/EC, different 'degrees of implementation' of the right to have access to personal data can be found across Member States. Access rights are not operationalised evenly across Europe and a substantial lack of harmonisation can be observed. In addition, this fragmented framework is also complemented by objective difficulties data subjects have in getting access to personal data, because of the inability in locating data controllers or of limits concerning the storage period. As illustrated earlier, from the point of view of the data subject the right of access to personal data is the cornerstone of data protection. A higher degree of implementation of access rights in Europe should be encouraged in order to ensure higher data protection standards.

References

Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act) (Norway). Available at: http://www.datatilsynet.no/Global/english/Personal_Data_Act_20120420.pdf

Arrêt de la cour de cassation n°57/2007 pénal. du 22.11.2007. http://www.cnpd.public.lu/fr/legislation/jurisprudence/juris-lux/57_2007_courcassation_22112007.pdf Accessed 09 May 2014

Article 29 Working Party, 11th Annual Report of the Article 29 Working Party on Data Protection, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf

Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended on July 19th, 2013; Unofficial English translation: http://www.dsk.gv.at/DocView.axd?CobId=41936 (last accessed 23 July 2013).

Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007, M.B. 31 May 2007.

Bundesverfassungsgericht, decisions volume 65.

Burkert, Herbert, "Privacy- Data Protection – A German/European Perspective", in Engel, Christoph; Keller, Kenneth H. (eds.), *Governance of Global Networks in the Light of Differing Local Values*, Baden-Baden 2000, pp. 43-70.

[58] Korff, Douwe, *EC Study on Implementation of Data Protection Directive 95/46/EC – Report on the Findings of the Study*, 2002, p. 103.

Cass. Civile, Sez. I, 09.01.2013, Sent. n. 349, in: www.ilsole24ore.com/pdf2010/SoleOnLine5/Oggetti_correlati/Documenti/Norme%20e%20Tributi/2013/01/corte-cassazione-sentenza-349-2013.pdf

Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data modified by the Law of 31 July 2006 the Law of 22 December 2006 the Law of 27 July 2007 (Luxembourg) available at: http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf

Corte d'Appello di Milano, Sent. 11.05.2010, judgement availble at www.garanteprivacy.it (last accessed 15 June 2013).

Decision No. 24/1998. (VI. 9.) AB (Hungarian Constitutional Court).

Decision No. 44/2004. (XI. 23.) AB (Hungarian Constitutional Court).

DLA Piper (2013) Data Protection Law of the World, available online at: http://www.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf

Durant v Financial Services Authority [2003] EWCA Civ 1746.

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

ECJ, *European Commission v. Federal Republic of Germany*, case C-518/07, 9 March 2010.

ECJ, *European Commission v. Republic of Austria*, case C-614/10, 16 October 2012.

ECtHR, *Gaskin v. the United Kingdom*, application no. 10454/83, judgment of 7 July 1989.

ECtHR, *Leander v. Sweden*, application no. 9248/81, judgment of 26 March 1987.

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.

European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigations, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (General Data Protection Directive), COM(2012) 10 final, Brussels, 25 January 2012.

European Union Agency for Fundamental Rights (FRA) *Access to data protection remedies in EU member states*, 2013.

European Union Agency for Fundamental Rights (FRA) *Access to Justice in Europe: an overview of challenges and opportunities*, 2011.

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

Ezsias v Welsh Ministers [2007] All ER (D) 65 (Dec).

Garante per la protezione dei dati personali, *Video Surveillance decision dated 8 April 2010*: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1734653

Grundgesetz, available at: http://www.bundestag.de/bundestag/aufgaben/rechtsgrundlagen/grundgesetz/index.html

Hannah, Matthew, *Dark Territories in the Information Age. Learning from the West German Census Controversies of the 1980s*, Farnham, Ashgate, 2010.

IV. ÚS 40/03, The Constitutional Court of Slovakia, The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2003a/190_03a.pdf

IV. ÚS 44/00, The Constitutional Court of Slovakia. The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2001a/10_01a.pdf

KLAGESAK 2005-02: Klage på Datatilsynets vedtak om å avvise sak med krav om innsyn i innbetalt forsikringspremie Personvernnemndas avgjørelse av 9.8.2005: available at: http://www.personvernnemnda.no/vedtak/2005_2.htm.

Korff, Douwe, *EC Study on Implementation of Data Protection Directive 95/46/EC – Report on the Findings of the Study*, 2002, p. 103.

McCahill, Mike and Clive Norris, "Estimating the extent, sophistication and legality of CCTV in London", in Gill, Martin (eds.), *CCTV*, Leicester, Perpetuity Press, 2003. Gras, Marianne L., "The legal regulation of CCTV in Europe", *Surveillance & Society*, Vol. 2, 2004, pp. 216-229.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Spain) available at: http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html

Metropolitan Court (Hungary) 26.K.32.704/2012/5.

Nijman, Janne Elisabeth, *The concept of international legal personality. An enquiry into the history and theory of international law*, T.M.C. Asser Press, 2004
PL. ÚS 1/09, The Constitutional Court of Slovakia, The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2011a/1_11a.pdf

Personal Data Protection Code (Italy) available at: http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf (last accessed 15 June 2013)

René Seerden, *Administrative law of the European Union, its member states and the United States: a comparative analysis*, Antwerp, Intersentia, 2007.

The Data Protection Act (1998) (UK) available at: http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 31 March 2013)

Tribunal de Première Instance de Bruxelles, Civ. Bruxelles (pres.), 22 March 1994.

Tribunale di Milano, Sent. 04.02.2009, judgement available at: www.garanteprivacy.it (last accessed 15 June 2013).

Locating Data Controllers – A Meta-Analysis of ten EU Member States

Dr Xavier L'Hoiry & Professor Clive Norris

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. Informational self-determination, a term derived from a fundamental ruling of Germany's Federal Constitutional Court concerning the legality of the personal data collected by the German census in 1983, concerns the ability of data subjects to determine how and to whom they wish to disclose their personal data[59]. In their analysis of the German census case, Hornung and Schnabel explain the concept of informational self-determination thus:

> 'The self-determined development of the individual is a precondition for a free and democratic communication order. If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, and if they cannot even appraise the knowledge of possible communication partners, they may be inhibited in making use of their freedom. If citizens are unsure whether dissenting behaviour is noticed and information is being permanently stored, used and passed on, they will try to avoid dissenting behaviour so as not to attract attention. They may even abstain from making use of their basic and human rights. In a potentially all-knowing state, freedom of speech and freedom of choice are virtually impossible.'[60]

For informational self-determination to work in practice, data subjects must have access to their personal data and be able to know how this is processed and with whom it is shared. In this context, 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

[59] Bundesverfassungsgericht, decisions volume 65, p. 1 ff.

[60] Hornung G. and Schnabel, C. (2009) 'Data Protection in Germany I: The population census decision and the right to informational self-determination', *Computer Law & Security Report*, 25(1): 84-88 pp: 85-86

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, we collected both quantitative and qualitative data. The quantitative data would enable us to paint a broad picture as to how citizens might fare in their quest to exercise their rights, and qualitative data would help us in understanding the processes which either facilitated or hindered these requests. From the quantitative data we therefore formulated a number of *indicators* to explore the ease or difficulty of locating data controllers and their contact details, and also measure the transparency of practices in facilitating subject access requests.

Overall findings[61]

Table 1 – Success[62] ***rate in locating data controllers***

Country	**Success rate**	**Success rate %**	**Total**
Austria	24/32	75%	32
Belgium	33/35	94%	35
Germany	26/32	81%	32
Hungary	29/31	94%	31
Italy	26/33	79%	33
Luxemburg	23/33	70%	33
Norway	25/33	76%	33
Slovakia	25/34	74%	34
Spain	23/30	68%	30
UK	28/34	82%	34
Total (average)	262/327	80%	327

In order to exercise one's rights, one must firstly be able to locate the data controller. As evidenced in Table 1, the percentage of cases in which it was possible to do this among the ten participating countries ranges considerably from 68% to 94% with the overall average success rate being 80%. This effectively means that in a fifth of instances, it is not possible to locate a data controller or their contact details in order to proceed with a subject access request.

[61] All numerical data is rounded up to the nearest whole number (or half number in some instances).
[62] 'Success' in this context is defined as identifying a data controller and locating their contact details.

These overall findings mask some significant variations. For instance, in Belgium and Hungary, it was possible to locate a 94% of data controllers (and the two failed attempts in Belgium concern Facebook and Google, both of whom appear to employ ambiguous and complex privacy policies[63]). Putting these two countries aside, in the remaining eight countries data subjects are unable to fulfil the basic pre-requisite of making an access request in around a fifth of all cases.

In trying to understand how citizens are denied even the most fundamental requirement to exercise their rights and knowing who to demand them from, we need to explore the mechanisms through which the citizen can locate the person, or office, responsible in an organisation for dealing with their requests. As it turns out, each of these (on-line, telephone or in person) have their own peculiar features which promote or thwart citizens' attempts. We explore these further below.

First, we need to consider which methods were most frequently used and, secondly, the 'success rate' of the differing methods.

Table 2 – Methodology used in successful instances of locating data controller

All Countries	**Method – Web[64]**	**Method – Phone**	**Method – In person**	**Total**
Total	166 (63%)	70 (27%)	26 (10%)	262 (100%)

Of all the cases where data controllers were successfully located, the majority of these were located online. The web method, which includes locating data controllers via email, totals 63% of all 'successful' cases. In other words, using the telephone and visiting sites 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. Vicariously, 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 internet.

Table 3: Success and failure rates of locating data controllers according to method used[65]

[63] See for example Amberhawk, who analysed Google's privacy policy and highlighted a number of fundamental failings. Available at http://www.amberhawk.com/uploads/Google_privacy_docs.pdf

[64] The web method includes successfully locating data controller information via email.

[65] 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.

All Countries	Online – Success	Online – Failure	Phone – Success	Phone – Failure	In person – Success	In Person – Failure	Total – Success	Total – Failure
Total (average)	166 (70%)	70 (30%)	70 (77%)	21 (23%)	26 (43%)	34 (57%)	262 (68%)	125 (36%)

Locating the data controller online

The main method of locating data controllers 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.[66] 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.

Data controllers can hinder or facilitate data subjects' attempts to find and view an organisation's privacy policy 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 on-line 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.

Time spent locating data controller details

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.

Table 4: How long (in minutes) did it take to locate data controller details on organisations' websites?

All	1-2 minutes	3 - 4 minutes	5+ minutes	Total (%)	Mean Average

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

Countries	(%)	(%)	(%)		Minutes
Total	50 (34%)	40 (27%)	57 (39%)	147 (100%)	4.5

Where the data controller contact details were sought on organisations' websites, as Table 4 shows, in only 34% of 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[67]. This raises questions regarding the visibility of privacy-related links on websites as well as the quality of the content available. Reinforcing these findings, some country-specific results are noteworthy – in Austria, a significant majority (83%) of data controller details were located within 1-2 minutes of browsing a website. At the other end of the spectrum however, in Luxemburg and Spain it took 5 minutes or more to locate data controller information in half of all cases.

Organisations largely rely on online platforms to disseminate their privacy and data protection policies which should also outline subject access procedures to data subjects and potential service users. As a result, their websites should be designed and equipped with sufficient functionality to enable the user to locate the relevant subject access information quickly and easily. In the majority of cases, data subjects are helped to do this by the presence of search functions and the availability of content without having to log in to 'registered members only' sections. However in 39% of cases it required five minutes or more of searching online before locating data controller details. In over half of all cases, it is also necessary for users to complete three or more 'clicks' before arriving at the desired content. The absence of templates, (less than 1 in 5 sites provides them) further restricts the ease of making access requests, as does the failure of half of all organisations to provide data subjects with basic information about what type of data that is collected and stored about them. The failure to provide this information demonstrates poor transparency practices on behalf of data controllers, a finding reinforced by the ratings given to the visibility of privacy links and the quality of the content in privacy policies which, in approximately a third of cases were rated as poor.

Locating the data controller by telephone

In several instances, it was necessary to contact data controllers via telephone and as Table 2 illustrates, this was the case in more than a quarter of all successful attempts to locate data controller information (26%). The qualitative data shows that the choice of telephone as the method via which to contact data controllers was often a secondary one insofar as a different method had at first been attempted but this led the researchers to a telephone number that they were advised to ring for further information. In Norway for example, the researchers made considerable use of the telephone method in part because their online searches frequently led them to telephone numbers as the sole medium through which to contact data controllers directly. In several other countries, in the context of CCTV systems, researchers attended sites in person but often found signage directing them to a contact telephone number for further information. These instances are illustrative of the data subject necessarily undertaking a concerted effort to locate the type of information which, in theory, should be openly accessible.

[67] All researchers in this project had above average computer literacy.

The experiences of researchers seeking data controller information on the phone varied. The use of the telephone was often a secondary attempt after other methods had failed or had naturally directed researchers to telephone a data controller. The difficulty of using this method to locate data controller details is indicated by the speed with which they successfully found such details. More than half the time (54%), data subjects will need to be on the phone for over 5 minutes before successfully obtaining the requested information. As such, in many cases, individuals may incur a pecuniary disadvantage due to the costs of premium telephone lines. If data controllers choose to direct citizens' queries to a telephone number, they must ensure that the respondent is able to answer such queries. However, we found that researchers had to speak to more than one person in half of all cases. This suggests that telephone numbers are either not directed to departments/officers with the requisite knowledge to answer data protection-related queries or that telephone respondents in general are insufficiently trained in data protection matters. Finally, in over a fifth of cases where researchers received guidance on the phone, it was rated as being of such 'poor' quality, that it effectively undermined data subjects' ability to exercise their informational rights.

Locating the data controller 'in person'[68]

While online and telephone enquiries were successful in over two-thirds of cases, this was not true of in-person enquires. In less than half of all instances where a site was visited in person were researchers able to locate data controllers (43%). This represents the highest 'failure rate' of any of the methods utilised in this study. There are a number of reasons for this. First, the level of knowledge and expertise of representatives of data controllers to whom researchers spoke when attending sites 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. Second, 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 Norway for example, respondents consistently (and incorrectly) instructed researchers to contact the police in order to make an access request for CCTV footage. Finally, these findings show that in some cases, representatives of data controllers simply could not be located on site. Instead, many sites rely on (often inadequate) signage to notify the public of the surveillance measure and re-direct queries to a postal address, telephone number or an email address.

Locating the Data Controller in person at CCTV sites

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, we were 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 (i.e.: in the UK, Austria, Hungary, Norway, Spain and Belgium (and in some cases in Italy)) to identify the data controller within such signage, as well as provide contact details for queries from members of the public[69].

[68] While a small number of non-CCTV sites were researched in person, this section focuses only on CCTV sites given the issues of legality/illegally as well as good and bad practices employed by data controllers.
[69] See Appendix 1 for individual country reports regarding data protection legislation.

As the qualitative data revealed, interactions with organisational staff either on the phone or in person often showed a systematic lack of knowledge, expertise and awareness concerning data protection and privacy matters, and particularly access right procedures. This lacuna was most prominent in the context of access rights in relation to CCTV systems. In one case in the UK, the researchers were advised that a company's policy was never to share CCTV footage with members of the public under any circumstances, a statement clearly in contravention of British legislation. In Germany, researchers were provided with extremely unclear explanations about CCTV recordings, firstly being told that footage only records the previous hour and then, having sought clarification on this advice, being met with animosity and told that the footage was not stored locally so could not be accessed in any case. In Spain meanwhile, the researchers were required to speak to four different people on the phone before finally obtaining an acknowledgement that they were indeed legally allowed to submit an access request for their employment records. In Italy, the mere use of terminology such as 'data controller' confused members of staff and researchers were simply advised to search online for such information. In a number of other countries, most notably in Norway, researchers were advised to contact the police in order to request CCTV footage. Such advice is plainly wrong. These denial strategies appeared to be unwitting insofar as these were the results of behaviours and practices undertaken in good faith even if in contravention of national legislation. In these cases, data controllers and their representatives did not appear to *deliberately* deny data subjects the opportunity to exercise their access rights but nevertheless delivered services or provided advice which was legally inaccurate and ultimately misdirected the researchers in their attempts to locate and contact data controllers.

The lack of experience in dealing with subject access requests and other data protection queries went hand in hand with low levels of awareness and indeed several of the researchers were advised by data controller respondents that they had never before received queries about access rights.

The poor level of awareness and knowledge of data protection and privacy law may be attributed to a lack of training for members of staff, and is in turn is linked to the inexperience of staff in receiving these types of queries. Related research concerning data subjects' access to redress mechanisms has found a similarly low level of legislative expertise across Member States[70]. The absence of data protection training is in itself attributable to a low demand amongst service users/customers for this type of expertise, thereby negating the need for staff to be trained in this type of so-called niche request. Something of a vicious circle therefore emerges in which staff are not trained in data protection matter because such queries rarely arise. But when these queries are made, staff lack the knowledge with which to address them adequately and data subjects are discouraged from pursuing this type of request. At an organisational level, the failure to train staff and develop clear policies and procedures to be followed can be characterised as a strategy of denial.

Alongside the absence of awareness and experience of dealing with data protection (and specifically access rights) queries, a further strategy of denial was the negative and discouraging attitudes and behaviours displayed by frontline staff. In many instances, the first response researchers received upon asking for data controller contact details was to be asked why they were making such a request. Although a seemingly innocuous remark, this response immediately placed the researchers in a position in which they were expected to justify their request rather than simply expect to receive an answer. In some such instances, data

[70] European Agency for Fundamental Rights (2014) Access to Data Protection Remedies in EU Member States, available at http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

controller representatives refused to disclose data controller contact details if researchers' justifications were not deemed to have fulfilled their expectations of a legitimate reason for seeking such information. Aside from some minor exceptions[71], European and national legislation does not necessitate a justification, it is merely one's right, to submit an access request and so such demands to know why one wishes to obtain data controller contact details from data controller representatives has no basis in law.

In a number of cases, when researchers asserted they simply wished to exercise their legal right of access, this seemed to antagonise data controller representatives. Many of the researchers reported that they were often made to feel as though their queries were unimportant and a waste of valuable time for staff members who had infinitely more pressing matters to deal with. Elsewhere, queries were treated with indifference by staff who assumed that such requests were neither urgent nor imperative and provided inaccurate and misleading responses. Even more discouragingly, at other times requests were met with open suspicion and hostility, requiring researchers to be persistent and resolute in demanding information. An asymmetry of power emerged in such cases with the data subject being placed at an immediate disadvantage and effectively forced to negotiate with data controller representatives in order to exercise his/her legal right of access.

Such dismissals of data protection and privacy queries potentially serve to discourage data subjects from pursuing such interests, once more feeding into the vicious circle of low numbers of data protection queries being met with low levels of such expertise and awareness.

Many of these troublesome interactions could have been avoided in the case of CCTV systems if adequate signage had been provided.

Presence of CCTV signage[72]

The first question to address is 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 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.

Table 11: Was signage present at location of CCTV?

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

[71] In Belgium for example, national legislation demands that data subjects provide a justifiable reason for requests to obtain CCTV footage.
[72] See Appendix 1 and the individual country reports for photographs taken on site of CCTV signage.

Researchers were able to locate CCTV signage on site on average in over four fifths of cases (82%). This effectively means that approximately 1 in 5 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 surveillance. While in some countries the presence of signage is the norm, (in Italy, Luxemburg, Slovakia and the UK signage was displayed in all the sites visited), in other countries such as Belgium, Spain and Norway, signage was absent 40% of the time.

Contact details on CCTV signage

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: altering 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.

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?

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

On average, researchers found that contact details on signage are only available in just under a third of cases (32.5%). This effectively 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. In Austria, Germany, Hungary and Norway, contact details on signage were *never* found.

If national legislation is fully complied with, citizens in a number of countries should, in theory, be able to identify operators of CCTV systems and obtain their contact details simply by attending a site in which CCTV is operated and looking at the relevant signage[73]. However, this is frequently not possible. In over two thirds of all cases, researchers were not able to identify a data controller only by visiting the site of the CCTV.

This was borne out by the qualitative data which reveals that the placement and visibility of CCTV signage also caused significant problems. In large areas, researchers at times found only a single sign, requiring the researchers to search for several minutes before locating such signage. At its most basic, one may expect signage to be easy to locate and to be legible, requiring data controller representatives to place such signage appropriately to achieve these simple aims. In Austria, researchers reported that whilst signage was present in most sites, several signs were so small that they were practicably unreadable. In Norway, the researchers found signage to be located far from the cameras themselves and as well being generally displayed in poorly designated areas. In several other countries meanwhile, including

[73] In the UK, Austria, Hungary, Norway, Spain and Belgium (and in some cases in Italy), CCTV operators must identify the data controller/operator of the system on the CCTV signage.

Slovakia and Germany, signs were present but the content of this signage failed to identify the data controller or even provide any form of contact details for further queries. As such, the location of signage in areas with obvious flaws such as low footfall, far beyond one's eye line, or remote locations raises the possibility of negligent placement which may lead one to infer ulterior motives here, whether deliberate or otherwise.

The content of signage also caused problems for the researchers. Unless data controllers were identified together with their postal addresses, researchers were required to make further enquiries. National legislation prescribes that subject access requests must be made in writing. As such, as a legal minimum standard, data subjects must obtain a postal (or email) address for the data controller in order to make a subject access request. In many cases, CCTV signage provided a telephone number via which citizens are invited to make further enquiries. This was particularly prominent in the UK. In such cases, further problems were experienced due to the telephone numbers provided. These numbers often led to general customer services contact centres with little or no awareness of data protection matters. In other cases, telephone numbers led to context-specific departments – signage in a car park provided a telephone number for the parking enforcement department – but these still lack the required expertise to answer questions regarding the collection of CCTV footage. In many instances therefore, the telephone respondents were not equipped with the requisite level of data protection and privacy knowledge to answer queries of this type and the problems detailed above duly ensued. As a result, inaccurate and misleading advice was provided leading the data subject to be ultimately discouraged from pursuing his/her query. Alternatively, if data subjects do indeed continue to pursue their requests, as in the case of this research, the burden is firmly placed upon data subjects to pro-actively locate the relevant information, negotiating with data controller representatives and explaining the nature of their query several times to many different people until they finally reach a respondent capable of answering their questions. As a minimum standard, one may expect telephone numbers provided on CCTV signage to lead directly to a respondent able to discuss matters pertaining to the collection of footage captured by the CCTV. The failure to ensure this is the result of poor procedural and organisational practice and is considered in the context of this research as a clear strategy of denial.

Conclusions

Our results paint a picture of widespread restrictive practices both 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, researchers were not able to locate data controller information, effectively terminating the process of exercising informational self-determination before it has even begun. The over-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 organisations' websites in order to enable data subjects to locate relevant information. Problems naturally arise here in light of the existence of the so-called digital divide[74] 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.

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

The above findings with regards to online interactions with data controllers showed facilitative practice in most cases but also demonstrated poor practice in a significant minority. This includes the 53% of instances in which 3 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 absence of search functions in 1 in 5 of all websites as well as templates being available less than a fifth of the time indicates poor website design on behalf of organisations as well as the content provided within these 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.

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 sites in person. In over two thirds of all cases, it was not possible to successfully identify a data controller only by visiting a site 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 negative findings in this part of the 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.

Submitting Access Requests – A Meta-Analysis of ten EU Member States[75]

Introduction

Access to one's personal data is a fundamental element of the EU's data protection framework, ensuring that data subjects are able to effectively manage their data as well as holding data controllers accountable for the ways in which they collect and process personal data.

This phase of the research involved submitting access requests to data controllers. In doing so however, researchers sought to obtain not just their personal data but also questioned data controllers as to the ways in which their personal data is processed. Specifically, requests asked data controllers to disclose information regarding their third party data sharing practices and whether they used any automated decision making processes (and if so how) in the course of collecting and storing personal data. The meta-analysis below is composed of quantitative and qualitative findings. As such, the first section will describe how often facilitative and restrictive practices were encountered in the research before the second section elaborates on how such practices manifested themselves in the course of data subjects' attempts to exercise their informational rights.

Quantitative Analysis

In order to delineate between facilitative and restrictive practices of data controllers in the context of the access request process, a number of indicators were formulated. These indicators sought to determine firstly whether data controllers acted in a manner which was legally compliant and secondly whether they employed practices which helped and encouraged data subjects to exercise their informational rights or discouraged and restricted them from doing so[76].

The discussion and accompanying tables below are considered in a chronological sequence, beginning at researchers' attempts to submit their access requests and ending with an analysis of the quality and fullness of the responses received.

The discussion below will show that researchers generally struggled in all aspects of the access request procedure. It was frequently difficult to obtain personal data and data controllers showed clear reluctance to answer queries regarding third party data sharing and automated decision making processes. Table 1 brings together the three main features of researchers' requests (personal data; third party data sharing practice; automated decision making systems) and shows, on average, how often researchers obtained positive outcomes in the responses from data controllers.

[75] All percentages are rounded up/down to the nearest whole number.

[76] See Appendix 3 for a description of how facilitative and restrictive practices were coded in the researche.

Table 1: Summary of findings regarding the responses received to subject access requests

Countries	**Positive Outcome**[77]	**Negative Outcome**[78]	**Total**
Austria	6 (35%)	11 (65%)	17 (100%)
Belgium	8 (44%)	11 (56%)	19 (100%)
Germany	8 (50%)	8 (50%)	16 (100%)
Hungary	8 (42%)	11 (58%)	19 (100%)
Italy	6 (33%)	12 (67%)	18 (100%)
Luxemburg	8 (44%)	11 (56%)	19 (100%)
Norway	5 (33%)	10 (67%)	15 (100%)
Slovakia	7 (37%)	12 (63%)	19 (100%)
Spain	8 (38%)	13 (62%)	21 (100%)
UK	15 (71%)	6 (29%)	21 (100%)
Total	79 (43%)	105 (57%)	184 (100%)

Across the entire study, less than half (43%) of all applications resulted in a positive outcome. In the majority of cases therefore (57%), some aspect of researchers' requests was answered inadequately. This ranged from non-disclosure of personal data to receiving inadequate responses to queries regarding third party data sharing practices or the use automated decision making processes. The lowest rate of positive outcomes was experienced in Italy and Norway (both 33%), where on average, only a third of responses could be regarded as adequate. This figure was barely higher in Austria, Spain, Slovakia and Norway, where no more than 40% of adequate responses were received on average. Indeed, nine out of the ten the countries in the study did not receive positive outcomes in more than half of all instances. Only the responses received by the UK-based researchers resulted in more than half of the outcomes being positive with 71% of cases ending in a positive outcome.

Number of correspondence necessary in order to receive personal data

The process of submitting a request can often be complex, necessitating clarifications and the provision of additional information to the data controller before the request is considered to be 'complete'. In turn, the research found that it was frequently necessary to correspond at length with some data controllers before a request could even be successfully submitted let

[77] Positive outcomes are cases in which all three of researchers' queries were adequately addressed by data controllers.

[78] Negative outcomes are cases in which at least one out of three of the researchers' queries were not adequately addressed by data controllers.

alone processed. On average, the results show that researchers needed to send over two correspondences in order to successfully submit an access request and obtain access to one's personal data (2.15 on average). In some countries, the average number of requests sent was as high as 3.1 (Belgium and Spain). However, in Austria, it was only necessary to send only 1.3 correspondences on average in order to successfully submit a request.

The higher averages of requests in some countries can be partially explained by the lack of information provided by data controllers regarding informational rights. In such cases, researchers were often required to send somewhat general letters to addresses which were frequently not those of the relevant department/officer. In the absence of guidance regarding what to include in an access request, additional correspondence was often necessary to provide data controllers with identification, payment or other further details regarding the request. In contrast, sites in which just a single correspondence was necessary in order to submit a request tended to reflect a strong level of information provided to data subjects coupled with the easy availability of data controllers' contact details which ensured that requests were directed to the appropriate department in an organisation. Specifically, the provision of templates via which to submit access requests frequently meant that data subjects had a clear pathway to exercise their rights, indicating the type and level of information required to process a request as well as any other requirements.

Receipt of a Holding Letter

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 and setting a deadline by which time the request will have been processed and responded to. Generally speaking, holding letters may 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. 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.

At the other end of the scale however, in the UK (71%) and Germany (69%) in over two-thirds 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.

Access to personal data

A variety of general and sector-specific legal exemptions exist across different EU member states restricting data subjects' access to personal data. Even when data subjects' right to access are denied, if this denial is based on a coherent legal argument, even if contestable, we deemed this a success. Nevertheless, the research results show that access to personal data was still denied illegitimately in a high number of cases.

Researchers were able to obtain access to their personal data in only just over half of all cases (57%). In 43% of instances, researchers were denied access to their personal data with either no reasons provided or by relying upon incorrect or inaccurate legal reasoning. Indeed, in half (five) of the countries involved in the research, it was not possible to access one's data in any more than half of the sites visited. This was true of the researchers' experiences in Belgium, Italy, Luxemburg, Norway and Spain. At the other end of the spectrum, access to personal data was successfully achieved in 81% of cases in the UK, 80% in Germany and 74% in Slovakia. However, this still means that access was denied in a significant minority of cases in these countries and even an 81% success rate should not be celebrated as an outstanding result. It still means that one in five requests were denied without a valid reason.

Receiving incomplete personal data disclosures

Successfully receiving one's personal data should not be taken to automatically indicate good practice on behalf of data controllers. In some cases, researchers reported having received partial disclosures with little or no explanation why the remainder of the data was not available (see the country reports for specific case summaries of such instances). In such cases, the burden habitually falls on to data subjects to pursue data controllers often with no substantive evidence of these incomplete disclosures aside from the individual's belief that some data remains undisclosed. This problem of 'unknowables' occurred frequently in the study as researchers were often left with the impression that the personal data disclosed by data controllers was incomplete. However, in the absence of absolutely certainty, researchers noted difficulties in challenging such disclosures particularly in cases involving large, multinational data controllers.

It was necessary for researchers to demand additional disclosures from data controllers in one-third of all cases, although the disclosure of personal data was eventually successfully completed. This was because data controllers had failed to provide all the data held about the data subjects in their first attempt to fulfil the access request. Why data controllers did not disclose all personal data in the first instance is open to speculation but some context-specific cases indicate that some data controllers were at best negligent in their disclosures and at worst wilfully attempted to restrict the amount of data they provided to data subjects.

Although some countries show such partial disclosures to be a relatively rare occurrence (only 8% of cases in Germany and 7% in Slovakia), the results in other countries are significantly worse. In Belgium, personal data was fully received in the first instance in only one quarter of cases (25%). In the remaining 75% of cases, it was necessary for the researcher to send several correspondences before finally receiving the remainder of the data.

Receiving an adequate response from data controllers regarding third party data sharing

As well as obtaining access to their personal data, researchers asked data controllers for details regarding their third party data sharing practices. Although researchers asked for specific details of specific data being shared with specific third parties, existing legislation allows data controllers to provide only 'the recipients or *categories of recipients of the data*'[79].[80] The impact of this legislative wording upon data subjects' informational rights is discussed elsewhere[81] and indeed the proposed reform of EU data protection law will no

[79] 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, OJ 1995 L 281/31.
[80] Emphasis added by author.
[81] See the above cross-European comparative analysis of legal and administrative framework of access rights.

longer allow data controllers to respond to future requests in such general, non-specific terms[82]. Nevertheless, these were the legal obligations upon data controllers at the time of the fieldwork and as such, generalised and non-specific responses of this type were considered to be 'successful' for the purposes of the research since they were legally compliant, although clearly unsatisfactory from an informational rights perspective.

The results show that in over half of all cases (56%), data controllers did not provide an adequate response concerning their third party data sharing practices. Such inadequate responses ranged from complete non-response; a response being received to the request but failing to address third party data sharing; or finally, some mention of third party data sharing but in an insufficient manner as to be considered legally compliant. In some countries, the number of inadequate responses was as high as 76% of cases (Austria), 61% (Italy), 63% (Slovakia) and two thirds of all instances in Spain.

Even in those countries where the majority of data controllers provided adequate responses concerning their data sharing practices, such as 71% in the UK, there still remained a substantial minority of instances in which only inadequate responses were received (29% in the UK and 33% in Germany).

Receiving an adequate response from data controllers regarding automated decision making processes

Alongside querying data controllers' third party data sharing procedures, researchers also sought information regarding the use of automated decision making processes and the impact of such systems upon their personal data. It should be noted that questioning the use of such systems was not appropriate or relevant in every site. However, the question was designed not only to obtain specific information about this type of data processing but also to analyse data controllers' willingness to respond to queries about the use of such processes given the potential issues of disclosing trade secrets[83].

In over two thirds of cases (71%), data controllers did not provide an adequate response with regards to the processing of their personal data via automated decision making processes. An adequate reply was received in just one case in Slovakia, meaning that inadequate responses were received in 95% of instances. Austria and Italy demonstrated similarly poor findings with only 24% and 17% (respectively) of data controllers addressing automated decision making queries adequately.

The number of correspondences exchanged between data subjects and data controllers (and other intermediaries such as national DPAs etc) can often become significantly burdensome for the individual data subject. Such instances may in some cases discourage data subjects from exercising their rights, so convoluted, costly and time-consuming is the access request process that some individuals may become unwilling to persevere with their involvement in the process. In Table 2 we document the 'worst' cases in each country – i.e.: the cases that required the most correspondence to complete the access request and to receive an adequate response concerning third party data sharing and automated decision making processes.

---

[82] LIBE Draft report 2012/0011 (COD) dated Dec. 17 2012 (12 PVLR 65, 1/14/13), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

[83] See for example the issue of trade secrecy in a recent German case which considered the disclosure of credit scoring data. A summary of the case is available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=2ef8cefa03b7d0493f54c1bc71ee0a53&anz=1&pos=0&nr=66583&linked=pm&Blank=1

Table 2: Single highest number of correspondences required in each country in 'worst' cases to resolve the request

Countries	**Access request considered complete**	**Third party data sharing adequately addressed**	**Automated decision making processes adequately addressed**
Austria	2	2	2
Belgium	6	4	3
Germany	4	4	N/A[84]
Hungary	3	2	4
Italy	5	5	4
Luxemburg	3	2	2
Norway	6	6	6
Slovakia	2	3	1
Spain	12	9	8
UK	10	3	6
Average[85]	5.3	4	4

The results of the study show that in the most extreme cases, researchers were required to send an excessive number of correspondences before their requests were accepted and considered to be 'complete' by data controllers. Specifically, in Spain, the case in which the most interaction was necessary saw 12 correspondences exchanged while in the UK, the most extreme case involved 10 correspondences. Rather more positively however, even the worst case in Austria required only two correspondences to be sent before a request was considered complete, demonstrating the relatively straightforward process of submitting a request in the sample approached in this country.

Sector-specific analysis

Public vs. Private Sectors

At the outset, we had speculated that there may be a significant difference between how public and private bodies would respond to our requests. This is indeed borne by the results.

[84] Not applicable since not a single adequate response was received concerning automated decision making processes in Germany.

[85] Average calculated over 9 countries since Germany did not receive an adequate response to automated decision making processes during the research.

Table 3: All Facilitative and Restrictive Practices[86] based on public organisations compared with private organisations

Public – Facilitative	Public – Restrictive	Public - Total	Private – Facilitative	Private – Restrictive	Private – Total	Total
40 (57%)	30 (43%)	70 (100%)	43 (38%)	71 (62%)	114 (100%)	184

As Table 3 shows, the public sector delivered a significantly higher proportion of facilitative practices in the research in comparison with private sector organisations. While 57% of requests made to public sector agencies resulted in facilitative practices, a substantial majority (62%) of requests to private sector organisations led to restrictive behaviours and procedures. However, exceptions to these conclusions should not be ignored. In over two fifths of public sector cases (43%), restrictive practices were evident. Parallel to this, almost 40% of organisations in the private sector employed facilitative strategies, enabling data subjects to effectively exercise their access rights and often displaying best practice across the entire research.

Variations on this overall finding were found in some countries. In Belgium, Luxembourg and Spain, the private sector actually performed at least as well as public sector agencies, generally displaying more facilitative practices and helping citizens to enact their access rights in a smoother way. It is also worth mentioning that in the UK and Germany, responses received from public sector organisations were almost universally facilitative. The public sector in these two countries showed extensive strategies of facilitation and represented the best examples of public sector practices and procedures across the research.

In the main, broadly facilitative practices were experienced when contacting public sector organisations in this study. Although it might be thought that the police would be one organisation who would be most reluctant to share information with citizens and would often have a legal basis for not doing so, we found the contrary. In fact the responses received to requests made for police records were almost universally facilitative, with an adequate response being received in seven out of eight cases.

The type of data disclosed usually took the form of a statement that no data was held about the data subject. In the case of two requests (in the UK and Germany), the data included entries held on police records when the requesters had been recorded as victims of or witnesses to criminal incidents.

Similarly, the responses to requests made to local authorities/municipalities broadly demonstrated good practice, with seven out of the eight requests being dealt with in a facilitative manner.

These public sector organisations usually disclosed personal data as well as outlining with whom the data is shared and how data is processed. One request - made in Italy - encountered problematic practices chiefly because it was evident during interactions with the data

[86] Facilitative or restrictive practices determined by individual researchers by considering overall experiences in a given case.

controller representative, that the request was the first of its kind to be received by the organisation.

The type of data disclosed ranged widely, demonstrating the breadth of information held about data subjects by this type of data controller. Data included biographical information (such as address, date of birth, etc), tax information and details about dependants (i.e.: children).

CCTV

In our original sample, we included a high number of CCTV sites in a range of different settings. We were particularly interested to discover whether, as an increasingly pervasive and highly visible surveillance technology in Europe, this had led to well developed access rights being developed compared with other sectors. This is also particularly important because citizens never explicitly consent to having their data captured by CCTV cameras. Therefore, accountability and transparency mechanisms gain more importance. As Table 4 demonstrates, this was not the case.

Table 4: Facilitative and Restrictive Practices based on CCTV sites compared with Non-CCTV[87] sites

CCTV – Facilitative	**CCTV – Restrictive**	**CCTV – Total**	**Non-CCTV – Facilitative**	**Non-CCTV - Restrictive**	**Non-CCTV – Total**	**Total**
15 (30%)	35 (70%)	50 (100%)	67 (50%)	67 (50%)	134 (100%)	15 (30%)

It is clear that subject access rights concerning CCTV across Europe are extremely difficult for citizens to enact. In over two thirds of cases, data controllers employed restrictive practices which prevented citizens from exercising their rights and in 60% of cases data was withheld without referring to a valid legal reason.

Because of the low numbers in each country, it is difficult to make meaningful comparisons. However, it is noteworthy that in Belgium, every site engaged in restrictive practices and no personal data was disclosed (although in two cases a valid legal reason was given for this non-disclosure). In contrast, in the UK half of the sites facilitated citizens' in their requests and in five out of six cases, access to footage was allowed.

Overall, European citizens are particularly ill served when attempting to obtain their personal data in the form of CCTV footage. The research found that data controllers employed a variety of strategies to deny data subjects' access to this type of personal data, employing a wide range of restrictive practices with only a handful of organisations following correct legal procedure in responding to access requests.

Table 5: Facilitative and Restrictive Practice based on public CCTV sites and private CCTV sites

CCTV	**CCTV**	**Total**	**CCTV**	**CCTV**	**Total**

[87] Non-CCTV cases are all requests made for data which did not include CCTV footage.

Public – Facilitative	Public Restrictive		Private - Facilitative	Private - Restrictive	
11 (38%)	18 (62%)	29 (100%)	4 (19%)	17 (81%)	21 (100%)

As Table 5 shows, public sector practices were restrictive in the majority of cases with only 38% of data controllers in the public sector enabling citizens to exercise their rights. Worse still, in the private sector, only 19% of data controllers employed facilitative strategies, meaning that a vast majority of organisations demonstrated the use of restrictive policies and procedures, substantially hampering data subjects' attempts to access personal data in the form of CCTV footage or be given further information on how the data was processed and with whom it was shared.

Data controllers in the digital age

Unlike in the case of CCTV footage and arguably local authority records where much data is not necessarily in a form that may easily be shared with data subjects, in the case of banking, mobile telephony and loyalty card schemes, the data is purely digital. As such, this data is potentially relatively straight-forward to disclose to data subjects and there should be clear policies surrounding data sharing and in particular automated decision making processes. We would argue that the data held by such organisations is regularly subjected to automated decision making processes. For instance, the practice of customer profiling which targets specific promotional offers to a particular customer is in our view clearly a case of automated decision making. Similarly, as was confirmed to us in a Luxembourg bank's response to our access request, automated decision making is involved every time a customer makes a withdrawal from an ATM machine since the customer's account balance must be recalculated to reflect the withdrawal. Indeed, such processes are required by law to screen all transactions for the purpose of fraud and money laundering detection.

Table 6: Facilitative and Restrictive Practice when requesting digitally-held records

Data controller Type	Facilitative	Restrictive	Total
Loyalty card schemes	15 (68%)	7 (28%)	22 (100%)
Mobile Telephony	3 (30%)	7 (70%)	10 (100%)
Banking Records	5 (50%)	5 (50%)	10 (100%)

As Table 6 shows, a substantial majority of cases displayed facilitative practices in the context of requesting data from loyalty card providers. As such, an example emerges of private sector organisations responding, in the main, in a positive way to access requests.

A notable exception exists however insofar as only 50% of responses included adequate descriptions of how the data is processed, specifically concerning the use of automated decision making which, as customer profiling is a crucial function of the use of loyalty cards, is a potentially significant omission.

In the case of one request made in Slovakia to a department store, clear and unambiguous contact details were provided for citizens on the organisation's website to make access requests. Having done so, the data controller responded by disclosing full details of the personal data held as well as an exhaustive list of parties with whom data is shared. Regarding automated decision making, the company's Director has previously stated publicly

that such processes analyse data at an aggregate rather than individual level. Similarly, a request made in Spain regarding a national supermarket's loyalty card scheme generated a response which outlined in detail the range of information collected, how it is processed and a statement that data is not shared with third parties.

In contrast, a request made from Luxembourg in French to a department store whose headquarters were based in Germany, received a response in German which failed to disclose any personal data, ignored the issue of automated decision making and provided confusing information regarding third party data sharing practices. Attempts to clarify the unclear content and receive the missing information by the data subject were met only with silence.

Table 6 also shows that broadly speaking, requests made to mobile phone carriers proved problematic. 70% of cases were considered to have experienced restrictive practices concerning most prominently the depth of data disclosed. Researchers frequently felt that data had only been partially disclosed, particularly since geo-locational data was often missing in response received from data controllers.

In the UK, a request made for data held by a mobile telephone carrier generated a wide range of data which included locational information in the form of coordinates indicating where and when the device was used. The issues of data shared with third parties and automated decision making were also directly addressed in a legally compliant manner.

In contrast, a request made in Italy received incomplete responses save for a clear statement that data is not shared with third parties. The request appeared to create much confusion amongst the data controller's representatives who initially treated the request as a complaint and required significant clarification before attempting to process the request correctly. Similarly in Slovakia, while access to personal data, data sharing practices and automated decision making processes were only partially addressed, the issue of meta-data was explicitly refused by the data controller leading to a referral to the national DPA for adjudication (which is pending at the time of writing).

Meanwhile, Table 6 demonstrates that requests for banking records generated a notable dichotomy between positive and negative experiences. While it was deemed in 7 out of 10 cases that personal data had been disclosed, information on third party sharing practices was rarely outlined (only 30% of cases) and explanations of automated decision making processes were also often absent in 60% of cases.

In Hungary, a request for banking records resulted in complete non-disclosure as a result of administrative deficiencies and procedural inflexibility which included lost mail and a refusal to respond to the request by email. In the end, a promise to re-send a letter which included the personal data was not fulfilled as the letter was never received.

In contrast, a request made in Slovakia received full disclosure of personal data across the entirety of the services provided by the bank as well as specific examples of data sharing with third parties together with the contact details for these third parties.

In the UK, the response from the data controller to a request for banking records highlighted the mixture of practices a data controller may employ when responding to requests. Personal data was fully disclosed by the data controller and data was sourced from a wide range of departments within the corporation, simplifying the data subject's request and avoiding the burden of making several different requests to different departments. However, the data controller completely failed to address the issues of third party sharing practices and the use

of automated decision making processes and when challenged about these omissions, all communications from the data controller ceased. As such, both facilitative and restrictive practices were employed in this case.

Big Five – Big Data

We were particularly interested to see the problems and issues which may emerge in dealing with transnational corporations when relying on national legislative frameworks.

Table 7: Facilitative and Restrictive practices when comparing transnational corporations – Facebook; Google; Microsoft; Amazon; Twitter

Data Controller	**Facilitative**	**Restrictive**	**Total**
Facebook	0 (0%)	8 (100%)	8 (100%)
Google	0 (0%)	7 (100%)	7 (100%)
Microsoft	3 (33%)	6 (67%)	9 (100%)
Amazon	4 (57%)	3 (43%)	7 (100%)
Twitter	2 (67%)	1 (33%)	3 (100%)
Combined	9 (26%)	26 (74%)	35 (100%)

As Table 7 shows, transnational corporations such as Google and Facebook are particularly restrictive in allowing citizens to exercise their rights. In over 50% of cases, they failed to disclose personal data or provide a valid reason for not doing so and they were similarly reluctant to disclose information regarding third party data sharing practices or to adequately address the issue of automated decision making processes.

In the case of requests made to Google, data subjects faced a number of difficulties. In one case, two letters were sent to Google's national headquarters but were returned with a notice that the recipient had not taken delivery. When requests could be made to national offices, these offices refused to process the requests based on the fact that Google's US headquarters act as the data controller. The responses never offered to forward the access requests to the US office and the impetus to do so was left to the data subjects. Once requests were sent to Google's US headquarters, all but one case resulted in silence thereafter.

Requests made to Facebook, at their European headquarters based in Ireland, were also problematic. Five out of eight requests obtained no reply while the remaining three were simply referred to Facebook's self-download online tool. In only one case were the issues of third party data sharing and automated decision making directly addressed and this was the result of an official complaint made to the Irish DPA.

The experience of submitting requests from different countries to the same corporation reveals remarkably varied responses. For instance in the case of Amazon, the Austrian request was essentially denied with the data subject being told that all the relevant information could be found by logging into their account and there was a refusal to address the issues of third party data sharing practices and the use of automated decision making. In Norway, although Amazon agreed to disclose the data and indeed sent the passwords to unlock a disc in which the data was contained, the disc was never itself received. Moreover, the response to the request (which was made in Norwegian), was in English. In the case of the Italian request to Amazon, after a lengthy correspondence, not only was all data held fully disclosed, all the documents were written in Italian. Furthermore, the issue of data sharing

was addressed not just at a generic level (of only the categories of recipients) but specifically detailed the specific identities of the parties that data is shared with. In relationship to automated decision making, Amazon stated categorically that they do not make decisions about their customers based solely on automated decision making processes. While one may dispute whether this is the case, Amazon were at least prepared to clearly state what their policy is.

With regards to requests made to Twitter, there were considerable procedural problems in obtaining an initial response from the relevant department within the corporation charged with responding to access requests. However, once such a response was received, a clear procedure emerged which ultimately led to the disclosure of personal data and in the case of the Italian request, clear statements on the practice of third party data sharing and the use of automated decision making processes.

Summary

In over four out of ten cases, researchers as citizens were denied their subject access rights. Overall, our results illustrate the difficulties faced by researchers in submitting subject access requests and attempting to enact their legally prescribed rights in relation to their personal data. The inability to access one's personal data (or receive a legally accurate reason for the denial) in four out of ten of all cases (43%) means that the right of access is illegitimately and routinely denied by data controllers in a substantial minority of cases, undermining the essence of data subjects' informational rights. Alongside this, researchers were unable to obtain adequate responses from data controllers concerning their third party data sharing practices and their use of automated decision making processes in 56% and 71% of cases respectively. As a result, not only are data subjects denied access to their personal data but data controllers also fail to inform them of how their data is processed, giving data subjects little opportunity to effectively manage their data. Even in those cases where personal data was disclosed and adequate responses were received regarding how data is processed, the findings show that such responses were often not received without significant difficulties. Instead, researchers were required to chase data controllers for a response. Almost a third (31%) of personal data was not fully disclosed in the first instance while a quarter (24%) of responses regarding third party data sharing were only received after the data controller's first response had failed to address this adequately, requiring the data subject to re-submit this part of the request. In the context of automated decision making processes, this figure rises to 37%, representing well over a third of instances in which data controllers failed to address researchers' questions adequately in the first instance (when they did address it at all).

The analysis therefore shows that researchers generally struggled to obtain access to their personal data. However, they also struggled to get answers to specific questions regarding aspects of how their personal data is processed. Where answers were successfully obtained and personal data disclosed, this was often with great difficulty and in fact was often the result of researchers' tenacity rather than the facilitative practices of data controllers. While some countries' results suggest broadly facilitative practices, there are notable exceptions even in these generally positive findings. For example, the UK's results are perhaps the most positive of all the countries in this research. But the UK nevertheless experienced some significant problems. For instance, it was necessary to send on average three correspondences before receiving personal data. In Germany meanwhile, the broadly positive findings were somewhat undermined by the fact that this country was the only one in which not a single adequate response concerning automated decision making processes was received. The same

may be said of Slovakia in which 95% of data controllers failed to address this matter adequately despite otherwise broadly positive results in other aspects of the study.

At the other end of the scale, Spain and Norway often showed the poorest results, seemingly illustrating the broadly restrictive practices of data controllers in these countries. In Italy too, some significantly poor results were evidenced, including the low rate of successful personal data disclosure (44%) and adequate responses regarding third party data sharing practices (39%).

The burden of obtaining a successful response from data controllers is therefore often placed upon the shoulders of requesters while data controllers seemingly employ restrictive tactics involving delays, ignoring queries, poor communication processes or simply failing to respond to a request altogether.

Qualitative Analysis[88]

The previous discussion analysed the outcomes of the research from a quantitative perspective as data subjects attempted to submit access requests. As such, the analysis showed *when* subject access requests are successful or unsuccessful. This section explores *how* and *why* access requests succeed and fail and outlines the discourses and strategies employed by data controllers in facilitative or restricting citizens' attempts to exercise their informational rights. We end by considering the policy implications of our research.

Best Practices

Although much of the analysis below will focus upon why and how data controllers restricted citizens' attempts to access their personal data, it is important to note that facilitative practices were found during the research. The cases below represent some of the best practices experienced and illustrate the myriad of ways in which data controllers helped data subjects obtain a satisfactory response to their requests. These cases display a range of facilitative practices and procedures, demonstrating what can be achieved by both public and private organisations when responding to access requests. Notably, one of the cases below includes a refusal to disclose a copy of the personal data to the data subject. However, in doing so, the data controller relied on a correct reading of relevant legislative provisions as well as attempting to temper this refusal by offering the requester a suitable alternative solution.

Mobile Phone Carrier (UK)

> The organisation's privacy policy can be easily accessed via its official website and the privacy link is located at the bottom of its homepage. The content of the policy itself is strong, including information on the type of data which is collected, retention periods and how the data is stored. This also includes a section entitled 'Access to your personal information' which provides a link to a downloadable template form for making access request. The section also mentions the £10 administrative fee and offers alternative ways to receive the template if one cannot download it. With this in mind, the online content demonstrates good practice by not only explicitly mentioning the right of access but also making available a template via which citizens can exercise this right. This demonstrates pro-activity on behalf of the data controller and

[88] Several case examples are outlined in this section of the analysis. The individual country reports in Appendix 1 present these cases in significantly more depth and provide a context-specific analysis of the access requests submitted in these cases.

a shift of burden away from the citizen. The form itself is fairly basic but covers the information required for the data controller to process a request. It also ensures that requesters enclose the necessary ID and fee for the request which allows citizens to make full and complete requests in the first instance and avoids unnecessary delays such as the exchange of correspondence asking for clarification of the request/the required fee/the required ID.

Having submitted the template, a response was received within the legal timeline. The response provided extensive data including the requester's billing history, transcripts of interactions between the requester and the data controller, data on outgoing calls and text messages and geo-locational data of when and where calls have been made using the telephone. Moreover, the issue of third party data sharing was addressed in a legally compliant manner. Following a further exchange of emails, the issue of automated decision making was also addressed in a satisfactory manner.

What emerged in this case was clear evidence of the organisation showing awareness, knowledge and preparedness of access rights and how to respond to requests for data. The existence of a structured administrative procedure meant that the submission of the request was clear and smooth for the data subject and a timely, unambiguous and extensive response was received from the data controller.

Loyalty Card (Italy)

The company's privacy policy was quickly and easily available via their official website. Having contacted the company asking for information about the data controller, we were provided with the name, phone and fax numbers of the relevant person. Just 13 days after sending our request, we received an email from the data controller with a pdf document attached containing disclosure of data along with information on data sharing and automated decision-making. Moreover, the data controller specified that "*the original document will be sent to you via recorded delivery letter*" (received one week later) and that he was keen to answer to any further questions and/or give clarifications.

The letter disclosed both personal data (name, address and email address) and what consumer data they collect when one uses the loyalty card, such as type of product and price, location of the retail outlet and date of the purchases. The letter also explained that such information is collected "*only when you use your loyalty card"* and data are processed by more than one data controller (for instance, database administrators can process information).

Additionally, the letter provided a list of five third parties with whom our data is shared together with full contact details for these third parties. They also informed us that the data are both paper-based and electronically stored. The address of the "datacentre" was fully disclosed along with information on who has access to the database and how. Finally, the letter explained that we have not been subject to automated decision-making processes and customers are not profiled.

Overall, a few distinctive strategies of facilitation seem to emerge. First, the procedure was very simple and the organisation displayed readiness to respond within the statutory term. It was clear therefore that access requests are dealt with as a matter of priority. Second, the organization was responsive to requests and was well informed about citizens' rights. All questions were addressed in a timely and unambiguous manner which reflected familiarity

with the procedure and also fulfilment of citizens' expectations. Third, and perhaps more notably, the response was comprehensive, transparent and accurate.

Banking Records (Luxembourg)

> The information about where to send the access request and the necessity of a proof of identity was available on the homepage of the bank's official website. The request was sent to the general office of the bank in Luxembourg City, and the reply was received within three weeks of having made the request.
>
> The response received was detailed and it was obvious that the data controller was anxious to provide the requested information. The communication was also very respectful without a hint of suspicion or annoyance around the fact that a request had been made in the first place.
>
> The personal data they sent was extremely thorough and included a printed 50 page file, starting from the data subject's first deposit account in 1993 to the renewal of the bank account in 2011. The received data was clear to understand and seemed complete. Alongside this extensive disclosure of personal data, the data controller also provided information concerning data sharing with third parties and automated decision making processes. Regarding third party data sharing, the bank responded by naming the company with whom data is shared, advising how frequently this is done (on a monthly basis) and explaining why (as part of the services used with a credit card). In terms of automated decision making, the bank directly addressed such processes by providing specific examples (i.e.: when an ATM is used and as part of anti-terrorism and money laundering procedures). Moreover, although highly technical and legal terms were used in the correspondence, the bank made the effort to give further explanations.

Overall therefore, this case demonstrated a range of facilitative practices. The extent of information disclosed, the clarity and the quickness in which the information was provided, as well as the amount of respect with which the data subject was addressed amounted to very good practice on behalf of the data controller.

Police Records (Germany)

> The request was sent to the city's police department and a reply was received just a few days later. The reply was a holding letter which acknowledged receipt of the request and provided an approximate timeline for a complete response from the data controller. As such, the data subjects' expectations were adequately managed and the data controller demonstrated a degree of self-accountability by setting a deadline to respond by.
>
> A few weeks later, another letter was received by the data subject which disclosed his personal data. This letter also outlined details on the database in which personal data is stored as well the legal basis for the collection and storage of the data. The personal data itself included details of specific incidents in which the data subject had been involved (as the parent of a victim) Moreover, the letter informed the data subject about the retention period of the data (3 years) and even provided the exact date at which this data set would be deleted (shortly after the request was submitted).

> Finally, the response from the data controller included full contact details for the city's Data Protection Officer and invited the requester to make further queries to this contact if any of the content of the letter was unclear.

As such, the behaviour and practices of the data controller were transparent as well as from a practical perspective, the response was timely and the disclosure of data through and complete. The receipt of a holding letter provided the data subject with a clear timeline and, at a more basic level, confirmed to the data subject that the request had been received and was being processed. The level of detail provided in the data controller's response was exemplary and included a specific date by which the data subject's data would be erased by the data controller.

CCTV in a government building (Hungary)

> A request was submitted to a public sector organisation for a copy of the CCTV footage captured on its premises. Just eight days later, the data controller of the administration responded. In its response, the data controller explained that it had been unsure how to deal with the request and had therefore sought further advice from the national Data Protection Authority. Acting on this advice, the data controller outlined that "*In compliance with your request and the concerning law, my Office is required to provide you information on the footage. What more I can offer to let you see the footage. I am not allowed to send you a copy of the recording since you are not the only person depicted on it (...). If I forwarded the footage to you, it would violate the rights of third parties."*

This response constituted a legally compliant reaction to an access request since access was granted to view the footage even if a copy of the footage itself was not disclosed to the requester. Moreover, the data controller showed an awareness of the potential privacy breach of third parties appearing on the footage and sought to take steps to minimise this.

As such, several facilitative practices emerge here. Firstly, the response of the data controller was very quick. Secondly, the data controller acknowledged its limitations in knowing how to respond to such requests. Rather than risk sending an incorrect reply, advice was proactively sought to ensure that the matter was dealt with accurately and with clarity, evidently treating the access request with respect and importance. Finally, the compromise proposed to the data subject attempted to strike a balance between fulfilling the request whilst protecting the privacy of third parties, showing a commitment on behalf of the data controller to meet the expectations of the data subjects as much as possible within the confines of the situation at hand.

The above cases therefore represent what can be achieved by data controllers and the ways in which requests can be facilitated even when full and complete disclosure is not available. These practices included clear communication strategies between data controllers and data subjects as well as extensive transparency and accountability practices, encouraging data subjects to trust that their requests are treated with respect and legitimacy and priority.

Discourses of Denial

More than anything exercising one's rights as a citizen to know what data is collected stored and processed about oneself and discovering with whom that data is stored is a communicative act. It is a communicative act in the sense that citizens must construct themselves as data subjects which then place them into a legally proscribed pattern of request

and disclosure. As a data subject, a citizen is placed in a particular relationship with a data controller who has a duty, when asked, to communicate to the citizen either what data is held about them, how it is processed and with whom it is shared, or to provide the citizen with a legally valid reason for not disclosing the information requested. The channels through which this communication is achieved are remarkably varied. It may necessitate the citizen writing a letter, filling in a pre-designed form and dispatching it through the postal email, it may be achieved through email or through an online platform. In some cases it necessitates telephone calls or face to face interactions. In others, correspondences must start with a fax.

The form of communication may have a significant impact in how citizens experience the process of exercise their rights, as will the content of that communication. As our research has found, trying to exercising our rights as citizens is oftentimes not a straightforward process. In a single case, it may involve many different forms of communication and an ability to evaluate and respond to the information communicated by the organisations' representative that a citizen is engaging with. During this process, it may take many months to achieve a satisfactory outcome as data controllers are often tardy in their responses and fail to address all of the information demanded.

In the first instance, the organisation must recognise that the citizen has a right to have a conversation about how their data is used. This turns out to be highly problematic in a significant number of cases. Even if the organisation recognises the right, it does not mean that the content of that communication fulfils citizens' requests. Rather, citizens have their requests discouraged or completely thwarted a series of discourses of denial. We have termed the discourses of denials encountered in this research as follows: out of sight; out of court; out of time; out of order; out of tune; and out of mind. Some of these discourses overlap significantly while others are unique to context-specific requests. Nevertheless, the collection of these discourses significantly restricted researchers' attempts to exercise their access rights in the research. We consider these discourses in detail below using case examples to demonstrate the ways in which our informational rights were restricted using specific examples.

Out of Sight

In order to exercise one's informational rights, the citizen needs to be able to locate the person or office within an organisation to communicate the request to. Somehow, the data controller must be made visible to the data subject and the data controller must recognise the citizen as a data subject, who as a 'data subject' is a bearer of rights. This process turns out to be pivotal as in many cases the invisibility of the data controller made it impossible to assert one's rights. The most obvious manifestation of this is in relationship to CCTV signage. For instance, in the open street system in Oslo, as there was no signage within the vicinity of the cameras, it has never been possible to identify the data controller. In the UK, in a branch of a leading high street retailer, no signage whatsoever could be found in the store despite numerous and visible CCTV cameras throughout the location.

The invisibility of data controllers is also manifested by silence when the citizen attempts to engage with a conversation about informational rights with the data controller. In 12 cases, we were met with complete silence. In a further 17 cases, although preliminary communications were entered into, any subsequent correspondence was again met with complete silence. In many instances, preliminary communications involved only automated replies to emails but no substantial responses thereafter. Alternatively, replies were sent to data subjects advising that a request would be addressed but no further communication was

received beyond this. In one in seven cases therefore, it would have been necessary to make a formal complaint to data protection authorities in order to further our attempts to exercise our rights.

Data controllers were able to remain 'out of sight' in other ways too, even when engaging in dialogue with data subjects. A general sense of anonymity pervaded many of the interactions with data controllers which often led to dialogues which were very much one-way and did not invite the data subject to make follow up enquiries. In many cases, correspondences were not signed by an individual but rather with a company or department name. Contact details for further queries were also absent, meaning that any attempts to submit follow up questions or clarify aspects of the disclosure were restricted as the data controller sought to ensure that the conversation was over. Similarly, data subjects often received responses from different officers every time they attempted to contact an organisation about the progress of their request. This was particularly true when dealing with large multinational corporations as in the examples of requests sent to Amazon, particularly those sent from Spain and Germany. The result of these staggered and fractured interactions was that it was necessary to re-state the nature of the enquiry every time a new correspondence was sent, lengthening the time in which a request is processed as well as adding to the frustration of the data subject in his/her attempt to gain access to personal data. These strategies and procedures all created a sense of anonymity amongst data controllers, ensuring that they remain sufficiently out of sight to discourage lengthy and in-depth dialogue and instead encourage data subjects to end their enquiries at the first instance of receiving any sort of data disclosure, whether this is complete or otherwise. In contrast, in cases which showed facilitative practices, correspondences were not only signed by a named individual but the same individual identified him/herself as the organisation's appointed Data Protection Officer and provided contact details inviting the requester to make further queries if they wished to do so.

Out of Court

Even if one is able to make visible the data controller, this does not guarantee that they will recognise a citizen's rights. As we have outlined in the cross-European legal analysis, the transposition of the Data Directive into national law has led to there being considerable interpretational latitude surrounding the scope of rights. This interpretational latitude leads to considerable uncertainty as to whether access rights will be granted. Indeed, in what would appear to citizens as being almost identical cases, the response will be completely different from one data controller to another. Thus in Hungary, in two administrative public sector buildings who operated CCTV systems, access to this footage was denied in one and in the other it was granted. Similarly, requests may be denied from the same institution when requests emanate from different countries. This was the case in requests made to Europol. The Austrian request was accepted but the Spanish request was rejected based on exemptions of national security.

Since the law contains many exemptions which limit data controllers' obligations to grant citizens their access rights, data controllers or their representatives can argue that they have exemption, effectively ruling the data subject's request out of court. It is unlikely that many citizens have the expertise to challenge the authoritative rulings of data controllers. For instance, citizens are told that:

- *'Only the police may have access to CCTV footage'*
- *'You don't have a right to see the data but only a list of what data is held about you'*
- *'You cannot view the footage because it would infringe the privacy of others'*

- *'As you are not a customer, you do not fulfil the category of 'personal' according to data protection law'*
- *'It would be illegal to share such data with a citizen'*
- *'We would never disclose such data'*

All these claims are contestable. However, for a citizen to do so, they would require extensive legal knowledge. It is worth illustrating this process in some detail in some specific contexts – CCTV in a bank (UK), CCTV in a department store (Luxembourg) and, on a more general basis, the regulation of CCTV in other EU Member States.

> ***CCTV in a bank (UK):*** We attempted to obtain CCTV footage from a bank. We rang the telephone number provided on the CCTV signage displayed in the bank to enquire about how to submit a subject access request. We were told categorically that the footage was usually only disclosed to the police. When we challenged this, we were eventually told that we could go to the branch in question to review the footage. We thus returned to the bank and asked to view the footage. The cashier clerk consulted the manager and returned stating that *'there is no way anyone would ever be allowed to see the footage'.* We asked why this was so and we told that *'this is the bank's policy'*. No further advice was offered. We then wrote a lengthy complaint to the bank, asserting that they were obliged under British law to recognise our request. Three weeks later, the management team contacted us on the telephone and invited us to the bank to confirm our identity. We attended this meeting and were promised that the data would be disclosed to us shortly thereafter. However, before this could happen, we received a further letter explaining that the footage could not be disclosed since other parties appeared in shot and disclosure of the data would infringe their privacy rights. We attended the bank again some weeks later in an attempt to get captured on film with no other customers present, after which we submitted a new request. Once more, we were advised that third parties appeared in the footage (much to our surprise) and that disclosure of the footage was not possible. Having seemingly exhausted communications with the bank, we submitted an official complaint to our national DPA. Many weeks later, the DPA contacted us to advise that our complaint had been upheld and that the bank would forward the relevant footage to us shortly. This arrived a few days later.

There are three notable issues raised by this example. Firstly, the data subject was required to draw upon national data protection legislation and know how certain provisions had been interpreted particularly relating to issues of third party privacy infringements. Secondly, to get the claim in this case ruled back in court required both time and administrative burden. The modes of interaction ranged from visiting the site in person as well as contacting the organisation by telephone, email and postal mail. The entire process took over six months from the first enquiry to the eventual disclosure of the data. Thirdly, the data subject was told on three separate occasions and for three different reasons that the data would not be disclosed. The upshot of these categorical denials is that the data subject must be combative and distrustful of the advice given by data controllers. This requires confidence and the willingness to enter into conflictual interactions with data controllers and their representatives.

In Luxembourg, a request made to a national supermarket for CCTV footage was denied using a range of arguments which attempted to rely on the relevant national legal regulations on CCTV. The case escalated to a complaint to the national DPA who comprehensively ruled in favour of the data subject. They judgement is summarised below:

CCTV in a department store (Luxembourg): The Luxembourg DPA's decision found that the viewing of the recordings of the CCTV surveillance is not exclusively reserved for the security, administrative and superior authority but also for *'every data subject who wants to execute his right of access to data in concern (stored footage on which the data subject is identifiable) […] upon request'.*

If other data subjects are part of the footage, the data controller has to make sure to blur the images or make them unidentifiable before the data subject can view the footage. In general with CCTV footage, it is however not always necessary to provide a copy of the footage to the data subject in concern.

In Luxembourg, the assumption by the data controller that only if particular events happen, the footage may be stored for longer – for eventual investigations – is not correct. If the data subject makes a request, the data controller has to ensure that the concerned footage is saved until the right of access has been executed, in order to prevent the automatic deletion of the footage after a certain amount of time – in this case one month (for some cameras five and eight days).

The presence of other data subjects on the CCTV footage must not represent a reason to limit or deny the right of access. Furthermore, the proof of a legitimate interest is not to be asked to the data subject, but to his beneficiaries exercising his right of access.

The response of the DPA in this case demonstrates the ways in which the data controller had erroneously invoked numerous legal provisions in an attempt to restrict the data subject's access request. Not only does this therefore highlight an instance of a data controller providing the requester with incorrect advice, it also emphasises the importance of DPAs in clarifying inaccurate legalistic interpretations and enabling data subjects to exercise their rights.

Reliance upon incorrect legislative provisions to deny access was a recurring practice in other contexts across Europe, particularly in the case of requests made for CCTV footage. In Belgium, there existed a clear tendency for citizens to be denied access to CCTV footage on erroneous grounds. This is because data controllers wrongly inferred that because they have a legal right to disclose CCTV footage to the police, this is an exclusive right and it trumps citizens' access rights. In Hungary, access to CCTV in the public transport system was in the course of the correspondence denied for three different reasons, two of which appeared to confuse and conflate the national legislation concerning transport and data protection regulations. In Germany, although data controllers were correct in explaining to the data subject that they were not obliged to disclose CCTV footage, the legal exemptions relied upon to do so were incorrect.

In a number of cases therefore, data subjects are unable to exercise their rights because data controllers respond by invoking incorrect or inaccurate legal regulations which seek to restrict their disclosure obligations. The direct result of such instances is that citizens must be armed with a combination of sufficient legal knowledge, data protection awareness and the confidence to challenge such assertions that their requests are somehow legally illegitimate. Quite how many requests are abandoned by data subjects in the face of such denial strategies is incalculable but it was evident in the course of this research that being ruled 'out of court' by data controllers is a frequent occurrence.

Out of Time

The dimension of time is used in several ways to restrict or deny citizens' requests. Two of the most prominent ways in which this is done are: firstly, data controllers claim that requests have been received after data is erased and are thus 'out of time' and; secondly, on a broader level, data controllers employ extensive delaying tactics which may be aimed at discouraging citizens' attempts to access their data with a view to abandoning requests altogether.

In the case of CCTV, data controllers frequently relied on the fact that the footage had been erased before it could be disclosed to the data subject. The practice of data deletion, particularly in the context of CCTV footage, is a positive one in principle. However, it became apparent during the course of sending requests to CCTV operators that the deletion of footage was at times used to deliberately deny access to citizens.

In most countries, requests must be made in writing and often to a postal address. Data controllers then have several weeks within which they must respond to the request. These processes inevitably take time and it is during this time that footage is likely to have been erased. This was the case during a number of requests sent in the UK including one case in which only part of the footage could be disclosed since some of it had been erased before the request had reached the data controller. This was despite the data controller's best efforts to retrieve the footage and his sincere apologies for the incomplete disclosure.

In Spain and Hungary researchers used a recorded mailing system when submitting their requests which irrefutably demonstrated that data controllers received requests prior to the stated deletion date. As such, data controllers effectively utilised the data deletion procedure to deny citizens' requests and delayed their responses so that data was no longer available.

Even when requests were submitted via email which guaranteed instantaneous delivery, data controllers replied *after* the deletion period claiming that the data had been erased and was therefore unavailable for disclosure. This was true also in Austria, where all but one of the data controllers approached responded by advising that the footage had been deleted prior to receiving the access request because the standard data retention period for CCTV footage is 48 hours (the other data controller approached failed to respond at all to the request).

Time was also used as a delaying tactic in numerous cases throughout the research. Since data controllers are (theoretically) bound by legal response times, the delay in responding to request was not only a restrictive practice but an unlawful one too. In Italy, for instance, only one out of 18 requests submitted received a response from the data controller within the legal timeline. In Spain meanwhile, well over half of the responses from data controllers arrived beyond the legal time limit.

While such delayed response times may be viewed as bureaucratically incompetent but not an act of bad faith per se, the length of time data subjects had to wait before receiving an adequate response from some data controllers represented plainly restrictive practices and procedures. In the UK, a request made to Amazon took five months to result in the disclosure of personal data. This time period included three months during which no response whatsoever was received (necessitating a follow up enquiry to be submitted). Similarly, a request for CCTV footage from a bank took over six months to be resolved. In Norway meanwhile, a request for records held by the local municipality took over four months to be resolved while the Spanish request to Amazon took over two months before receiving an adequate response. Finally, in Luxembourg, a request for vehicle licensing records took almost three months to elicit any sort of response from the data controller and even this reply

was inadequate, forcing the data subject to submit a formal complaint to the national DPA.

Most of these examples of course relate only to cases in which a successful outcome was reached. In a large proportion of cases, requests remained unfulfilled during the time span of the research which encompassed approximately nine months from the beginning to the end of the empirical phase of submitting access requests.

Finally, in many cases, our first attempts at contacting the data controller were completely ignored and only on the second attempt did our requests elicit a response. Although this is not conclusive proof, the volume of instances in which this occurred strongly suggests that the initial non-response is strategic rather than the result of poor administrative processes. As such, the dimension of time is utilised once again to delay and thereby restrict data subjects' requests, perhaps in the hope that if no answer is received to a first enquiry, the passage of time will lead the requester to abandon the query. Although it is highly problematic to measure the impact of such practices upon data subjects' attempts to make access requests, it is inevitable that a section of requests submitted by citizens are indeed discontinued as a result of not receiving any response to a request and the long delays experienced in the course of attempting to exercise one's access rights.

Out of Order

Even if citizens have rendered the data controller visible and managed to get their requests back 'in court', they may then encounter a series of administrative and bureaucratic obstacles which delay, restrict and ultimately deny their requests.

There are two dimensions to a request being 'out of order'. The first is that the data controller deems the data subject's request out of order. The second that the administrative processes followed by the data controller are so out of order that they effectively discourage and even in some cases deny citizens the chance to exercise their rights. A multitude of organisational and administrative deficiencies were evidenced during the research, including:

- Missing pages from disclosed documents and incomplete sentences.
- Letters apparently not being received by data controllers despite data subjects obtaining proof of delivery.
- Responses from data controller not being received by data subjects despite assertions from data controllers that they had been sent.
- Access requests misunderstood to be complaints or requests for cancellation and/or erasure of data.
- Outdated information provided by data controllers (including details on CCTV signage).
- Mail correspondence being sent to the wrong address.
- Online submission forms restricting the amount of text data subjects can enter.
- Telephone numbers unanswered or lines being dead.
- Being advised that the request cannot be fulfilled because the company does not have the manpower to do so.
- Data controllers citing law which is not yet or no longer in force.

These administrative failures occurred time and again during the research. At best, these instances slowed the access request process considerably and required the data subject to pro-actively take steps to restore lines of communication. At worst, even after prolonged attempts

to elicit an adequate response from data controllers, we still failed. It is worth mentioning some specific examples here:

> ***Local Municipality (Italy):*** We made a request to access our data from the local municipality. The data controller's details were located online. Fifteen days later, we received a phone call from the Office for Relations with the Public, acknowledging our request and explaining that they would send us a letter. The person we spoke to emphasized that they had never dealt with such a request and that our documents were ready for us to check. The respondent sounded anxious and asked whether we were looking for a specific document. We received a timely response which enclosed basic information which was, however, very generic ("*the demographic office holds data on you, as it holds data on every resident*"). The organization failed to disclose any specific information on data sharing with third parties and only partly disclosed information on automated decision-making. Moreover, we were asked to go, in person, to the Office for Relations with the Public.
>
> We went to the Office and we met the person that we had spoken to over the phone who made us sign a document declaring that we had submitted the data access request. This person also showed us a folder with our name on it and reiterated that no one had ever submitted such a request. Clearly, the data controller representative was not trained to process data access requests and had no previous experience of doing so. We sent a second letter asking for clarification as far as data sharing and automated decision-making are concerned. Again we received a phone call, two weeks later, from someone we had never spoken to before. She asked for more time in order to respond properly to our requests. Since then, we have not heard from the municipality and therefore made a complaint to the DPA but this was dismissed due to its informal nature[89].

The access request process therefore broke down due to apparent bureaucratic failure. The data subject spoke to different people when contacting the relevant office and each officer was evidently unsure how to process our request, leading to incomplete responses and severe delays. In the end, communication was cut off altogether which meant we never received an adequate answer to our enquiries.

> ***Mobile Phone Carrier (Austria):*** Since we couldn't find an e-mail address on the company's official website, we decided to call the company and ask where to send our request. Calling the company costs € 1.09/minute. The first person on the other end of the line had no clue what we were talking about, had never heard the expressions "Datenschutz (data protection)" or "Auskunftsbegehren (subject access request)". He seemed to be overstrained by our request and had to ask another person. While he was asking, we were placed on hold. When he was back, he asked for our name to pass us on to the next level, then he stopped speaking - nothing was happening and we were still waiting. After a minute, we were switched to the waiting loop. Then another person was on the line. He said he had heard our request would be about data protection. He told us that he could not help with this request but was not offering to pass us on to someone who might know something about access requests. We asked to be transferred to someone more but he refused and told us to use a form on the company's website to submit our request. We asked for an e-mail or postal address to which we could send a request but he refused to give us any address. In the

[89] See the Italian country report at Appendix 1 for a further explanation of why the complaints were dismissed by the national DPA.

background it sounded like the whole call centre was listening to this conversation. He repeatedly advised us to use a form on the German website which is used for complaints. We tried to explain that we live in Austria and that we didn't want to complain, we just wanted to be informed about the data that is stored about us and that we have a right to get this information. He told us that the form for complaints is probably also available on the Austrian website and that we should use this one for our request. The call ended after six minutes.

We proceeded to search for the form on the website. After we had found it, we entered our request although the categories we had to fill were not useful for a subject access request and the text on this site explicitly stated that the form is only for complaints and questions regarding the operating system can be directly sent to the organisation's parent company. Since the person on the phone recommended especially this form we decided to use it anyway. After sending the request, we got an immediate generic reply confirming that customer support will deal with our complaint. Moreover, the reply explained that if we don't have a complaint, we should use the contact options listed in the support section of the website.

The administrative procedure in this case was disastrous. It was obvious that the company had no formal process in place to accept and process access request, to the extent that one of the respondents on the telephone had never even heard such terminology. Data subjects were flatly denied information on a possible contact address for the data controller and ultimately pointed to an online form which was not helpful or conducive to submitting an access request.

Amazon (Spain): We sent our request to the postal address in Luxembourg provided on the organisation's official website. Some weeks after submitting our request, a representative from the company called us. We were advised that the purpose of the call *"was just to confirm that it was you and not someone else requesting access to the data".* Two days later, we simultaneously received two separate envelopes: one contained information about their privacy policy and two passwords that were supposed to unlock a CD-ROM containing the disclosure of personal data (which came in a separate envelope). The letter was signed by the legal department, but no name was provided. However, despite these extensive security arrangements of double passwords, the passwords themselves didn't work and we couldn't unlock the document containing the personal data disclosure.

We therefore contacted the data controller once more to seek a solution. They responded by stating that they needed more information to provide us with a solution. Quite why this was the case was unclear since we had already submitted a request and all we needed now were new passwords. Nevertheless, we called them and underwent many interactions with different officers during which every new e-mail was from a different person. This continued until we requested that we be assigned a single person to pursue our case. Finally we were assigned with a specific officer who became the only contact point. Several weeks later, we finally received a new CD-ROM with new passwords which successfully unlocked the content. The disclosure of personal data was extensive and we considered this to be complete.

This case was a clear example of facilitative policy undermined by totally inefficient administrative practices and poor time keeping. While all representatives were respectful throughout our interactions, the process was lengthy and at times confusing as well as

punctuated by the technical failure of the passwords which added further delay to obtaining a successful resolution to our request.

Another way that requests were deemed 'out of order' was to refuse to even acknowledge or deal with them in their original tongue. A request in French, Norwegian or German, for instance, to many of the multinational corporations in the sample, was simply deemed out of order, and either responded to in English or frequently, not responded to at all. During the course of submitting their access requests, researchers always formulated their first requests in their native languages in order to determine whether data controllers chose to respond in the same language (thus showing facilitative practices) or failed to do so (thus restricting data subjects ability to exercise their rights). This procedural inflexibility reflects further administrative failures in the ways that organisations are designed to respond to citizens' requests and demonstrate a failure to facilitate the range of potential consumers who may engage with data controllers' services. For instance, a Norwegian user of Facebook's Norwegian interface may reasonably expect that an access request written in Norwegian receives a response from the data controller in this language. This was not the case in this research as Facebook simply responded in English using an automated reply system. Indeed, this was the case in all Norwegian requests sent to multinational organisations who all responded to requests in English without checking that this would be suitable (or understandable) for the requester. This was also true of a Hungarian request to Microsoft which elicited a response which stated that "*At this time, I would like to let you know that we are only able to respond using the English language. Please provide your information in English, so that we can provide you the required support option*." The same occurred in response to Italian and French (from Luxembourg) requests to Twitter. In some cases, this problem arose even before an access request was submitted since companies' privacy policies were also only available in English despite the organisation operating in a number of countries. It should also be noted here that this linguistic imperialism was not restricted only to the use of English. A request written in French sent from Luxembourg to a department store whose headquarters are based in Germany resulted in a response written in German. These linguistic practices showed no attempt to respond flexibly to data subjects' requests despite the fact that many citizens will not necessarily speak the language chosen by the data controller. Oftentimes, it was simply assumed that a requester could speak English and the responses were written in English with no attempt to check that this was suitable for the data subject. These are clearly restrictive practices which further illustrate the impact of inflexible and rigid bureaucratic and administrative practices upon the ability of data subjects to exercise their rights in a facilitative and unambiguous manner.

This succession of administrative and bureaucratic failures places the burden upon the data subject to find a resolution if they wish to achieve a successful outcome. In many cases, the inadequate procedures encountered were the result of simply not having any sort of formal process in place to recognise what an access request is and escalate it suitably to a responsible officer/department. This absence of formal processes goes hand in hand with an endemic lack of knowledge and awareness amongst members of staff regarding data protection and privacy issues. As a consequence, this led to requests being incorrectly treated as complaints or incurring significant delays as data controller representatives pondered how to respond to such requests, often deciding not to respond at all.

Out of Tune

Rather than facilitating subjects' rights under data protection law, a number of data controllers insisted during the research that by following their own procedures, accessing

what they classed as citizens' personal data would satisfy the request. But in fact, what is offered is incomplete disclosure of partial data and no attempt to address issues of data sharing or automated processing in an individuals' case other than that which could be found in organisations' privacy policies. In essence, data controllers argue that data subjects' requests were out of tune with their policies and procedures and needed to be re-modulated so that both data subject and data controller were singing to the same tune. Such practices should not be mistaken as being attempts to facilitate requests in a unified and efficient way. Rather, they reflect a tacit refusal amongst data controllers to accept requests in any format other than the mode pre-determined by the organisation, but not compliant with European or national law. These are also procedures which block any attempt to obtain individualised answers about how organisations process one's personal data since all responses to requests are pre-formed, automated and are not designed to accept specific queries.

Requests made to Facebook followed this pattern and the access request made from Norway to the organisation reflects the experiences of all requests sent to Facebook in this research:

> ***Facebook (Norway):*** The initial data access request was sent via postal mail and was made in Norwegian. The request was sent to the company's Ireland headquarters address provided on their website in the 'Data Use Policy' section which was easy to locate. The reply from the data controller was received by email exactly one month after the initial request was sent (just one day after the 30 days time provided by law). In the response, the data controller stated that there are several ways to access your data from Facebook, either by simply logging in to your account or by using an online tool provided by Facebook. The online tool permits you to download an offline copy of the data linked to the account. A link to this tool was given by the data controller, along with a step-by-step guide on how to use it. We followed these instructions and followed the provided link to the online download tool. A few days later, Facebook sent a second automatic email, announcing that the data of the user were available for download. The data subject followed the link included in the message and downloaded the data. The download operation was rather smooth and the .htm format of the files received allows for simple navigation of the data. However, while the online tool permits users to download data that would not be available via merely logging in to one's account, some kinds of data are still missing: for example the pictures uploaded by other users where the data subject has been 'tagged' and further metadata concerning the use of personal data by third parties. Finally, it is not very clear how the access rights of a data subject that has never been a user of Facebook (but whose data are stored and processed by Facebook) can be enforced.

This experience highlights several interesting aspects of the practice of handling data access requests. First, the messages from Facebook were signed by the *"Facebook Data Access Request Team",* which highlights how the organisation has created an office to handle this kind of request. This apparent commitment to developing a procedure to receive such requests seems to be confirmed by the existence of a standard procedure and an online tool. However, this practice is also fundamentally limited. The data disclosed using the online tool does not appear complete and furthermore, no response was given on questions that 'did not fit' the procedure: i.e.: queries concerning third party data sharing and automated decision making. Therefore, the use of a standard procedure has a strong channelling and morphing effect on the way in which data access rights may be enforced. Finally, it should be noted that the Facebook Data Access Request Team used English in their first response, despite that fact that the data access request was formulated in Norwegian.

It is important to note at this point that extensive work completed elsewhere has found that Facebook's self-download tool is inadequate in disclosing users' personal data[90]. In the UK, following a similar chronology of events as those described above, a complaint was made to the Office of the Data Protection Commissioner (ODPC) in Ireland since Facebook flatly refused to accept an access request other than by pointing the data subject in the direction of the organisation's online download tool. Unfortunately, the response received from the ODPC did not enable the request to proceed, leaving us with no other avenue other than submit a complaint to the European Commission which is currently pending.

Similar problematic practices were experienced when submitting requests to Google. As with Facebook, Google utilise a pre-determined procedure in responding to requests which directs data subjects to use online tools such as Google Dashboard and Google Takeout all the while assuring data subjects that all the data held about them by Google can be accessed using these tools. Several issues arise here: firstly, as with Facebook, the automated referral to these online tools does not address requests on a specific basis and indeed ignores questions on how one's personal data is processed and shared. Attempts to obtain this kind of information about personal data are therefore blocked by the organisation's procedures.

Secondly, it is extremely difficult for the individual data subject to know whether the information contained in the online tools are indeed all the data that is held about them by the data controller. This is the problem of 'unknowables' which pervades all requests made to organisations which have the potential to collect large amounts of data about data subjects. With the absence of certainty that some data has not been disclosed, it is hard for data subjects to challenge the assertions of organisations like Google, Facebook and other multinational corporation who collect meta-data when they claim that no other data is held about them beyond what is available via the users' own accounts.

In the UK for instance, following a complaint to the Irish DPA regarding what was deemed to be incomplete disclosure of personal data by Facebook, the data subject was advised to inform the DPA of what he believed was still being withheld by Facebook before the DPA could take any remedial action. But herein lies the problem of unknowables – data subjects have only a suspicion (strong or otherwise) that more data than has been disclosed is held by some data controllers. Without concrete evidence of this however, DPAs appear reluctant to take action against data controllers, leaving data subjects with the impression that they requests for personal data will forever remain unfulfilled.

Aside from those instances involving multinational corporations, the problem of unknowables arose in other contexts and in different ways including pre-empting the submission of a request altogether, as in the following case:

> ***Police records (Belgium):*** We introduced a formal access request to the Belgian DPA asking for access to police records and any files processed by the police about us. The Privacy Commission replied to this request promptly, within a few days after our enquiry. Our access request was considered inadmissible and was rejected. The DPA pointed out that the access request did not contain all information requested by law in order to be considered as valid and legitimate. In particular, it did not mention details about the police authority or the specific police service which processed our data.

[90] See for example www.Europe-v-Facebook.org which has claimed that around only 29% of data is disclosed when using Facebook's download tool and is drawn from less than half of the categories of data held about users by Facebook.

> Moreover, the DPA highlighted that the request did not contain any reference to the data to which we sought access such as their nature, origin and the circumstances in which the police obtained them.
>
> This experience shows that the access to personal data processed by the police is allowed in specific circumstances only, when data subjects have a real and concrete concern linked to their previous criminal record. Accordingly, Belgian legislation does not allow Belgian citizens to know if the police might be processing personal data about them. In other words, data subjects cannot submit 'general' or 'exploratory' request but rather specific requests concerning a particular issue. In this case, national legislation creates a sort of fictitious presumption that the data subject has a criminal record, substantiated by concrete evidence. If so, the concerned person has to prove that the police processes or processed data about him/her.

Hence, the Belgian legislation sets significant limitations to the right to have access to personal data if data are stored in police files or police records. In this case, the provisions established under the Belgian law make the scope of access rights very vague and unclear. Access rights are basically meant to allow data subjects to take control of their data by finding out what is held about them, should any data indeed be held about them. If legislation requires data subjects to know what is held about them and by whom *before* they can even enquire about this, then the right of access loses somehow its *raison d'être* and becomes a tautology.

Once more, data subjects are asked to know the unknowable in order to exercise their informational rights and organisations' rigid access request submission criteria limit data subjects' ability to find out about the data held about them. Moreover, as well as being out of tune, the above example can be deemed as demonstrating the request as being out of order since the very nature of the access request process inherently demands that data subjects know what they cannot know. As such, the process itself is broken and is thus out of order.

Out of Mind

In many cases, citizens' subject access requests were dealt with administrative efficiency and bureaucratic neutrality and in some even with a kindness and helpfulness that was indicative of data controllers' willingness to go beyond the minimum legal standard for compliance and achieve high levels of satisfaction on behalf of data subjects. However, in a significant minority of cases, data subjects were made to feel that they were somehow 'mad' – or 'out of their minds' – for even wanting to know the information requested. Perhaps worse still, they were seen as having nefarious motivations for submitting requests. Of course, if someone is treated with distrust and disrespect, this may discourage them from continuing with their request. In Italy, for instance, a request for CCTV from a department store was met with clear suspicion and the data subjects were asked numerous times why they wished to make such a request before finally receiving reluctantly-provided information on the data controller's contact details. A similar scenario was experienced when attempting to submit a request for CCTV footage from an open street system as the data subjects contacted the police in person and were treated suspiciously and had to speak to three different officers before finally receiving contact details for the data controller.

In Austria meanwhile, during a request for CCTV footage in a transport setting, the data subject was told that although the footage had been erased in any case, disclosure of such footage may have been a very costly and lengthy exercise, indicating to the data subject that

such requests were not welcome. In Spain, a request for CCTV footage from a transport setting led to unhelpful responses from the data controller, creating a sense amongst the data subject that the request had been useless and time-consuming for the data controller. While a request for bank records in Luxembourg resulted in very comprehensive and lengthy disclosure of personal data, the correspondence from the data controller also repeatedly explained to the data subject that all personal data held by the organisation had been provided to them by the data subject himself in the first place. Therefore, the data subject ought to know what data was held about him without resorting to the submission of an access request. The use of such arguments suggests that organisations do not welcome access requests and perceive them as a nuisance rather than an opportunity to enable the data subject to manage his personal data more effectively.

In Hungary, several responses to access requests directly led to the data subjects being made to feel that their requests were not only an irritant but almost an abuse of process. When requesting access to CCTV footage captured in a public place, the data subject initially received only a partial response, necessitating her to telephone the organisation for further information. Having done so, the data controller representative became confused and responded, somewhat angrily, *"then what's your problem? I really don't understand your point".* Meanwhile, whilst seeking to obtain CCTV from a department store, the requester received a telephone call from the Head of Security who treated the request as suspicious leading the data subject to feel as though the purpose of the phone call was to determine whether the request itself was legitimate or nefarious. Finally, the data subject received a particularly surprising response in the course of requesting access to mobile telephone records. Following extensive interactions with a legal officer acting on behalf of the data controller, the data subject was informed that her request had been formulated in such a broad manner that it represented a request made in bad faith and in turn the data subject was made to feel that she was abusing her democratic right of access.

These experiences are of course subjective but it is clear that in some cases during the research, data subjects were treated in manner which belied an attitude of annoyance and dismissal on behalf of data controllers.

The Privacy Paradox

During the course of the research, an intriguing phenomenon arose which may be termed as the privacy paradox. As part of submitting access requests, data subjects came to feel that they were required to reveal more data about themselves to data controllers than that which was already held about them. Therefore, data controllers in fact obtained more personal data about a data subject when responding to an access request. As a result, in the course of exercising informational rights, the citizen is in fact required to give away even more of his/her personal data. In the UK for example, as part of a request for ANPR data, the template form the requester had to complete asked for details on his height. It was compulsory to include this information even though it seemed to the data subject that such level of detail was not at all necessary to process his request. In Italy meanwhile, the data subject was advised (and later actually shown) that a folder had been created as a result of her submission of a subject access request. This folder was kept in the data controller's office and contained information on the interactions conducted between the data subject and the data controller since the request process began.

In submitting an access request, the data subject appears to invite the spot light upon him/herself and this was reflected in the experiences of data subjects in this research. In

Luxembourg, the data subject tracked (using Google Analytics) a sharp increase in visits to his online academic profile during the period in which he submitted access requests. Indeed, the visits to his profile emanated from IP addresses based in Luxembourg suggesting that data controllers sought to check who the requester was. Meanwhile, in Hungary, one data controller representative actually advised the data subject that he had 'googled' her before responding to the request.

Another dimension of this so-called privacy paradox is the data and personal vulnerability experienced during the process of exercising one's access rights. Personal data was often sent to data subjects in the post using no security measures to ensure the safety of delivery. Moreover, data subjects were often advised by data controllers that responses had been sent but must have been lost in transit. In one case, personal data was sent to an old address despite the fact that the data subject's new address was known by the organisation. Such lax and carefree practices perhaps represent the low level of importance assigned to the security of documents containing personal data, rendering this personal data potentially vulnerable. Meanwhile, on two occasions in Spain, personal data was actually delivered in person which left the data subjects feeling somewhat exposed since an officer had visited their home address. On one such occasion, the data itself was in fact delivered without an envelope meaning that the delivery person could have viewed this data (or indeed anyone else in the course of the data leaving the data controller and arriving with the data subject).

This intriguing by-product of submitting an access request therefore demonstrates the potential pitfalls data subjects may experience in the course of exercising their democratic rights. Despite the right of access being designed to enable citizens to take control and inform themselves about how and what personal data is collected and stored about them, one consequence of such action appears to be additional exposure to data controllers' gaze as well as the potential vulnerability of one's personal data.

Legal Perspectives

The spirit of the law and the letter of the law

The EU Directive 95/46/EC was designed in part to empower citizens, via the exercise of their ARCO rights, to gain control over the ways in which their data is processed by data controllers. However, during the course of this research, it has become clear that the implementation of the Directive in national legislation has often led to the subversion of the Directive's original intentions. While exemption categories are to be expected in such legislative provisions, some Member States appear to have specifically formulated their national laws to restrict the citizens' ability to exercise their access rights.

In the research, this was most keenly felt in Belgium in the context of accessing CCTV footage. Belgian legislation states that requests for CCTV footage should be "dûment motivée"[91], or in other words duly motivated. In the absence of clarification within the relevant legislative provision, the Belgian DPA outlined to the data subject that such motivations would include the occurrence of an actual crime or the suspicion that a crime had occured crime. In the absence of such circumstances, requests will be denied and indeed this was the case in the research. Similarly in Luxembourg, national legislation states that *'a request is subject to proof of legitimate interest'*[92] and some data controllers tried

[91] Article 12 of *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007

[92] Article 28 of Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (2007), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A – N°91: 1835-1854.

(unsuccessfully) to deny the data subject's request based on this provision during the research. These legislative provisions demand that a citizen demonstrate a justified reason for submitting access requests and follow other trends of national implementation of European law taking a restrictive approach to citizens' informational rights[93]. In these contexts, the original intentions of the law are systematically undermined by national legislatures who choose to narrowly interpret citizens' rights to exercise their informational, and specifically access, rights.

Cross-European Consistency

The different experiences of data subjects from one country to another during this research are symptomatic of the lack of consistency across EU Member States in the context of practices and procedures in data protection (and specifically access) rights.

Data subjects living in Europe and engaging with multinational corporations face considerable uncertainties insofar as how their requests will be processed by data controllers and possible avenues for recourse, should a dispute arise in the process of exercising their informational rights. For instance, some data subjects can expect to submit an access request for free (Belgium, Luxembourg, Germany and Spain) while others are expected to pay a fixed administrative fee to exercise exactly the same right (for instance £10 in the UK). Once a request is submitted, some data subjects can expect data controllers to (theoretically) abide to a 15 day response time (Italy) while others may have to wait up to 56 days (Austria) for a response. Others still will have no such measures since their national legislation places no fixed timeframe for data controllers to respond to requests (Luxembourg).

The varying obligations for the appointment of DPOs also mean that some data subjects can expect, as this research has found, that their access requests will be treated with considerably more expertise in some countries than in others. And in cases where disputes arise and matters are escalated to complaints to national DPAs, data subjects once again face starkly contrasting practices depending on whether they are submitting their complaints to one DPA or another. While some DPAs charge a fee in order to allow data subjects to bring substantial complaints for consideration (Italy), most others allow complaints to be submitted free of charge. However, the absence of consistency and certainty goes beyond merely administrative and bureaucratic practices here as DPAs in different Member States show radically differing levels of staffing and other resources in order to promote informational rights and act effectively as independent dispute resolution authorities.

The issue of consistency therefore goes far beyond merely standardising procedural matters. However, doing so would undoubtedly represent a good starting point which would help to eliminate the uncertainty faced by data subjects when they seek to exercise their informational rights.

The Role of DPAs

Interactions with Data Protection Authorities throughout the course of the research inevitably differed from one country to another. This is to be expected given not only the context-specific circumstances of individual cases but also the (at times) vastly different resources available to DPAs in different countries[94]. Nevertheless, Table 1 below provides a broad overview of the results (or lack therefore) of making complaints to DPAs.

[93] See for example the development of case law in the UK which has significantly narrowed the definitions of 'personal data' and 'relevant filing system'.

[94] See the comparative analysis of legal and administrative frameworks in Europe above for further information.

Table 8: DPA complaints submitted and status of complaints at time of publishing

Countries	**Complaints Submitted**	**Complaints resolved**[95]	**Complaints outstanding**[96]
Austria	2	0	2
Belgium	6	4	2
Germany	0	0	0
Hungary	1	0	1
Italy	5	2	3
Luxembourg	6	2	4

[95] Either by direct order/enforcement by the DPA or by the data controller responding after a complaint has been made to the DPA.
[96] Outstanding at time of publishing

Norway	0	0	0
Slovakia	1	0	1
Spain	14	4[97]	10[98]
UK	4	4	0
Total	39 (100%)	16 (41%)	23 (59%)

The majority of complaints remain unresolved (59%) at the time of writing, but this should not be taken to tell the whole story and the results above should be considered in their national contexts. In the UK for instance, every complaint submitted had been successfully resolved while in Belgium, four of the six complaints were also completed. In contrast however, in Austria, Hungary and Slovakia, none of the complaints submitted were successfully resolved and in Italy, Luxembourg and Spain, the majority of complaints were still outstanding despite some cases being settled. Given that most of these complaints had been submitted several months ago, the fact that they remain outstanding at the time of writing gives some indication of the length of time data subjects may need to wait before obtaining a response from DPAs.

The conduct of the Italian DPA is particularly noteworthy here. In Italy, data subjects are able to submit either formal or informal complaints. Formal complaints cost 150 Euros to submit and may therefore be described as the preserve of only those individuals wealthy enough to pay such high costs. Informal complaints are free and the data subjects in this research used this means to submit their complaints in five cases:

> ***Complaints to the DPA (Italy):*** Having deemed five cases to be sufficiently non-compliant to warrant a complaint to the DPA, we made a 'collective' complaint to the DPA which was submitted on 16/12/13. At the end of January, we received a response from the DPA claiming that the authority considers only *"circumstantial claims"* which lead to formal investigations. Indeed, we were informed that this holds true for all the complaints we made, except for the one made regarding Google (which was dealt with separately and is still outstanding at the time of writing). However, the response of the DPA addressed only three of our five complaints. As such, two of our complaints were not mentioned whatsoever and we have effectively received no response from the DPA on these matters.

In Italy therefore, it seems informal complaints are not enough for the DPA to intervene. This can be deemed as a restrictive practice for at least two reasons: first, circumstantial claims are expensive. The case handling fee is 150 Euro. It is therefore likely that only citizens who can afford this fee will be able to use the formal complaint mechanism which will presumably enhance their ability to exercise their democratic rights. However, as the researchers documented:

[97] One of these cases involved the US DPA resolving the complaint.
[98] One of these cases concerns the Dutch DPA's lack of response at the time of writing. The Spanish DPA had in fact responded by advising us to direct our request to the Dutch DPA. Therefore, the Spanish DPA may be seen as having completed its duty in this case but the data subject's complaint still remains unresolved.

> The authority did not show any interest in our numerous complaints. We received a letter mentioning our complaints and access rights but failing to 'go beyond' mere bureaucratic features (e.g. description of access rights and lists of documents to provide with the circumstantial claim). We had different expectations pertaining to communications with the Italian DPA. Given that our complaints featured a range of poor practices and behaviours from different data controllers, the general lack of interest and assistance received from the DPA was disappointing in the extreme and raises significant questions as to the fulfilment of their duties as mediators in disputes between data subjects and data controllers.

DPAs in different countries have varying levels of resources available to respond to and resolve citizens' complaints. However, while this may account for slow response times, the example of the data subjects' experiences in interacting with the Italian DPA demonstrates an example of an organisation's own administrative procedures inherently limiting citizens' ability to seek resolution from a body which is supposed to act independently and impartially.

Summary

The qualitative analysis above has shown that data controllers seek to restrict data subjects' attempts to submit access request in a wide variety of ways. Several discourse of denial are pursued in doing so, some of which can reasonably be described as the unfortunate result of poor administrative and bureaucratic purposes. However, although these processes were often complex, time consuming and difficult to navigate for data subjects, these may be viewed as incompetent but not necessarily representing bad faith on behalf of organisations. A number of the other discourses outlined above however, are undeniably undertaken with the deliberate intention of denying citizens' requests or at best severely restricting the process of exercising the right of access. This was particularly evident in the delayed responses received to some requests in order to ensure that data was erased before the data controller replied to the data subject. Elsewhere, data controllers systematically breached legal obligations by, for instance, failing to reply to requests within legal timelines but perhaps more importantly by failing to reply at all in many cases.

When citizens' exercise of rights are not being hampered and restricted by data controllers however, they are often undermined by legal frameworks surrounding the exercise of informational rights. The implementation of European law into national legal frameworks has involved narrow interpretations of data subjects' access rights including the obligation upon some data subjects to justify their own requests by showing a legitimate motive behind their desire to exercise a democratic right. Moreover, citizens face considerable uncertainty, particularly when interacting with multinational corporations since matters are jurisdiction become blurred and it is unclear by which national legal framework data controllers and data subjects are complying.

The policy implications of these conclusions are manifold. From a legal perspective, increased consideration should be given to harmonisation at a number of levels. Moreover, data subjects should not have to justify their wish to exercise their democratic rights, in particular, their right to the protection of personal data. If data controllers perceive that an exemption category applies to an access request, it should be their responsibility to justify this. Data controllers should also make efforts to render themselves considerably more 'visible' and indeed more transparent. This can be achieved relatively simply by providing clear content to data subjects (via privacy policies) and ensuring that data controller representatives receive sufficient training to deal effectively with data protection enquiries.

DPAs may have a potentially important role to play here and they should give serious consideration to how awareness levels may be improved regarding informational rights amongst both data subjects and data controllers.

Despite the generally negative conclusions outlined above, the examples of best practices presented at the beginning of this analysis demonstrate what can and indeed is already being achieved by some data controllers. These organisations evidently prioritised transparency and accountability alongside customer/client satisfaction and show that the policy recommendations emerging from this research are eminently achievable.

Policy Implications & Recommendations

Dr Xavier L'Hoiry & Professor Clive Norris

In light of the experiences outlined above, a number of policy implications and recommendations can be outlined here. These are aimed on a practical level at both data controllers and DPAs as well as on a more theoretical level at the legal frameworks surrounding the exercise of informational rights by data subjects.

Legal

The research found that the intentions of European legislation concerning data protection and privacy are sometimes undermined by the implementation of these laws into national legislative frameworks. Through both national legislation itself or in the development of case law, citizens' ability to exercise their informational rights are oftentimes interpreted narrowly, providing data controllers with exemptions from their obligations to disclose personal data and restricting data subjects in their attempts to improve their understanding of how and what personal data is processed. Moreover, there is a fundamental absence of harmonisation of both administrative and bureaucratic processes as well as resources provided to bodies such as DPAs from one Member State to another. As a result, the following should be considered:

- The concept of 'motivated requests' in national legislation should not be used – exercising one's democratic rights should be considered as sufficient motivation.
- Data controllers should show a legitimate legal reason for denial of requests. In other words, the burden of proof should be on data controllers to show that a request should be denied rather than the burden of proof being on data subjects to legitimise their requests.
- The form and content of CCTV signage should not be left to the discretion of the operators but should be legally regulated i.e.: signage should be standardised in terms of size and the information contained within.

Data controllers

Some data controllers demonstrated high levels of facilitative practices during the research and these instances demonstrated that best practices can be achieved across different sectors and in the context of requesting different types of data. However, other data controllers frequently employed a wide range of restrictive practices, policies and procedures which, deliberately or otherwise, prevented citizens from exercising their access rights. Amongst many others, such restrictive practices included administrative and bureaucratic failures, rigid and pre-determined processes which did not encourage specific queries and perhaps worst of all, outright silence. As a result, we propose the following:

- Data controllers should make themselves as 'visible' as possible. Thus, the relevant office/department/individual to whom access requests must be sent should be easily identifiable, and a full contact address provided. This would give citizens a clear line of sight to the data controller.
- Data controllers should have a designated individual or department whose responsibility it is to deal with receiving and processing access requests. This does *not* mean that all data controllers should employ a dedicated Data Protection Officer who deals exclusively with data protection matters. Rather, this may simply be an existing member of staff with other duties and responsibilities who has received sufficient

training to enable them to process and respond to requests in a legally compliant manner.

- When disclosing to data subjects with whom their data is shared, it should not be sufficient to simply list categories of recipients. Such practices undermine data subjects' ability to exercise their informational rights. Instead, data controllers should specifically list the third parties with whom data is shared and their contact details.
- When disclosing information about automated decision making processes, data controllers should give clear and complete information about how these processes work, the logic underpinning these processes and the affect they have on the decisions made about the data subject.
- When data controllers use their online privacy policies to disclose content about their data protection and privacy practices, these policies should include a section on access rights indicating the following:
    - A statement that data subjects have the right of access
    - A reference to the relevant legislation
    - A description of how to submit an access request including an outline of what to include in a request
    - An outline of identification requirements as part of submitting an access request
    - Contact details for the individual/department who processes requests
    - Privacy policies should always outline what type of data the data controller collects, processes, for what purposes it is collected, with whom it is shared (see above) and whether it is subject to profiling (and if so, how).
- Telephone numbers given as the contact for privacy queries (i.e.: on CCTV signage) should not lead to a generic call centre. Instead, they should be directed to a member of staff with requisite expertise to answer questions on privacy. Alternatively, data controller should ensure that members of staff answering these telephone calls receive sufficient training to recognise a data protection query and escalate/pass such queries appropriately to a relevant officer/department. Ideally, this process should never involve more than two people.
- Telephone numbers for data controllers should not involve premium phone charges as this essentially represents an additional tax on citizens in exercising their democratic rights.
- Members of staff should also be sufficiently trained to either answer privacy-related question themselves or have a clear protocol to escalate such queries to a relevant management figure. Ideally, this process should involve no more than two people.
- Contact details on CCTV signage (whether postal or otherwise) should be for the data controller rather than a general contact point lacking the requisite expertise to respond to data protection queries appropriately.
- Data controllers should consider providing data subjects with templates via which to make their requests. This may ensure that requests are easily recognised and that all the required information is included in a single correspondence[99].
- The issue of language should be given serious consideration by data controllers in responding to subject access requests. Ideally, responses to access requests should be

[99] See for example the template provided by Interpol available at http://www.interpol.int/About-INTERPOL/Structure-and-governance/CCF/Access-to-INTERPOL%27s-files. This is a simple and short template but ensures that all necessary details are included in order to process the access request in a timely and efficient manner. Indeed, this proved to be the case during the research.

made in the requester's own language. However, while it may not always be possible to respond to data subjects in their own language, it should not simply be assumed that the requester can speak English.

- Data controllers should show flexibility in their processes when receiving access requests. For instance, the use of email as an acceptable format via which to submit requests should be encouraged, especially in cases when the data controllers themselves are inherently digitally-based (i.e.: social network organisations).
- Data controllers should carefully consider the manner and format in which they disclose personal data in order to ensure the intelligibility of the data. This is especially important for those data controllers who process large amounts of data held in big data sets.
- In the case of CCTV images, the rights of third parties should not be used to thwart access requests. Data controllers should be required to develop policies and proceedures to enable this[100].

Data Protection Authorities

The research revealed an endemic lack of awareness of informational rights and specifically access rights amongst both data subjects and data controllers. The absence of knowledge amongst data subjects that they have the right of request copies of their personal data meant that this right is rarely exercised and few requests are submitted to data controllers. In turn, given the scarcity of receiving such requests, many data controller representatives do not receive any sort of training on how to process and respond to such queries in a legally compliant manner. The results of this vicious circle are that data controllers frequently display inadequate practices and procedures when faced with access requests and data subjects lack of the awareness to recognise such poor practices and challenge them in order to achieve a satisfactory outcome.

When poor practices are challenged, the recourse is usually to DPAs first. However, the research also showed that in some cases, DPAs' resources (or lack thereof) are such that they are unable to process complaints in a satisfactory manner and this can therefore become a lengthy process. As a result, we propose the following:

- DPAs should prioritise the promotion of informational rights to citizens and give some consideration how training/awareness-raising could be delivered.
- DPAs should provide standard model templates for data subjects to use in order to submit an access request.
- DPAs should, in conjunction relevant stake holders such as consumer rights and labour orgnisations, promote the development and acceptance of standard templates in specific sectoral contexts.
- DPAs should provide detailed guidance to data controllers in how to respond to access requests including examples of best practice[101] and give some consideration to how specific training could be delivered[102].

[100] For instance, data controllers should make use of footage blurring technology if they possess this. If this is not available, data subjects may for instance be invited to inspect the footage even if they cannot be given a copy of it.

[101] See for example the Information Commissioner's Office (2012) 'Draft Subject Access Code of Conduct' http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/draft_subject_access_cop_for_consultation.ashx

[102] See for example the courses provided by Amberhawk in the UK – http://www.amberhawk.com/training.asp

- DPAs should also provide detailed guidance to data subject on how to exercise their rights.
- DPAs should ensure that a clear, unambiguous and affordable complaints procedure is always available to data subjects in case of data breaches.
- DPAs should have the power of audit and inspection as this would go some way to redress the asymmetry of power experienced between data subjects and data controllers.
- DPAs should proactively audit public and private sector orgnaisations web sites and other channels of communciation to see whether all relevant information is available to citizens to make a sucessful access request.

Post-script – Policy recommendations in light of the European reform

The policy implications and recommendations resulting from our research findings are made on the basis of the existing European and national legislation. The EU is currently in the process of reforming Directive 95/46/C and some comments can be made here in light of our research findings which address the substance of the proposed reforms.

First, our research has found considerable variation in how subject access rights are enacted in different Member States. The use of regulation rather than a directive would lead to greater consistency between different countries.

Second, the research demonstrated that the presence of DPOs facilitated the access request procedure for the data subject. Any proposal which seeks to diminish organisations' responsibilities to appoint DPOs will need to consider the detrimental effect that this may have on citizens' abilities to exercise their rights.

Third, our research illustrated that privacy policies often lacked the requisite depth of detail to enable data subjects to manage their data in a meaningful way. If citizens are to be empowered to exercise their rights, organisations must clearly describe their subject access procedures and policies and provide explicit protocols to submit an access request.

Fourth, the research found that data controllers were generally reluctant to disclose any information about their data sharing protocols and even when pushed, only revealed generic lists of those they shared personal data with. While this is in accordance with the current legislation, it is quite clearly inadequate as data subjects are completely unable to know with whom data is actually shared and how it is then used and continues to be processed.

Fifth, our research showed the almost complete inability of data controllers to address when and how automated decision making processes were used. As such, proposals which demand that data controllers properly address issues of automated decision making and profiling should help to alleviate this problem.

Sixth, our research showed that the obligation to justify and motivate requests acted as an unwarranted restriction on data subjects' ability to exercise their rights. This should be explicitly addressed in the proposed reforms.

Finally, as our research has clearly illustrated, in the case of transnational corporations, there is a lack of clarity as to which national legislation they are subject to and whether they are subject to European legislation at all. This would appear to be an area that legislators need to urgently address.

References

Amberhawk, 'An Analysis of Google's Privacy Policy and Related FAQs': http://www.amberhawk.com/uploads/Google_privacy_docs.pdf Accessed 19 May 2013

Amberhawk, 'Training': http://www.amberhawk.com/training.asp (last accessed 21 May 2014)

Bundesverfassungsgericht (1983) Decisions volume 65, p. 1 ff.

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, OJ 1995 L 281/31.

Europe v Facebook - http://europe-v-facebook.org/EN/en.html (last accessed 21 May 2014)

European Agency for Fundamental Rights (2014) Access to Data Protection Remedies in EU Member States, available at: http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

Hornung G. and Schnabel, C. (2009) 'Data Protection in Germany I: The population census decision and the right to informational self-determination', *Computer Law & Security Report*, 25(1): 84-88

Information Commissioner's Office (2012) 'Draft Subject Access Code of Conduct': http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/draft_subject_access_cop_for_consultation.ashx (last accessed 21 May 2014).

Interpol – 'Access to Interpol's file': http://www.interpol.int/About-INTERPOL/Structure-and-governance/CCF/Access-to-INTERPOL%27s-files (last accessed 21 May 2014).

LIBE Draft report 2012/0011 (COD) dated Dec. 17 2012 (12 PVLR 65, 1/14/13), available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf (last accessed 26 May 2014).

Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (2007), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A – N°91: 1835-1854: http://www.legilux.public.lu/leg/a/archives/2002/0091/a091.pdf (last accessed 21 May 2014).

Loi réglant l'installation et l'utilisation de caméras de surveillance, 21 March 2007, Article 12.

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

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