Chapter 9
Exercising Access Rights in Luxembourg

Roger von Laufenberg

Abstract This chapter outlines the experiences of attempting to exercise one's right of access in Luxembourg. Using rich, ethnographic examples, this chapter tests how easy or difficult it is for a data subject based in Luxembourg to obtain their personal data, firstly by locating the required information about organisations and their data controllers and secondly by submitting subject access requests to these organisations. The chapter reflects on the differences (if any) between public and private sector organisations in the process of responding to access requests as well as the role of the national Data Protection Authority in Luxembourg.

9.1 Mapping the Legal and Administrative Frameworks of Access Rights in Luxembourg

9.1.1 Introduction

In Luxembourg the 'Coordinated Text of the Law of 2nd 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 and the Law of 27th July 2007'[1] (hereinafter 'the Law of 2nd August') regulates data protection principles. The Law of 2nd August 2002 replaced the 'Act of 31st March 1979 concerning the Use of Nominal Data in Computer Processing',[2] which had been widely ignored as it was out of date in regard to modern technology. The Law of 2nd August 2002

[1] Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel modifiée par la loi du 31 juillet 2006, la loi du 22 décembre 2006, la loi du 27 juillet 2007.

While normally the legislation in Luxembourg is only provided in French, the National Commission for Data Protection provides an English and German translation of the Act. The quotes are based on the translated version of the Act.

[2] Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques.

R. von Laufenberg (✉)
VICESSE, Vienna, Austria
e-mail: roger.von.laufenberg@vicesse.eu

C. Norris et al. (eds.), *The Unaccountable State of Surveillance*, Law, Governance and Technology Series 34, DOI 10.1007/978-3-319-47573-8_9

implemented Directive 95/46/EC and led to the creation of a new data protection authority, the '*Commission nationale pour la protection des données'* (CNPD), the National Commission for Data Protection, replacing the former *'Commission à la protection des données nominatives'*.[3] The regulation of privacy relating to telecommunications is treated in the Law of 30th May 2005,[4] which implemented the EU Directive on Privacy and Electronic Communications (2002/58/EC).

The 'data controller' and 'data processor', in the Act simply called 'controller' and 'processor', are described respectively as:

"a natural or legal person, public authority, agency or any other body which solely or jointly with others determines the purposes and methods of processing personal data. When the purposes and methods of processing are determined by or pursuant to legal provisions, the controller is determined by or pursuant to specific criteria in accordance with those legal provisions"; (Article 2 (n)) and
"a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"; (Article 2 (o)).[5]

As for the collection and processing of the data, there are three important Articles, which need to be emphasised here. Prior to the collecting and processing of the data, the controller and/or processor must notify the CNPD of the reason and purpose for their data processing activities. This notification must include the name and the address of the controller and the purpose of the processing (c.f. Article 12 and 13). The processing of sensitive data, such as genetic data, recorded data for supervision reasons, biometric data, processing of credit status and solvency (of non-professionals in the financial sector), as well as data processing for historical, statistical or scientific reasons, need an authorisation from the CNPD. In this case, the request for authorisation needs a much broader explanation of the means and ends of the processing. This includes the data controller providing a reason/justification of why the processing of data is in compliance with the law, outlining the origin of the data, and giving a detailed description of the data and the proposed processing operation (including an evaluation on the compliance with the security measures of the processing provided in the Article 22 and 23, e.g. technical and organisational measures to ensure data protection (c.f. Article 14)). Processing operations notified

[3] Chapter VII of the Law of 2 August 2002, deals with the creation of the national commission as a supervisory authority, with the charge 'of monitoring and checking that data being processed are processed in accordance with the provisions of this Law and its implementing regulations' (Art. 32 (1), Law of 2 August 2002).

[4] Texte coordonné de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques. Mémorial Journal Officiel du Grand-Duché de Luxembourg, A – N°172: 2941–2948.

[5] The Act even provides a definition of the term 'supervision' (or in other words, surveillance), as "any activity which, carried out using technical instruments, consists of observing, collecting or recording in a non-occasional manner the personal data of one or more persons, concerning behaviour, movements, communications or the use of electronic computerised instruments"; (Article 2 (p)).

or authorised by the CNPD are published in a national register, which is accessible to the public, in order to simplify the right of access to data for the data subject. This register is available on the website of the CNPD (see more below).

9.1.2 Application (Primary and Secondary Legislation) and Interpretation (Case Law) of the Right of Access to Data

Chapter VI of the Law of 2nd August 2002 describes the rights of the data subject which are categorised as the subject's right to information, the right of access and the right to object. For the first point, the subject's right to information, the data subject has to be informed of the processing of their personal data, as this information is the main precondition for the subject to exercise his other rights. At the moment of the collection of the data, the subject must be informed about 'who the data controller is' and 'for what purpose the data is collected'. Information as to whether the data is provided to third parties and who they are has also to be given (Article 26). In the case of CCTV surveillance, citizens are informed through signage. For other types of data processing citizens are informed through terms and conditions forms/documentation whilst registering for the service linked to the data processing.

As for the right of access, the subject has the right, upon application to the controller, to obtain free of charge, without excessive waiting periods and at reasonable intervals, the access to data (Article 28 (1) (a)), a confirmation whether personal data is being processed (Article 28 (1) (b)) and the revelation of the data undergoing the processing in an understandable way (Article 28 (1) (c)). Unfortunately there is no specific information as to how long the waiting period should be and can result in a broad interpretation. If the access to data is intentionally obstructed in any way, a prison sentence of between eight days and one year and/or a fine of between 251 and 125.000 Euros may be received (Article 28 (2)). In case of a supposed non-compliance between the data delivered to the data subject and the processed data, the subject can notify the CNPD, who will then check the case and take further action if necessary (Article 28 (6)).

Important case law on the right of access to data in Luxembourg is non-existing, although an increase in complaints, filed at the CNPD concerning the right of access to data and the right to object has been monitored between 2008 and 2011. While in 2007 only 34 complaints were filed at the CNPD, those numbers rose to 63 in 2008, 133 in 2009, 145 in 2010 and 115 in 2011 (CNPD 2012). According to the CNPD, the main reason for this rise in numbers is an increase of international companies, like eBay Europe, PayPal, Skype Communications or Amazon EU, having their head office in Luxembourg. As a result, some of the complaints were forwarded from foreign DPAs to the CNPD.

9.1.3 National Exceptions to the EU Data Protection Directive and to the Right of Access to Data

There are no uniquely national exceptions to the EU Data Protection Directive and the exceptions to the right of access to data are similar to those included in the Directive. In the Law of 2nd August 2002 those exceptions are specified in Article 29 and consist mainly of the safeguard of national security, in the context of crime prevention and solving, or in case of 'major economic or financial interest of the State or of the European Union, including monetary, budgetary and taxation matters'(Article 29 (1) (e)). Also, the right of access to data may be constrained for the protection of the data subject or the rights and freedoms of others (Article 29 (1) (a)–(g)).

In contrast to the Directive 95/46/EC, the Law of 2nd August 2002 goes even further as to how to handle the exceptions to the right of access to data. On the one hand, an exception is added for personal data processed for journalistic, artistic or literary expression, as they may be entitled to only 'cover information concerning the origin of the data making it possible to identify a source' (Article 29 (3)). On the other hand, the controller must explain why the right of access to data is limited or deferred. In this case, the CNPD has investigative powers and can rectify, delete or block any data of which the processing doesn't comply with the law (Article 29 (5)).

9.1.4 Compatibility of National Legislation with Directive 95/46/EC

The national legislation translated Directive 95/46/EC almost word for word, without any exceptions but with several additions. For example the Article 8 of the Directive, the processing of special categories of data – in the Law of 2nd August, Articles 6 to 8 – has in the national legislation more specific explanations as to how genetic, health and legal data should be processed. In the Luxembourgish legislation, Articles 10 and 11 were also added to clarify the processing for what the legislation calls 'supervision purposes' (seemingly referring to CCTV surveillance in public and private spaces for security purposes) and supervision at the workplace, which is not treated by Directive 95/46/EC.

A further addition compared to the Directive 95/46/EC is found in Article 28 of the Law of 2nd August 2002, concerning the right of access. A specification as to how the right to access has to be provided in case of health data of patients is included in the Luxembourgish legislation. Particularly, the right of access will be exercised by the patient or through a doctor they appoint. In case of the patient's death, the right to access may be exercised by 'his non legally separated spouse and his children as well as any other person who at the time of the death has lived with him in his household, or in the case of minors, his father and mother' (Article 28 (3)).

Processing for the purposes of supervision at the workplace is not dealt with anymore in the Law of 2nd August 2002 since the changes on 27th July 2007. This is now covered in Article L. 261-1 of the Employment Law.[6] According to the Article, processing for the purposes of supervision at the workplace is only possible if needed for the security or the health of employees, for the protection of the properties of the company, for the control of the production process handled by machines, for the temporary control of the production or the service of employees if this is the only way to ascertain the exact salary, or for the organisation of flexible working hours.[7]

9.1.5 Surveillance and Access Rights

The practice of CCTV surveillance in Luxembourg has been largely influenced by four different circumstances, namely the amendment of the Law of 2nd August 2002; the judgment on the role of the CNPD; the judgment on the use of CCTV evidence in court; and the judgment on CCTV footage used for criminal investigations. These circumstances and cases are described in greater detail here below.

1. Revision of the Law of 2nd August 2002 on 27th July 2007

Up until 27th July 2007, CCTV surveillance in public spaces was only permitted if the site "presents by its nature, its situation, its layout or its frequentation a risk making the processing necessary for the safety of the user and for the prevention of accidents".[8] On 27th July 2007, the legislation was changed, leading to the current version of the Law of 2nd August 2002 which extended Article 10 (1) (b) by adding: 'the protection of property, if there is a characteristic risk of theft or vandalism' (the Law of 2nd August 2002). This therefore allowed CCTV to be operated for the prevention of theft and vandalism. An important point in Article 10 (1) (b)[9] is the phrase 'that makes the processing necessary'. This wording was chosen on purpose, as CCTV surveillance needs authorisation from the CNPD, who thus has to decide from case to case whether or not CCTV surveillance is necessary. The applicant needs to provide a proof of necessity; the possible risk of theft, vandalism or safety (which has to be in any case higher than the average risk).

---

[6] Service Central de Législation Luxembourg – Code du Travail 2013: 142.

[7] Art. L. 261-1. (1) of the Employment Law.

[8] Translated from the French: Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, Article 10 (1) (b).

[9] Article 10. Processing for supervision purposes

(1) The data may only be processed for supervision purposes:

(b) in surroundings or in any place accessible or inaccessible to the public other than residential premises, particularly indoor car parks, stations, airports and on public transport, provided the place in question due to its nature, position, configuration or frequentation presents a risk that makes the processing necessary for the safety of users and for the prevention of accidents, (…).

2. The permission of the CNPD to interpret legislation

The judgement[10] from the administrative court on 15th December 2004 and the subsequent appellate judgement[11] from 12th July 2005 confirmed that the CNPD is entitled to interpret provisions concerning the use of CCTV cameras. In case N° 17890, a company wanted to annul of the decision of the CNPD which had refused the authorisation of CCTV surveillance on their sales counter. The CNPD stated that there was no reasonable argumentation as to why the CCTV surveillance should be installed, as there was neither evidence of a high risk to the safety of their customers, nor to the safety of their employees. The company only wanted to install the CCTV for the protection of its goods.[12,13] At the administrative court, the company argued that the CNPD had made an interpretation of the legislation, which they were not entitled to do. Both the administrative court as well as the appellate court replied that the legislator, by using the wording *'necessary'* in the legislation and endowed the CNPD with the task to evaluate the necessity of the processing.[14] As argued by the courts, the proof of necessity needs to be made by the applicant.[15]

3. Usage of illegal CCTV footage in court

The case concerned the use of illegally obtained CCTV evidence. Heard in the first instance in the district court of Luxembourg City,[16] it concerned the lawfulness of CCTV evidence. The evidence was part of a criminal proceeding, where a police officer was convicted for making an assassination threat and announcing a non-existent danger triggering the intervention of the police. On 18 February 2005, the officer made a telephone call to the Grand-Ducal Palace and threatened to carry out an assassination at the palace. This call was made from a telephone box in Luxembourg City, on the premises of the telecommunication company, P&T. The only evidence, which made it possible to identify the police officer, was a recording of the telephone call from a CCTV camera installed in the telephone box in 2004 (Elvinger 2012: 1). According to Article 14 of the Law of 2nd August 2002, CCTV for the purpose of ensuring safety and security needs authorisation of the CNPD. Although the company filed a request for authorisation in 2004, on 18th February 2005 the file was still being processed by the CNPD. So at the moment of the crime, the CCTV was not authorised by the CNPD and thus was illegal. Still, the investigation used the video material to identify the caller, who was charged and

[10] Jugement N° 17890 du rôle du tribunal administratif du Grand-Duché de Luxembourg du 15 décembre 2004.

[11] Arrêt de la Cour administrative N°19234 C du 12 juillet 2005.

[12] This case happened before the changes from the 27th July 2007 in the Law of 2 August 2002 took place, extending CCTV surveillance on theft and vandalism.

[13] Judgment N°17890: 2 ff.

[14] Ib.: 10.

[15] Appel N° 19234 C: 11.

[16] Judgment n°2523/2006 of the district court of Luxembourg City, 13th July 2006.

interrogated 1 day later, on 19th February 2005.[17] The defendants' lawyers underlined that the video material was acquired in the most illegal way and thus all the investigations and judgements were based on that unlawful evidence. Therefore, the defence proposed "to cancel, because of violation of the rights acknowledged to the citizen, by the international conventions as well as by the constitution, the entirety of the preliminary investigations and the resulting judicial inquiry".[18]

The prosecutor on the other hand argued that for the non-authorisation of CCTV, Article 14 of the Law of 2nd August 2002 provides for a sentence between eight days and one year and a fine between €251 and €125.000. However, he pointed out that Article 14 did not prohibit the use of the information acquired in an illegal way. Therefore, as long as the credibility of the material evidence was not affected, the prosecutor saw no reason not to accept the CCTV material. It was further argued that "in the end one has to consider the proportionality between the unlawfulness and the offence being part of the criminal proceedings".[19]

The court decided in the first instance in favour of the defence. To permit the use of illegal CCTV usage would set the door wide open for a massive, non-authorised surveillance by private organisations and could also 'result in a much broader interpretation of the fundamental rights for the protection of the citizen, his freedom and his duties'.[20] As for the use of unlawfully acquired evidence material in court, the court urged that the prosecutor should act as the guardian of the law and therefore should not act in any illegal way.[21] As such, the court of first instance declared the evidence and thus the CCTV material null and void and cancelled the hearing and the conviction resulting from the investigations.[22]

The prosecutor appealed against the decision of the district court and the case was heard in the second instance at the appellate court. There, the prosecutor reminded the court that under certain circumstances illegitimate evidence has been accepted. The court considered the objection of the prosecutor and agreed that illegally obtained evidence does not need to be discarded right away. However, quoting the case law in Luxembourg and Belgium, the court outlined that there are three main issues which needs to be respected here. They asserted that circumstances when evidence is to be seen as illegal (and thus not to be used in court) are:

1. In case of a precise judgement of invalidity on a case-by-case basis, where certain conditions of illegitimacy of the evidence are met;
2. In case illegitimacy affects the reliability of the evidence;

[17] Jugement n°2523/2006: 3 f.

[18] Ib.: 3.

[19] Ib.

[20] Ib.: 8.

[21] In making this ruling, the court also criticised the Belgian Court of Cassation, who, in a judgement of 14 February 2001 decided that illegally obtained evidence could be used in court under certain circumstances. Cour de Cassation de Belgique, Arret n° P001350F; P001353F, 14 février, 2001, available at http://jure.juridat.just.fgov.be/?lang=fr (last accessed 1 July 2013).

Jugement n°2523/2006: 12 f.

[22] Jugement n°2523/2006: 12 f.

3. In case of a violation of Article 6 of the European Human Rights Convention (ECHR).[23,24]

Although the first two issues did not apply in this case, the court noted a violation of Art. 6 ECHR. The court of appeal said that the case was based on a single piece of evidence, illegally obtained and thus the defendant could not be proven guilty according to law. This was the main difference to the Belgian and French cases. The court agreed that at the district court, the rationale of the judgement and the defence arguments regarding the global surveillance character – which may be truthful – were exaggerated for the present case. The court also agreed that the CCTV request for authorization was filed at the CNPD by the P&T. Although it was not accepted on the date of the crime, there would have been no reason for the CNPD to oppose it. However, since the prosecutor could not bring valid arguments as to why *only* this illegal evidence had to be used in this case, the violation of Art. 6 Section 2 of the ECHR persisted and thus the court decided not to accept the evidence and to dismiss the appeal.

The prosecutor appealed a second time, this time in front of the Luxembourgish Court of Cassation. The court of cassation did not agree with the appellate court, acknowledging errors in the judgement and quashed the previous judgement. The main reason was that the appellate court had failed to consider the case as a whole. According to the Court of Cassation,

> the judge can deduce this conclusion [of the case] only after the examination of the facts as a whole, which has to contain the examination of the manner in which the evidence was collected and thus the circumstances in which the illegality has been committed, including the quality and the goal of the perpetrator. This is a decisive criteria which the judge cannot refuse to acknowledge as a principle when examining if the right to a fair trial has been violated.[25]

So, the Court of Cassation sent the case back to the appellate court for revision. Responding to the objections of the court of cassation, the appellate court evaluated and weighted the evidence a second time, paying attention on the case as a whole. The court considered that the tracking of evidence is exclusively governed by the investigating judge. Finally, the appellate court reconfirmed the first judgement, declaring that the illegally obtained CCTV evidence could not, under these circumstances, be used in court (Elvinger 2012: 3). As a consequence, although under certain circumstances CCTV evidence may be used in court, in cases where it violates the right to a fair trial, the evidence cannot be used.

4. Revelation of CCTV footage in public

[23] Article 6: Right to a fair trial, especially segment 2: *"Everyone charged with a criminal offence shall be presumed innocent until proved guilty* ***according to law****."* (European Convention on Human Rights: 9).

[24] Arrêt de la cour d'appel, N°126/07: 17.

[25] Translated from French: Arrêt de la cour de cassation n°57/2007 pénal. du 22.11.2007: 3.

Finally, the last case of importance is the 'arrêt n°254/12 Ch.c.C.' of 24th April 2012 heard in the appellate court. The appellant demanded the annulation of his investigative files from the police and the investigative judge due to illegal CCTV evidence and the revealing of the CCTV footage in public by the investigative judge. Briefly, the appellate was convicted as a result of an assault after the police noticed an injured person on the 15th December 2011 on a train and seized the CCTV footage. On 4th January 2012, the investigative judge also seized more CCTV footage from the train station in Luxembourg City.[26] The appellant argued that firstly, the CCTV processing had not been authorised by the CNPD and secondly that the investigative judge and the police, by publishing the footage on the national television channel RTL and on the police homepage, violated the principle of judicial confidentiality.[27] As such, the appellant demanded all his investigative files be annulled. Following consultation of the national register of the CNPD, the appellate court noticed that the CNPD *had* authorised the CCTV surveillance and its use as evidence was thus not illegal. As for the revealing of the CCTV footage on national television, the appellate court stated that neither Art. 8, nor Art 35 of the Code of Criminal Investigation, nor any other legislation forbids the investigative judge from publishing 'the recorded surveillance documents in order to identify the author of a criminal offence'.[28] As a result, the appeal was dismissed by the court.

9.1.6 The Promotion of Access Rights by DPAs and National Authorities and Their Role in Ensuring Compliance to National Norms

The CNPD provides on its website's homepage an extensive explanation about citizens' rights regarding data protection, including a detailed, and understandable description of the right of information, right of access and the right to object. The information is provided in French and German and is in fact a simplified version of the Law of 2nd August 2002. Information about how to assert your rights and what to do in case of infringement of your rights is also provided on the CNPD homepage. Unfortunately, there is no template letter available for citizens to use when making subject access requests. However, the CNPD suggests simply writing a registered letter and including a copy of identification. They refer to the national register in order to verify if personal data is processed or if a company is registered and thus allowed to process the data.

In cases where your rights are infringed, the CNPD suggests that you should first complain to the data controller insisting on your rights. If a satisfactory response is not received from the data controller, data subjects are then advised to file a

[26] Arrêt n°254/12 Ch.c.C.: 2.

[27] Violation of the Articles 8 and 35 of the Code of Criminal Investigation.

[28] Arrêt n°254/12 Ch.c.C.: 3.

complaint to the CNPD. This can be done via an online form that is available on the CNPD internet site, and can be signed digitally. This document is only available in French. Furthermore a downloadable template letter addressed to Google is available on the CNPD website, forbidding the use of unblurred Google Street View images of your premises. Like in other European countries, the collection of unsecured Wi-Fi data by the Google Street View car in Luxembourg led to a temporary prohibition of the service in Luxembourg. As Google had already taken pictures in different regions in Luxembourg in 2009, the CNPD provided the template form, so citizens could demand the blurring of their premises. According to the CNPD, approximately 500 complaints have been made. It took Google several years to meet the demands of the CNPD as well as the complaints of the citizens. Only in late 2014 Google Street View was available in Luxembourg, while citizens still have the possibility to have their face, house, car or other objects blurred on Street View (Luxemburger Wort 2014). The CNPD also publishes on its website national and international news on data protection, issues statements on important topics, provides brochures about data protection and privacy and publishes annual reports about the work of the CNPD.

9.1.7 Role of National DPAs in Ensuring That Data Controllers Allow Citizens to Exercise Their Access Rights

On the website of the CNPD, data controllers are informed about their duties in order to allow citizens to exercise their access rights. On the one hand, information about how to process data and how to inform citizens (including how to respond to access rights requests) are given on the website. On the other hand, the CNPD provides a national register of data controllers. As soon as a data controller informs the CNPD about a data processing or receives authorisation for the processing of sensitive data, the data controller is added to the national register. This register is available on the homepage of the CNPD (2014) and can be accessed by anyone.

The register provides two kinds of information. The first concerns contact information concerning the data controller or processor, including the address. In many cases however, the data controller is not specified and the address leads only to the head office of the company. The second concerns the information that is available in the register about how the data is processed. This includes a short description about the processing, the reason why the data is processed, categories of the data subject, categories of the processed data, conditions of the legitimacy of the processing, legal basis or specific regulatory requirements, categories of recipients and categories of data which are submitted, data transfer outside the EU and the expected storage time of the processed data. The database can either be searched by key words, such as the name or the location of the company, or simply browsed. Due to a large number of exceptions regarding the notification of processing under the Law of 2nd

August 2002 (Art. 12 (2) a–e; (3) a–n), many data controllers are missing on the national register.

9.2 Exercising Access Rights in Practice

9.2.1 Introduction

This part describes, analyses and summarises the experience gathered during our attempts to locate data controllers and, having done so, submit access requests to organisations. As part of this process, we attempted to locate data controllers in 33 organisations and subsequently submitted 19 subject access requests to a wide range of data controllers both in the public and private sector in Luxembourg and, in case of some multinational companies, beyond its borders. Below is a summary assessment of the findings is presented, followed by the detailed analysis of experiences with public and private sector organizations, including multinational companies, and, as a specific category, CCTV operators. In the concluding section of this report the authors not only summarize their findings but also identify some possible outcomes of the research.

9.2.2 Locating Data Controllers

Before citizens can submit an access request, they must of course locate the organisation to whom a request should be sent. Within these organisations, citizens must identify the person or office nominated as the data controller whose responsibility it is to receive and response to subject access requests. We attempted to locate data controllers within 33 different organisations in total (Table 9.1).

In total 33 sites where visited for the research in Luxembourg of which 23 could be completed. Although the task of locating the data controller was initially anticipated to be easy, it proved to be more difficult than expected. Of all the 33 researched sites, only 8 could be completed by checking the legal/privacy section of the website of the organisation, informing citizens about their right to access personal data and how to make a request including the contact details.

Other sites only provided an e-mail address, often a general ‘info’ or ‘office’ address, and made it necessary to write an e-mail asking for the contact details. For 13 of the researched sites it was often necessary to search for general contact details like an e-mail address or a telephone number, in order to ask for data controller contact details and information on how to make a subject access request. Four sites did not even have a privacy policy section on their website at all. Thus to summarize, of the 33 research sites in total:

Table 9.1 Summary of findings when attempting to locate data controller contact details

Data controller contact details successfully identified in first round of visits	8 of 33 cases (24.24 %)
Data controller contact details unable to identify in first round of visits	25 of 33 cases (75.76 %)
Total number of data controller contact details successfully identified after second round of visits	23 of 33 cases (69.70 %)
Total number of data controller contact details unable to identify after second round of visits	10 of 33 cases (30.3 %)
Contact details identified via online privacy policy	8 of 23 (successful) cases
Contact details identified after speaking to member of staff on phone/via email	15 of 23 (successful) cases
Contact details identified after speaking to member of staff in person	0 of 23 (successful) cases
Average rating given to visibility of privacy content online[a]	1.97
Average rating given to the quality of information given by online content	1.29
Average rating given to visibility and content of CCTV signage	1.40
Average rating given to quality of information given by staff on the telephone	1.86
Average rating given to quality of information given by staff in person	1

[a]Rating Guidance
1 = Poor – This should indicate a level which is not fit for purpose in its specific context and forces citizens to explore alternative means to locate a data controller
2 = Reasonable – This should indicate a level which is reasonable in the circumstances and which fulfils the minimum legal standard
3 = Good – This should indicate a level which goes beyond the minimum legal standard and demonstrates good practice in a particular context

- Eight sites mentioned the access rights and included at least the contact details for the data controller.
- Ten sites mentioned the access rights but did not give any details as to how to make a subject access request and failed to give data controller contact details.
- Eight sites failed to mention access rights at all, or did not have a legal/privacy section on their website.
- Four sites didn't have their own internet site.
- Three sites mis-interpreted access rights, blocking every attempt to obtain data controller contact details.

Most of the problems were encountered at the level of *national* organisations, both public and private. The privacy policies were mostly very short and important information relating to what data is processed and how to make a subject access request was often missing. For instance, the loyalty card programme of a large supermarket chain informed us about the right to access data and included the data controller contact details but without clear information about what to include in the subject access request. Interestingly, since their head office is situated in France,

they give as reference the French legislation and data protection authority, despite relating to the loyalty card programme for Luxembourg. Moreover, most of the information within these privacy policies was specifically for the personal data entered on internet sites and not for other data related to their service as a whole. Finally, what data is processed was often not clear, as it was neither outlined in their online privacy policies, nor properly explained we asked about this by mail, phone or in person, thus making it inscrutable for the citizen.

Overall however, most of the sites investigated in this research showed some effort to help us in our enquiries, especially during contact with staff members, who often tried to help us regarding the subject access request process despite their lack of knowledge. Nonetheless, a lot of time and effort could be saved if we could have access to all the information we needed online, without having to ask.

- Generally speaking, the organisations we researched displayed many poor practices making the possibility of a citizen submitting a subject access request difficult. Especially for the national sites in Luxembourg, extra effort is needed to get the information one needs in order to make informed decisions about how their data is managed. This includes information such as the type of data which is collected, whom it is shared with and especially how to make a subject access request. Although most of the sites provide citizens with some of this information, sufficient information as to how to actually make a subject access request is rarely available. Only two of the international sites clearly provided all the necessary information and presented it in an intelligible way. But, crucially, none of the national organisations we studied managed this; the lack of expertise was probably one of the biggest difficulties concerning the right to access data on a national level.
- Many people we contacted did not know how to handle our requests and therefore gave us the wrong information. While this reflects a lack of training it also suggests that enquiries regarding access to personal data are not very common in Luxembourg.

9.2.3 Submitting Access Requests

In total 19 requests were sent to different organisations (Table 9.2) of which only four were returned completed within the timeframe.[29] Most of the answers received were incomplete and needed additional clarification. Thus after sending a second round of requests and pointing out the missing information, we received in total six *complete* answers, where our personal data was disclosed and all our questions answered in a satisfactory manner (Table 9.3).

[29] In Luxembourg, the law does not provide a fixed timeframe against which organisations must respond to subject access requests. In order to determine what one may consider facilitative or restrictive practice, we used a 40 day response time as an 'unofficial' timeframe against which to measure the timeliness of responses.

Table 9.2 List of sites to which subject access requests were sent

	Public/ private	Site
1	Public	CCTV in open street
2	Public	CCTV in a transport setting (train station)
3	Public	CCTV in a government building
4	Private	CCTV in a department store
5	Private	CCTV in a bank
6	Public	Local authority
7	Public	Police criminal records
8	Public	Interpol
9	Public	Vehicle licensing
10	Private	Loyalty card (department store)
11	Private	Mobile phone carrier
12	Private	Banking records
13	Private	Loyalty card (air miles)
14	Private	Advanced passenger information
15	Private	Twitter
16	Private	Amazon
17	Private	Facebook Ireland Ltd.
18	Private	Microsoft
19	Private	Google

In relation to requests for CCTV footage, the main concern that data controllers expressed when responding to our requests was the risk of infringement of third parties' privacy. Other concerns and reasons for denial of access were security reasons and vague and unclear legal interpretations, as some organisations misinterpreted the legal rulings in Luxembourg concerning the right of access to data. A special case of access to CCTV data was experienced with the public CCTV monitoring in the security areas of Luxembourg City, with the state prosecutor being 'the authority of control' and responsible for the right of access to data, but not being responsible for further information on the data, like third party sharing and automated decision making.[30]

In general, the quality of the responses varied widely throughout the different sites. The only consistency seemed to be in the way that citizens actively had to collect the different kinds of information necessary to submit the subject access requests. Generally speaking, the information provided by data controllers concerning how to make a subject access request is not extensive enough for citizens to easily access their data. For instance, there are no templates via which to write access requests, either on the website of the different sites, or on the website of the

[30] See the legal analysis above for more details about these legal regulations. See also the CCTV section below for a detailled describtion of the role of the authority of control regarding subject access requests in CCTV cases.

Fig. 9.1 Access on our academia.edu profile during the period of the research

CNPD, and there is often no information about whom to address requests to. In our research, this meant that we had to send several requests to general company addresses with instructions to forward the request to the data controller within an organisation. Due to the absence of templates, at times it seemed as though data controllers were not certain how to deal with access requests, often resulting in incomplete answers including misleading information. In only six cases, answers from organisations provided satisfactory information without the need for extra requests or clarifications. Most cases needed clarifications after the first response, lengthening and complicating the process of accessing personal data. Some of the responses also showed a lack of trust, and sometimes even respect towards the data subject.

A general trend in the response of data controllers, especially for the CCTV sites, was to state the justification that the surveillance system was ensuring the safety of those visiting, rather than addressing our subject access request. Moreover, data controllers often simply referred to the CNPD authorisation number[31] of the CCTV and the presence of the CCTV system in the national register as justification for its deployment. Although none of our subject access requests questioned the legitimacy of the data processing, it seems as if many data controllers interpreted our requests as such.

Involvement in the research also resulted in multiple Google searches for our names from Luxembourg quite shortly after sending the subject access requests. Using Google analytics via our academic.edu profile, it was possible to trace the searches back to the origin of the IP-address, in those cases to Luxembourg (Fig. 9.2). As Fig. 9.1 shows below, prior to making the requests, there were no searches.

[31] As outlined in the legal analysis of data protection in Luxembourg, CCTV systems must register with the CNPD upon which they will receive a registration number. This number is then often displayed on CCTV signage.

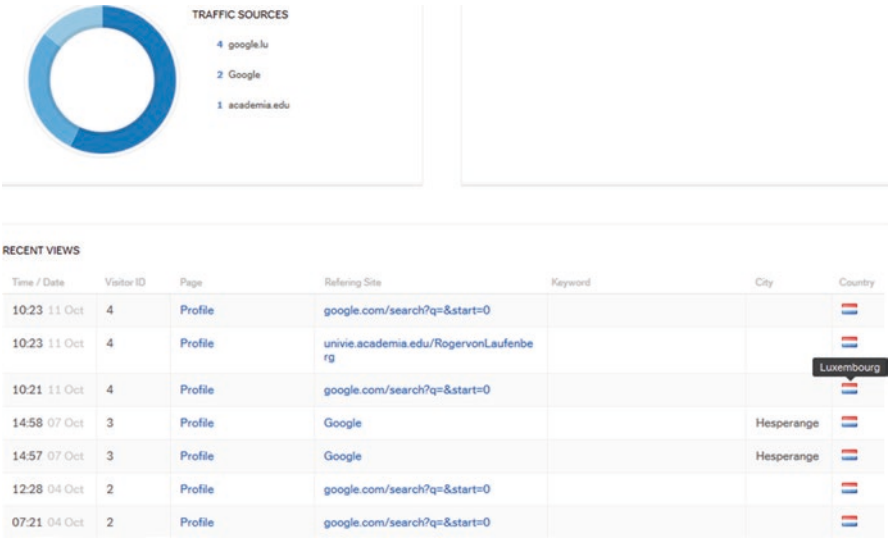

Fig. 9.2 Origin of the access on our academia.edu profile – the visitor ID indicates three different users all based in Luxembourg

However, these searches began after we submitted our requests and all but stopped some time after our requests had all been sent.

Thus one can infer that our subject access requests raised suspicion or curiosity on the part of the data controllers who evidently wished to know more about the person behind the requests.

Another problem arose with one part of the legal text concerning the access right, which led on a number of occasions to complications and delays during the request for data. The Art. 28 of 'the Law of 2nd August 2002' states that: *"the data subject or his beneficiaries*[32] *who can prove they have a legitimate interest may obtain (…)."* Some of the data controllers to whom requests were sent interpreted the wording of this article in a way that the data subject *himself* was required to prove a legitimate interest, rather than his beneficiaries. Thus, several data controllers initially refused the disclosure of the data necessitating extra communication to clarify this issue (Table 9.3).

[32] In French, the term 'ayants droit' is used, describing the persons eligible for a heritage, without the existence of a family relationship.

Table 9.3 Quantitative data pertaining to the submission of access request

Total number of complete answers received after a first round of requests	3 of 19 cases (15.79 %)
Total number of complete answers received after a second round of requests	6 of 19 cases (31.58 %)
Total number of incomplete answers received after a second round of requests	13 of 19 cases (68.42 %)
Of which non-disclosure of personal data[a]	10 of 13 incomplete cases
Of which no information about third-party sharing[a]	11 of 13 incomplete cases
Of which no information about automatic decision making[a]	11 of 14 incomplete cases
Total number of non-responses after a first round of requests	4 of 19 cases (21.05 %)
Total number of non-responses after a second round of requests	2 of 19 cases (10.52 %)
Official complaints filed at the DPA	6 complaints

[a]Incomplete answers can include not disclosing personal data, but still giving information about third party sharing and/or automatic decision making

9.2.4 Case by Case Analysis

Public Sector

Interpol

The request sent to Interpol was probably the best treated case of all during this research. Since this was the only site which provided an extensive explanation concerning the subject access request and including a template, sending the request was easy and quickly done. We sent our request to the commission for the Control of INTERPOL's Files (CCF) in Lyon, including a proof of identity. A reply from the CCF was received less than a month later and thus within the 40 days waiting period. The letter stated that the request was admissible as the required documents had been provided and informed us *"that the appropriate checks have been carried out and that there is no information to disclose that is applicable*".

This shows a highly professional way of treating the right of access to data by providing all necessary information beforehand, in order to grant a facilitate way of sending the request and by responding quickly, completely and in a respectful manner.

Police Records

Having submitted our request, our records were disclosed in two parts, with the second letter explaining that *"the transmission of the records isn't obliged by the Law of 2nd August 2002, but is done with the agreement of the prosecutor (…)."* We

were also advised that our records had not been shared with third parties – including Europol – and regarding the automatic decision making, as the authority is not the data processor, they could not make any comment about that matter.[33]

Local Authority

Our request was processed by the municipality within 3 weeks, disclosing the personal data file they held about us in their system and confirming that none of the data had been communicated with third parties. Unfortunately, our questions regarding the automatic decision making was not answered.

Vehicle Licensing Records

Several restrictive practices can be found in Luxembourg, though most of them probably not deliberate. This was particularly the case while trying to access our personal data in relation with our vehicle and driving license at the 'Société Nationale de Circulation Automobile' (SNCA). Trying to obtain any information about the processing of our personal data and who to send the subject access request to remained unsuccessful, despite sending several requests. After receiving no information as to how to submit a subject access request or to whom we should specifically address it, we sent our applications to the head office. We received no response whatsoever for 2 months (64 days).

Thus, we sent a second letter asking that our request be considered once more. This second attempt triggered a reaction from the SNCA, although not the desired one. A reply was received, referring to our initial request without mentioning any delays. Although they confirmed our presence in two of their databases,[34] they were not able to disclose our personal data: *"(…) I regret to have to inform you that unfortunately we don't have enough human resources at our disposal to answer your multitude of questions in writing (…)."* With this response, the SNCA seemed to confirm that due to a lack of manpower they were not able to handle subject access requests at all. This is clearly not in compliance with data protection law. This may also be an indication of the low importance and regard given to subject access requests by the organisation. Although we do not know the number of subject access requests the SNCA receives, they still have a legal obligation to handle individual requests. However, this was the only site in the research which responded that the request could not be processed at all.

[33] A more detailed description of 'problems' of the authority of control will be addressed in the CCTV section – open street CCTV.

[34] There is one database for the registration of all the vehicles and their owners in Luxembourg, as well as one database for the driving licence holders in Luxembourg. The government of the Grand-Duchy of Luxembourg has entrusted the SNCA with the management of these databases.

In order to grant us our right of access to the data however, they gave us the possibility, upon arrangement, to visit them in person at their office so we could – jointly with one of their experts – have a look ourselves in the databases for our personal data. According to their letter, the time spent by their expert showing us our personal data would however *"be charged on the basis of the rate concluded in point 12° table C of the article 43 of the modified Grand-Ducal Regulation of the 27. January 2001, defining the operational procedures of a system of the roadworthiness of road vehicles, being 37.83 EUR (excluding VAT 15 %) per half hour or part of half hour."*

Giving us the possibility to personally check the databases together with one of their experts may be an attempt to try to grant us access to our personal data, but several of the above mentioned points show a very restrictive practice in the disclosure of personal data. Firstly by not answering our initial request, we were forced to send a second request, causing a long delay and additional postage costs. The way our request was handled thereafter was not courteous at all, and we failed to receive any apology or acknowledgement of the long delay. Having to come to their office personally is additionally time consuming for the data subject and the supplemental costs for the visit seem not only totally excessive, but also in noncompliance with Art. 28 of the Law of 2nd August 2002 stating that the data subject *"may obtain free of charge (…) access to data about him."*

The approach by the SNCA is also questionable in this regard, as they are designated by department of transport – a department of the Ministry for Sustainable Development and Infrastructures – to act as:

> *"the organisation of the registration, including the assignment of the registration numbers (…) and the introduction and running of a computerised system for the management of a national database of the road vehicles and their owners and holders. The* SNCT[35] *is equally in charge of the current operations linked with the driving licences."* Furthermore the department mentions that *"in order to carry out the tasks entrusted by the government, the SNCT provides for the staff and the administrative, technical and data processing means necessary for the appropriate functioning of the service for the roadworthiness of the vehicles and the suitable offices for the processing of the vehicle registration requests and the issuing of the documents regarding the registration and the roadworthiness of the vehicles"* (Ministère du Développement durable et des Infrastructures 2014)

Due to the above mentioned reasons, particularly the noncompliance with data protection law, an official complaint was sent to the national data protection authority. At the time of writing, we have had no response from the DPA on this matter.

[35] Société Nationale de Contrôle Technique – The SNCT is the main organisation dealing with the vehicle registration, but mostly with the roadworthiness of the vehicles, while the SNCA is responsible for the actual registrations of the driving licence holders.

Private Sector

Bank Records

The clearest and most complete response across the entire research was obtained for our banking records without the need for a lengthy correspondence. The information about where to send the access request and the necessity of a proof of identity was available on the homepage of the company's website. Similarly to the other sites in this research (except for Interpol), the absence of a template as well as any specific guidance on the company's website made it necessary to send a general access request letter and required us to decide what information to include in order to obtain a satisfactory response in the shortest timeframe. In order to circumvent possible delays in regard to the general company address provided in the privacy section, an additional line was added to the address reading 'FAO the personal data controller'.

The request was sent to the general office of the bank in Luxembourg City, where it was processed by the legal and litigation services of the bank. The reply to our request followed just 3 weeks later, thus within the timeframe of 40 days.

The response received was detailed and it was obvious that the data controller was anxious to provide the requested information. The communication was very respectful – which wasn't the case for all answers we received in this research. The only critique might be that they pointed out twice that we had initially entrusted them with our personal data at the moment we made a contractual agreement with them. The way this was communicated seems as though they tried to make sense of the request by clarifying that it was us in the first place who provided them with our data, thus questioning why we would want to have information about it afterwards. This is only an assumption based on the lack of trust and understanding which we encountered in general during the research in Luxembourg.

The actual personal data they sent us was by far the most elaborate we received from all the sites in this research. In an annex to their reply, they sent us a printed 50 page file, starting from our first deposit account in 1993 to the renewal of our bank account in 2011.

Alongside this extensive disclosure of personal data, we also received information concerning data sharing with third parties and automated decision making processes. For the first part, it was stressed that for the functioning of our credit card, it was necessary for the bank to communicate our name, address and credit card limit to the credit card company on a monthly basis.

The information concerning automated decision making processes in relation to our data was addressed at length. It was explained that regarding our personal bank account, two different automated decision making processes are in evidence:

- The first one *"the logic of the 'know your customer rules', which has to be followed by our credit institution in accordance with the legal provision governing the combat against money laundering and the financing of terrorism."*

- The second is *"the logic of the respect for the contractual obligations imposed on the banker when intervening as custodian of the funds. So, automated decision making from our part will take place at every time when you want to make a money withdrawal at an ATM to the extent that our computer systems automatically verify the existence of a sufficient provision to justify the withdrawal."*

So although highly technical and legal terms were used in the correspondence, the bank also made the effort to give further explanations. Overall the extent of information, the clarity and the quickness in which the information was provided, as well as the level of respect with which the data subject was addressed has to be seen as a good reaction of the data controllers to the subject access request.

Microsoft

Of all the multinational private organisations, Microsoft disclosed the most information compared with the other sites. The information necessary in order to locate the company's data controller can be found relatively quickly on their homepage in the section: '*Privacy Statement'* (Microsoft 2014). Here, Microsoft informs the user about the different ways of accessing personal data through different online forms or profile sections of their various services. Furthermore, the privacy statement also mentions the possibility that "*if you cannot access personal data collected by Microsoft sites or services via the links above, these sites and services may provide you with other ways to access to your data. You can contact Microsoft by using the web form. We will respond to requests to access or delete your personal information within 30 days*" (Microsoft 2014).

Thus Microsoft gives the user the possibility to directly contact the company through a web form and assures the user that a response will be received within 30 days of the request. Moreover, the privacy statement, in its last section entitled '*Other Important Privacy Information'*, offers further ways of contacting the chief privacy officer of Microsoft, through mail or phone in the US, or the subsidiary in the respective country. Thus after a little bit more than 5 min, the address of Microsoft Luxembourg could be found on the company's website. In general therefore, the privacy section – although extensive – is lucid and comprehensible.

We sent our subject access request and were asked, some weeks later, to confirm our request through email, upon which the investigation of our request was assured. One detailed response was received via email a further month later with the disclosure of my data downloadable on 'SkyDrive'. It is worth noting that although our request was sent in French, the responses we obtained were all in English – therefore presuming that the data subject can speak and understand English. This is interesting insofar as they seemed to understand fully the request and all the details we had asked them, as their response addressed all the points and questions from our request. So the respondents were clearly proficient in French but nevertheless responded in English. However, on a positive note, a second similar answer from Microsoft was received some weeks later by mail, this time in French which mainly

consisted of an identical response to the previous letter but which had this time been translated into French.

Content-wise, although all of our questions were addressed, not all of the responses were satisfying. The disclosure of our personal data was extensive, including headers of our emails dating back to 2007 as well as IP-logging for a period of 1 year. Automatic decision making in regard to our personal data could not be identified. However, for the sharing of our personal data, no specific answer was given, except for a reference to the privacy statement.

Thus all in all, the response we received was clear and complete insofar as it can be verified – except for the third party sharing, where no exact third parties were mentioned. Although in the first instance the communication was in English, the additional responses were in French, which shows that the data controller is willing to be transparent in regard to the data protection principles. In contrast, the data controller showed an evasive practice concerning third party sharing – a crucial point regarding data protection. Compared to other similar sites like Facebook and Google however, Microsoft showed the best practice in responding to the subject access request, but a complete response including exact information about third party sharing would have been ideal and therefore leaves room for improvement.

Amazon

The data controller of Amazon, represented by the legal department, answered exactly within 40 days of the submission of our subject access request – disclosing our personal data from our amazon.fr, amazon.de and amazon.co.uk accounts. Since the disclosure of our personal data contained some sensitive data, like our credit card information, the encrypted CD-ROM which contained our data was sent separately from the passwords, which represents a good practice regarding the security of data. Third party sharing was confirmed by Amazon, referring to their data protection principles online, but only general potential receivers of data were mentioned, without specifying exactly which third parties have had access to our personal data – as we had asked in my request. Further, according to their response, automated decision making is not used by Amazon, although questions remain here concerning Amazon's customer profiling practices which appear to use algorithms which one would assume employ automated decision making processes.

Twitter

Our request to Twitter was sent via mail to the Twitter headquarters in the US, upon which we received an e-mail to confirm our request a little over a month later. Three days after this, we received another e-mail with a ZIP-file attached, disclosing our personal data. Our data mainly consists of.txt documents, thus not really easy to read and not very comprehensible. On the other hand, the disclosure was very extensive, including the log-ins with the IP addresses we have used. The Twitter legal

department also informed us that none of our data had been disclosed to law enforcement agencies, but did not provide any information about other types of third party sharing and automatic decision making and thus was also not complete. Moreover, the response was in English although our subject access request was, like for all the other sites, written in French.

Mobile Phone Carrier

While requesting our personal data processed by our mobile phone carrier, several difficulties occurred. The first one was simply not being able to identify the data controller. Although the right of access is mentioned on their homepage, users are advised to contact the customer service department. This department however, was not able to provide the necessary information in order to submit an access request. Since the CNPD provides a national register (CNPD 2014) for all organisations who registered their data processing – with the goal to inform citizens and make access easier – we tried to identify the data processer through the register. The company could be found, together with an outline of their data processing in relation to their customers (including what data is collected) and also their address. However, this address was only the general company address and not an exact identification of the data processer/controller.

Thus we submitted our request to the indicated address, asking for our personal data, including our communication details. We received no reply at all to this request and thus sent a reminder 2 month later. Since this letter also remained unanswered, we sent an official complaint to the CNPD.

Two months later, our reminder letter dated several months previously was sent back to us by the Luxemburgish Postal Service, indicating that the address did not exist. Indeed, on the homepage of the company, the main company address was different. Thus the information on the CNPD national register is outdated, defeating the initial goal of the CNPD's register. Still it seems strange that our first request, sent to the same address, was not sent back but simply remained unanswered.

Probably as a reaction to the complaint we had sent to the CNPD, the company finally issued us with an answer which included the disclosure of our data a further month later. Although the data controller did not mention our complaint to the CNPD, the letter apologised for the delay. The disclosure of our personal data was very complete, including personal as well as technical details such as our unique identifier corresponding to our home address, 'disability'[36] settings and 'Roam-NoSMS'[37] settings. Especially for the last two technical settings, we did not know these were possible, as this was not communicated to us when subscribing to the

[36] 'Disability' settings relate to whether the user does or does not want to receive welcoming SMS when in roaming mode.

[37] 'Roam-NoSMS' settings relate to whether the user does or does not want to receive SMS when in roaming mode.

company's service and thus shows the importance of access to personal data as a form of providing information.

Furthermore the data controller provided us with information about third party sharing, which mainly consisted of a printing company, an external call centre which has access to all our personal data, as well as their bank, but without specifically providing the names or the contact details of these companies. As for automated decision making, the data controller advised that our profile is currently not affected by any such processes.

Altogether, this example shows a multitude of different aspects concerning subject access requests. First of all, this case shows how an organisation could facilitate the right of access to data by providing the necessary information in a clear and understandable manner on their homepage or in another easily accessible way for citizens. In more general terms, this case also demonstrates the confusion which often surrounds the access request procedure in terms of who to direct requests to, which address to use and the lack of clarity concerning whether a request has been received or not.

Loyalty Card (Department Store)

Another interesting, restrictive case could be observed when trying to access our personal data collected by a department store in relation to a loyalty card. The privacy statement of the company's homepage, only available in English, did not provide a postal address but only e-mail addresses in order to contact the company for privacy reasons. On the 'Imprint' section however, a postal address was provided to contact the European office of the company, situated in Germany.

Thus, we emailed our request – in French – to the contact provided online. The answer arrived promptly a few hours later – in German – disclosing our name, address, e-mail address and date of birth, but no information about our purchased items and the automated decision making, which we had requested in our correspondence to them.

They did however include an answer about third party sharing, advising us that they make use of our personal data only for the loyalty card scheme and do not share such data with third parties. An extract of the privacy policy was included in the mail stating that *"(the company) collects and processes your personal data only for the performance of the (loyalty card) system (…). (The company) employs a contractor for the performance of the (loyalty card) system (…). The contractor (…) is legally obliged to process the data only at the behest of (the company)."* Thus despite stating that they do not share my personal data with third parties, the privacy policy says otherwise, as the contractor is considered as a third party. This demonstrates that there is a serious inconsistency within the legal department of the company insofar as what their official privacy policy states and what they communicate with individual customers. While the privacy policy clearly confirms the use of third

party sharing (although not specifically the identity of the third party), the response to our subject access request denied the use of third party sharing, thus providing misleading information to their customers. Although this was probably not a deliberate practice, the misleading communication – including the usage of German – and the missing data in the responses from of the data controller can be seen as a restrictive practice. As such, an official complaint was issued to the CNPD. At the time of writing, the complaint remained unanswered.

Loyalty Cards (Air Miles)

We sent our request to both the airline and the company operating the loyalty card scheme, since it was not clear which one serves as the data controller of the loyalty card scheme itself. The disclosure of our data was processed within less than a week but our questions regarding third party sharing and automatic decision making were not addressed. When contacting the airline a second time, the data controller invited us to meet in person in Brussels to discuss our query. Given that this was neither convenient nor a fulfilment of the data controller's legal obligations, we rejected the invitation and re-submitted our request. At this point, communication with the data controller broke off completely.

Advanced Passenger Information

Our first request, submitted via postal mail to the data controller, was unanswered by the airline. Only after we sent a reminder almost 2 month later was the request was processed. A total of 47 days had passed before we received a first response after sending a reminder. In this response, our flight bookings and our personal data – flight reservations, payment details excluding our credit card number, newsletter – in their different systems were disclosed, including the duration of the storage and the location of their databases (in Munich, Atlanta and Luxembourg). Information regarding the advanced passenger information, third party sharing as well as automated decision making were not addressed, although this was clearly and visibly emphasised in our requests.

Facebook

Our subject access request was sent to Facebook and requested details about third party sharing and automatic decision making. We received no response whatsoever to this query and as such proceeded to submit a complaint to the CNPD. At the time of writing, our complaint remains unanswered.

Google

Our subject access request was sent via postal mail to Google's the headquarters in the US – Google Inc. An answer was obtained a few weeks later which outlined the importance of the data subject's control of his personal data online and referring to their download services Google Dashboard and Google Takeout via which data subjects can allegedly control and monitor their own data. Information about third party sharing and automatic decision making was not provided by Google, except for a reference to their Privacy Policy. A second request sent shortly thereafter seeking clarification of their first response but this remained unanswered, leading us to make a complaint to the CNPD. At the time of writing, we have received no response from the CNPD on this matter.

9.2.5 CCTV & Signage

A wide variety of practices could be observed in all the steps of accessing CCTV data, from the moment of visiting the site, searching for information on CCTV signage, through to sending requests and asking for the disclosure of the data. In some sites, no CCTV signage could be found at all. This was the case in the site of CCTV in a government building.[38] In general however, CCTV signage could be found in almost all the sites.

The main purpose of the CCTV signage in Luxembourg seems to be to inform the citizen of the ongoing video surveillance rather than advise citizens as to the identification of the data controller or about the possibility of access to data. None of the identified signage included a detailed identification of the data controller or any information about the possibility of submitting subject access requests, although the Law of 2nd August 2002 indicates in Art. 26 that the data subject has a right to information concerning when the data is collected and the controller must supply information about *"the existence of the right of access to data concerning him and the right to rectify them inasmuch as, in view of the specific circumstances in which the data is collected, this additional information is necessary to ensure the fair processing of the data in respect of the data subject."* Although it is clear that CCTV signage only provides limited space, and with the unique CNPD authorisation number at least a partial identification of the data controller is granted, the signage observed in this research could be improved by simple means, such as simply adding one line with the specific contact details of the data controller.

[38] When visiting the site and despite the large amount of CCTV surveillance, no signage could be identified. Upon contacting the ministry they assured us that five stickers indicating the authorisation number of the CNPD are clearly installed outside on several locations of the ministry building. Without denying the presence of the stickers indicating the authorisation number of the CNPD, it has to be noted that upon observing closely for the research purposes, we did not notice this signage – which makes it questionable if lay people would identify the signage.

Picture 9.1 Signage of the CCTV surveillance at the train station in Luxembourg City in French, German and English, including the CNPD authorisation number

Picture 9.2 Signage in the form of a sticker on a revolving door at the shopping centre in Bertrange, also including the CNPD authorisation number but without mentioning the operator (Source: Own collection – photograph taken on 27/09/13)

The size of the signage which was observed during this research varied largely from metal signs to a small sticker indicating the presence of video surveillance (see Pictures 9.1 and 9.2). The larger signage has of course the advantage that it is easily spotted and provides more space for information and thus should be considered to be the advantageous form of signage. If a sticker indicating the video surveillance is mounted on an eye-catching surface, as in the Picture 9.2, on the entrance door, it is at least in compliance with Article 10 – Processing for supervision purposes, (2)[39] and Article 26 – the data subject's right to information of the Law 2nd August 2002, which both ensure that the data subject is informed about the data processing in question. Problems with those stickers arise here too however, when they are placed in corners or on other barely visible surfaces. If signage in the form of a sticker cannot be spotted for research purposes, it is highly possible that the signage is even less visible for lay people.

While most of the signs where only in French, a small number of the researched sites had bi- or multi-language signage, in combinations of French, English and

[39] "(2) Data subjects will be informed by appropriate means such as signage, circulars and/or letters sent by registered post or electronic means of the processing stated in paragraph (1) letters (b) and (c). At the request of the data subject, the controller will provide the latter with the information stated in Article 26, paragraph (2)."

Picture 9.3 Sign in the department store, indicating the video surveillance and referring to the French law for the planning of security issues – 'Loi N°95-73 du 21.01.1998 d'orientation et de programmation relative à la sécurité' (Source: Own collection – photograph taken on 28/09/13)

German, which proves to be a good practice due to the international setting of Luxembourg City.

Case by Case Analysis

CCTV in a Department Store

In this case, we visited a large department store located within a shopping mall. Perhaps strangely, the department store's CCTV surveillance system holds the same CNPD registration number as the shopping centre within which the store is located, despite the two entities being different limited companies.

Upon revisiting the store, we noticed newly installed signs informing of the CCTV surveillance. At least at every entrance of the department store, the signage was clearly visible hanging from the ceiling (see Picture 9.3). Although highly visible, the signage still represents bad practice for several reasons. Firstly, it provides misleading information by referring to one of the French laws regulating the video surveillance. Secondly, the signage fails to provide any contact details despite stating that customers should contact the security manager for any inquiry. Indeed, the signage clearly leaves space for a telephone number but this hasn't been filled in.

We sent our request by e-mail and postal mail and also addressed the erroneous information on the signage. An answer to our request was received just 2 weeks later from the head of the security department of the shopping centre and department store. In this reply, our right of access was denied with the argument that

'according to the Article 28 (1) of the Law of 2nd August 2002 (…), such a request is subject to a proof of a legitimate interest' and without such a justification our right to access could not be accepted. Furthermore, due to the presence of other data subjects in the footage, the footage could not be issued to us since there may be a conflict with their right to privacy.

Regarding the third party sharing of the data, the head of security stated that only in case of an incident or upon request, the footage could be shared with the police and/or the judicial authorities. The response also advised that automatic decision making is not part of the processing of the personal data in regard to the CCTV surveillance.

As this response was not adequate, mainly because of the non-disclosure of our personal data and the reason used by the head of security, we sent a second letter explaining that we deemed their interpretation of the law to be incorrect. We included a lengthy legal explanation of their mis-interpretation, hoping that our request would thus be expedited.

The answer from the company arrived roughly 2 weeks later. Compared to the first answer which lacked an official character, the second answer had more the appearance of an official company letter.[40] Content wise however, the second answer did not differentiate much from the first. Not only was no footage from our visit available anymore due to the automatic deletion of the material, even if the footage was still available, they still would not disclose the requested data, again arguing that the privacy of other 'shopping centre users' would be compromised. For this reason, they would need an adequate reason of our part as to why we should obtain access to our data. Furthermore the head of security stated that according to Article 29 (1) (f) the data controller can limit the right of access in order to *'protect the rights and freedoms of others'*.

The mentioned article 29, used by the data controller of the company indeed states that in order to safeguard the *'protection of the data subject or the rights and freedoms of others'* (cf. Article 29 (1) (f) of the Law of 2nd August 2002) the right of access to data may be restricted by the data controller. Since Art. 29 (4) also mentions that in case of an exemption of the right of access, the controller must notify the reason the CNPD, the head of security of the department store also forwarded the answer to the Commission.

While in the first answer a clear misinterpretation of the data protection law was the reason for the non-disclosure of our personal data, the data controller was, although sticking to his previous answer, more compliant with the law in his second reply by referring to Art. 29 and forwarding the answer to the CNPD. Still, reflecting on the whole process from visiting the site, identifying the data controller and accessing the personal data, we conclude that a lay data subject probably would have no chance at all to arrive at this last stage of communication. All the mentioned steps needed several requests, mails and rectifications, which were

[40] Whilst the first answer had a black and white header with the company's logo and used the Microsoft Word Font 'Comic Sans MS', the second letter looks like the official store's stationary, including the VAT ID and the registration numbers.

incredibly time-consuming and frustrating and caused also extra costs. The general suspicion with which we were confronted from the beginning of our research – although the communication was more respectful in the latter stages – was also reflected in the outcome of the subject access request, since it seemed like all efforts had been made to not have to disclose the CCTV surveillance footage for whatever reason.

As the data controller's final response had also sent to the CNPD, we received a reply some weeks later from the data protection authority with a copy of the answer they had sent to the data controller of the store. In this letter, the CNPD stressed that some of the aspects mentioned by the data controller were in conflict with the Law of 2nd August 2002:

1. 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'*.
2. 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.
3. The assumption by the company 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 1 month (for some cameras five and eight days).
4. 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.

Moreover the CNPD mentioned that in order to prevent future data subjects from being deprived of exercising their right of access to data granted by Article 28 of the Law of 2nd August 2002, the data controller should consider the above mentioned aspects to apply to any further subject access requests.

Again, the response of the CNPD also reflects that the way the company was handling the request for access to data in a very restrictive way and needs improvement. This practice of course does not have to be deliberate and can mainly be the result of a lack of experience in responding to subject access requests and data protection cases. It is to be hoped that from now on, after the intervention of the CNPD, subject access requests are treated by the data controller in compliance with the law and without the need of the long communications.

CCTV in a Transport Setting

A very restrictive practice, beginning with the identification of the data controller, was observed with the national railway company. Concerning the signage, citizens are informed about the video surveillance and the signs are clearly visible. The use of three languages also shows good practice (see Picture 9.1), although information concerning the right of access is not mentioned. After visiting the railway station of Luxembourg City as well as using their parking lot, we sent our first subject access request to the organisation, asking for our personal data collected by their extensive CCTV system.

Our request was unanswered, thus a reminder was sent a month later, asking for an answer to our subject access request. Since the reminder was also ignored, we filed an official complaint to the CNPD, advising them of the fact that the data controller had ignored every request we had made to the company making it impossible for us to access our personal data. Even if the data controller of the company is unfamiliar with subject access requests, which has to be doubted since the homepage of the organisation mentions access rights, ignoring all of our requests gives the impression of a deliberate neglecting of data protection principles by the company. At the time of writing, our official complaint remained unanswered from both the CNPD and the company itself.

CCTV in an Open Street City Centre

Regarding the CCTV data of the open street city centre, an even more complicated process was encountered. The open street CCTV system – also called the VISUPOL project – is controlled by Art. 17 of the Law of 2nd August 2002 initiating a Luxembourgish regulation for the creation of security areas in Luxembourg City – which has to be renewed every year. The CCTV system is operated by the police of Luxembourg with the state prosecutor serving as the supervisory authority.

The signage in the security areas is similar to the signage of the transport company (see Picture 9.1) insofar as it uses three languages in order to inform the citizens of the ongoing video surveillance. The identity of the operator is illustrated by the logo of the grand-ducal police, but information concerning the right of access and whom to contact with privacy-related queries is not available. However, it is stated in Art. 17 (2) of the Law of 2 August that "*The right of access to data referred to in this Article may be exercised only through the supervisory authority. The supervisory authority will carry out the appropriate verification and investigations, arrange for any necessary rectifications and will inform the data subject that the processing in question does not contain any data contrary to the treaties, laws and implementing regulations.*" Thus we were able to conclude that the state prosecutor was the supervisory authority and therefore the responsible data controller in this case.

As a result, we sent our subject access request to the supervisory authority seeking disclosure of CCTV footage. The first answer was received within just a few days. This response did not disclose our personal data, but rather corrected some of the information we had stated in our letter. First of all, although the first regulation from 01/08/07 states that recordings are deleted at the latest after 2 months if footage is not part of any investigation, the supervisory authority confirmed that normally the destruction of the recordings is initiated a lot earlier (without giving an exact period). Furthermore, the state prosecutor explained the fact that since the footage is only consulted in case of an infraction where one has to identify the eventual perpetrator, victim or witness, *'no personal identification is carried out and the* "footage" *is not* "as such" *identifying'*. Another point made in the letter is that the law does not specifically grant the right of direct access of the data.

A few days later, we received a second answer, responding to the questions about automatic decision making and third party sharing. This mainly informed us that the supervisory authority does not use any automatic decision making and it does not share the personal data with third parties, since the authority is not the data controller, but only controls *'the legality of the operational processes by the grand-ducal police who is the data controller'*. Thus, the supervisory authority could not give us specific information on these matters. While confirming again the initial non-identification of the data subject on the CCTV footage, the authority also added – by citing the Art. 17 of the Law of 2 August – that *'the supervisory authority will carry out the appropriate verification and investigations, arrange for any necessary rectifications and will inform the data subject that the processing in question does not contain any data contrary to the treaties, laws and implementing regulations'* and thus is not directed to provide the data subject with the data in question. Furthermore regarding the exceptions and limitations in the European Directive 95/46/CE, the right of access may be restricted for the prevention, investigation, detection and prosecution of criminal offences. As such, the authority can grant the access to data with the agreement of the public prosecutor's office and not as a result of the Directive or the Law of 2nd August 2002.

As such, reflecting on the procedure of the communication and the information provided – beforehand and during the process of trying to obtain access to data – the case of open street CCTV in Luxembourg is very complicated. Despite the respectful and informative communication from the supervisory authority, the available information was not sufficient and moreover was too confusing in order to provide clear guidance for citizens concerning if and how they are able to access their data. Since the legal information is dispersed among different regulations and laws and while the grand-ducal police operates as the data controller though the right of access has to be exercised through the supervisory authority, (which is only able to rectify data and inform the data subject), it seems to be crucial to provide this important information to the citizens beforehand in an understandable and easy way.

It is a positive trend that the open street CCTV system has to be renegotiated every year through national regulations, initiating a yearly debate in the media, among other parties and in other cities in Luxembourg about the usefulness of the open street CCTV (see for instance Luxembourger Wort 2013), preventing the mass

surveillance of citizens in public spaces. But it would prove useful if for example the CNPD would provide clear information about the functioning and regulation of the open street CCTV system.

CCTV in Bank

A subject access request was sent to the legal department of the bank to which we received a reply 1 week later. Besides the justification as to why they operate CCTV and the indication of the authorisation of the CNPD of the surveillance measures, our access was denied with a reference to the article 29. Exceptions to the right of access of the Law of 2nd August 2002 and additionally since we had not mentioned a legitimate reason for our request to access the data. In reply, we sought a revision of the way our request had been processed and a specification of the denial of our right of access since we argued that we do not need to provide a reason for our access to data. In response, the bank's legal department referred to the protection of the privacy rights of others (art. 29 (f)) and the prevention and prosecution of crimes (art. 29(d)). Thus our personal data in the form of CCTV footage could not be disclosed. Moreover, the data controller assured us that none of our data had been shared with third parties and we were advised that no automatic decision making processes had been used in the CCTV surveillance, except for the automatic deletion of the footage after a specific period of time (without mentioning the exact period).

CCTV in Government Building

Our subject access request was sent to the organisation and the response of the ministry arrived just 5 days later. In the first instance, the data controller denied that third party sharing of the CCTV footage had taken place and indeed used this as a reason not to be able to disclose our personal data – for data protection and privacy reasons. When we responded to the data controller that this would not be a valid reason to limit our right of access, he surprisingly answered that we indeed did have a right of access to our recordings, but they were not able to provide a copy of the footage due to the presence of other data subjects on the footage. Furthermore it would be necessary to render those data subjects unrecognizable before the footage could be disclosed. It was also explained that since the footage is automatically deleted within 10 days – even though they have the right to store the footage for 1 month – the footage from our visit no longer existed. Besides the automatic deletion of the footage, we were advised that no other such processes are applied to the CCTV surveillance. Thus in the second instance, our right of access was acknowledged by the data controller but it was by then of no use since the footage was already deleted. On reflection, this appears to makes the organisation's first response look like a deliberate refusal for the disclosure of our personal data and potentially a delaying tactic to ensure the footage was erased.

9.2.6 Conclusion

In Luxembourg, legal regulations concerning data protection principles are clear and for most of the time, they are very similar to the European Directive 95/46/EC. However, the implementation and the execution of the law are in large parts deficient. This is especially seen in how data subjects are informed about the processing of their personal data. This is often insufficient and most of the time fails to provide the contact details necessary for an individual to submit a subject access request. Moreover, upon contacting different people within an organisation, necessary information regarding data protection principles are not very proficient, which often results in misleading and contradictory information being provided to the data subject. CCTV signage often fails to properly inform data subjects about the ongoing presence of CCTV surveillance, nor about any other information concerning the operator of the CCTV system. In some cases, signage simply gives notice about the ongoing operation, which is – although better than no signage at all – not sufficient information to enable individuals to easily enact their informational rights.

Here, two recommendations could resolve this problem. First, it would be helpful to simply provide all necessary information to the data subject via privacy policies on organisations' websites, or through the signage of the CCTV surveillance. Second, basic knowledge of data protection principles should be necessary for employees of an organisation, or at least being aware of whom to contact in case of data protection questions for members of the public. As a result, any person requesting information would be able to – sooner or later – locate it.

Overall in Luxembourg, both for CCTV as well as non-CCTV data, trying to access one's personal data, as is granted by the Law of 2nd August 2002, needs to be improved on several levels. Although some good practices have been experienced and in most cases the obstruction of the right of access was most probably not deliberate, it is more than difficult for citizens to execute their rights. Coherent guidelines regarding the subject access request procedure, together with template forms for data subjects as well as for data controllers, would be helpful in order to make the right of access to data easier for all parties. Most of the problems encountered in this research resulted from a lack of information from data controllers and (probably) not enough experience in handling subject access requests.

As a result of this lack of information and experience, incomplete answers from the data controllers were often received, leading in the end to additional – sometimes frustrating – communications between the data subject and the data controller. These were frustrating to the extent that the data controller often seemed to show a lack of comprehension as to why a data subject could be so persistent in asking for his/her own personal data. Moreover, it makes the actual goal of the right of access to data complicated to achieve – only six data controllers provided comprehensive and complete answers to our requests and only twelve disclosed our personal data.

In general, regarding the whole process of the access to data however, there is no obvious difference between the way public institutions and private organisations deal with data protection principles. For the former as well as for the latter, facilita-

tive as well as restrictive practices were experienced and the same can broadly be said regarding non-compliance with the Law of 2nd August 2002.

Not only was the disclosure of personal data often difficult to achieve during this research, the request for precise information about third party data sharing and automated decision making processes was not always taken seriously by data controllers. In these cases, responses often failed to address these topics or gave only general explanations, including the very general and broad assertion that personal data might be shared in some cases with some third parties. The impression after the research remains that most of the data controllers approached did not really know how to respond to the requests made. If this is combined with a lack of manpower within an organisation, requests can be regarded as unimportant as well as burdensome, often forcing the data subject to write multiple letters before receiving any sort of reply, let alone an adequate one. If data controllers provided clear guidance alongside subject access request templates, this would undoubtedly be helpful for the data subject to issue a request that is understandable for the data controller and provides enough information in order to efficiently process the request and respond in a satisfactory manner.

Finally, The role of the *Commission nationale pour la protection des données* is an ambiguous one in Luxembourg. Although there is some information available on their website concerning data protection principles and also regarding subject access requests, the experiences of this empirical study show that there still seems to be a lack of knowledge concerning such information in Luxembourg amongst data controllers – which could potentially be remedied proactively by an information campaign from the CNPD. It should be noted however that the way the CNPD reacted concerning the complaints we submitted during this research – although the handling time of those concerns seems rather long with more than 2 months – shows that they are willing to ensure the right of access to data and that data controllers process data in compliance with the Law of 2nd August 2002.

Moreover, the role of the data protection authority, the CNPD is double-edged. The website of the CNPD provides a lot of information, including a register of data controllers and processors, but fails to provide any guidelines about subject access requests or provide a template for either the data subject or for data controller to ease the access request process. In the research, while a response concerning a complaint concerning CCTV footage captured by a department store was resolved quickly, in favour of the data subject, other complaints remained unanswered without even an acknowledgement that the complaints were being processed. It will be necessary for data protection principles in Luxembourg to have better guidelines for both sides – data subject and data controller – in order to ensure that the practices of organisations are in compliance with data protection law. The role of the CNPD could be a crucial one in this process, by both providing the necessary information and guidance, and by supervising whether the legal requirements are met within organisations – especially in cases where complaints are submitted to the supervisory authority.

References

Legislation and Case Law

Arrêt de la Cour administrative N°19234 C du 12 juillet 2005. http://www.cnpd.public.lu/fr/legislation/jurisprudence/juris-lux/cour_administrative.pdf (Accessed 9 May 2014)

Arrêt de la Cour d'appel N°126/07 du 28 février 2007. http://www.cnpd.public.lu/fr/legislation/jurisprudence/juris-lux/arret_126_07_cour_appel.pdf (Accessed 9 May 2014)

Arrêt de la Cour d'appel n° 254/12 Ch.c.C. du 24 avril 2012. http://www.cnpd.public.lu/fr/legislation/jurisprudence/juris-lux/24avril2012.pdf (Accessed 9 May 2014)

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 9 May 2014)

Coordinated Text of the Law of 2nd 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. http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf (Accessed 9 May 2014)

European Court of Human Rights (2010) 'European Convention of Human Rights' http://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed 9 May 2014)

European Union (1995) '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' http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri = CELEX:31995 L0046:en:HTML (Accessed 9 May 2014)

Jugement N° 17890 du rôle du tribunal administratif du Grand-Duché de Luxembourg du 15 decembre 2004. http://www.ja.etat.lu/17890.doc (Accessed 09 May 2014)

Jugement n°2523/2006 du tribunal d'arrondissement de et à Luxembourg. http://www.cnpd.public.lu/fr/legislation/jurisprudence/juris-lux/jugement_2523_2006.pdf (Accessed 09 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 (Accessed 9 May 2014)

Règlement ministériel du 10 novembre 2011 portant désignation des zones de sécurité soumises à la vidéosurveillance de la police grand-ducale (2011), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A – N°231: 3959–3960. http://www.legilux.public.lu/leg/a/archives/2011/0231/a231.pdf (Accessed 09 May 2014)

Règlement ministériel du 25 avril 2012 portant désignation d'une nouvelle zone de sécurité soumise à la vidéosurveillance de la police grand-ducale (2012), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A – N°86: 949–950. http://www.legilux.public.lu/leg/a/archives/2012/0086/a086.pdf (Accessed 09 May 2014)

Règlement ministériel du 7 octobre 2013 portant désignation des zones de sécurité soumises à la vidéosurveillance de la Police grand-ducale (2013), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A – N°181: 3468–3472. http://www.legilux.public.lu/leg/a/archives/2013/0181/a181.pdf (Accessed 09 May 2014)

Service Central de Législation Luxembourg (2013) 'Code du Travail' http://www.legilux.public.lu/leg/textescoordonnes/codes/code_travail/Code_du_Travail.pdf (Accessed 09 May 2014)

Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel modifiée par la loi du 31 juillet 2006, la loi du 22 décembre 2006, la loi du 27 juillet 2007 (2007), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A – N°131: 2330–2361. http://www.legilux.public.lu/leg/a/archives/2007/0131/2007A2330A.html?highlight (Accessed 09 May 2014)

Articles and Reports

Commission Nationale Pour La Protection Des Données (CNPD) (2012) 'Rapport annuel 2011' http://www.cnpd.public.lu/fr/publications/rapports/cnpd/rapport_activite_2011.pdf (Accessed 9 May 2014)

Commission Nationale pour la Protection des Données (CNPD) (2014) Régistre Nationale. http://www.cnpd.public.lu/fr/registre/application/index.html (Accessed 9 May 2014)

Elvinger, A. (2012) 'Jurisprudence comparée – Belgique, France, Luxembourg, Allemagne – en matière d'exigence de la régularité des preuves et des procédures': 1–6. http://www.aedbf.eu/fileadmin/eu/pictures/news/2012/luxembourg/Andre-ELVINGER.pdf (Accessed 7 May 2014)

Luxembourger Wort (2013) Videoüberwachung um ein Jahr verlängert http://www.wort.lu/de/view/visupol-videoueberwachung-wird-um-ein-jahr-verlaengert-52447881e4b0ca64e0e520aa (Accessed 9 May 2014)

Luxemburger Wort (2014) Luxemburg in Street View http://www.wort.lu/de/lokales/mit-pegman-durchs-laendchen-luxemburg-in-street-view-5448bbf9b9b398870807decc (Accessed 30 June 2016)

Microsoft (2014) 'Privacy Statement' http://www.microsoft.com/privacystatement/en-gb/core/default.aspx (Accessed 09 May 2014)

Ministère du Développement durable et des Infrastructures – Département des transports (2014) 'Immatriculation et contrôle technique des véhicules', http://www.mt.public.lu/formulaires/circulation_routiere/immatriculation_controle_technique/(Accessed 09 May 2014)