INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

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

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

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

LUXEMBOURG COUNTRY REPORTS

INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE, AUSTRIA

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN LUXEMBOURG – ROGER VON LAUFENBERG

LOCATING THE DATA CONTROLLER IN LUXEMBOURG – ROGER VON LAUFENBERG

SUBMITTING ACCESS REQUESTS IN LUXEMBOURG – ROGER VON LAUFENBERG

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN LUXEMBOURG

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

In Luxembourg the 'Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data modified by the Law of 31 July 2006, the Law of 22 December 2006, the Law of 27 July 2007'[1] (hereinafter 'the Law of 2 August') regulates data protection principles. The Law of 2 August 2002 replaced the 'Act of 31 March 1979 concerning the Use of Nominal Data in Computer Processing'[2], which had been widely ignored as it was out of date in regard to modern technology.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 2 August 2002 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 on privacy relating to telecommunications is treated in the Law of 30 May 2005,[4] which implemented the EU Directive on Privacy and Electronic Communications (2002/58/EC).

The Law of 2 August 2002 provides a large set of definitions, concerning the terms used in the Act. A selection of the most important definitions will be highlighted in the next sections: 'Personal data' is defined as:

"any information of any type regardless of the type of medium, including sound and image, relating to an identified or identifiable natural person ('data subject'); a natural (…) person will be considered to be identifiable if they can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to their physical, physiological, genetic, mental, cultural, social or economic, identity;" (Article 2 (e)).

Extra definitions are provided concerning the 'health' and the 'genetic data', which are defined as:

"any information about the data subject's physical or mental state, including genetic information;" and "any data concerning the hereditary characteristics of an individual or group of related individuals"; (Article 2 (f) (g)).

[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.

[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.

As for a 'personal filing system', the Act defines it as a follows:

(hereinafter referred to as 'filing system'): "will mean any structured set of data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis"; (Article 2 (e)).

The 'data controller' and 'data processor', in the Act simply called 'controller' and 'processor', are described 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]

Finally, 'processing of personal data' is defined as:

(hereinafter referred to as 'processing'): "any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"; (Article 2 (r)).

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, 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 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).

[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)).

In Luxembourg, there is one standout legal case regarding data protection and privacy. The case concerned the use of illegally obtained CCTV evidence. The case[6] was heard in the first instance in the district court of Luxembourg City and concerned the lawfulness of the 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 18th 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 mail and 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[7]. According to Article 14 of the Law of 2 August 2002, CCTV for the purpose of supervision needs authorisation of the CNPD. Although the P&T 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 interrogated one day later, on 19th February 2005.[8] Different reasoning was used regarding the lawfulness of illegal evidence material, whether or not the CCTV material should have been used for the investigation and prosecution. On the defence side, the lawyers underlined that the video material was acquired in the most illegal way and thus all the investigations and judgements were based on that one, 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'[9].

The prosecutor on the other hand argued that for the non-authorisation of CCTV, Article 14 of the Law of 2 August 2002 provides for a sentence between eight days and one year and a fine of 251 € and 125.000 €. But the Article 14 does not prohibit the use of the information acquired in an illegal way. Therefore, as long as the credibility of the material evidence isn't 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'[10].

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'[11]. 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. In making this ruling, the court also criticised the Belgian Court of Cassation, who, in a judgement of 14th February 2001 decided that illegally obtained evidence could be used in

[6] Judgment n°2523/2006 of the district court of Luxembourg City, 13th July 2006.
[7] Elvinger, A. (2012) 'Jurisprudence comparée – Belgique, France, Luxembourg, Allemagne – en matière d'exigence de la régularité des preuves et des procédures': 1. http://aedbf.org/fileadmin/eu/pictures/news/2012/luxembourg/Andre-ELVINGER.pdf (last accessed 07 May 2014).
[8] Jugement n°2523/2006: 3f.
[9] Ib.: 3
[10] Ib.
[11] Ib.: 8

court under certain circumstances.[12] 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[13].

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, referring to recent case law in Luxembourg, Belgium and France. The court considered the objection of the prosecutor and agreed that illegally obtained evidence doesn't 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 is 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 of the impact of the illegitimacy, on the reliability of the evidence;
3. In case of the violation of the Article 6 of the European Human Rights Convention (ECHR)[14] [15]

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 application for the CCTV was filed at the CNPD by the P&T and although it wasn't accepted on the date of the crime, there would've been no reason for the CNPD to oppose the application. However, since the prosecutor could not bring valid arguments as to why *only* this illegal evidence should be used on this case, the violation of the Art. 6 Section 2 of the EHRC 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 didn't agree with the appellate court, stating 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:

> *"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, a decisive criteria which the judge can't refuse to acknowledge as a principle when examining if the right to a fair trial has been violated; that the appellate court by refusing as a*

[12] 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).
[13] Jugement n°2523/2006: 12f
[14] 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).
[15] Arrêt de la cour d'appel, N°126/07: 17

> *principle and in a peremptory manner, on the grounds that an act is either illegal or not and the illegal character of an act isn't affected neither by the quality nor by the desired goal of the perpetrator, admitting that the consideration of the above-mentioned circumstances constitute decisive criteria with regard to the demand for a fair trial, has violated the rules and legal provisions".*[16]

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. The combination of the production of an illegal form of evidence and the proceedings in violation of the law was still in violation of the right to a fair trial. This right tends in respect to the rights of the defence and presupposes the lawfulness of the proceedings. Thus the appellate court reconfirmed the first judgement, declaring that the illegally obtained CCTV evidence could not, under these circumstances, be used in court.[17]

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

Chapter VI of the Law of 2 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 the 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 practice, citizens are informed through signage, especially in case of CCTV supervision, but there are also some cases where CCTV surveillance is undertaken, without any information that surveillance is taking place, the reason for the surveillance or the identity of the data controller. The information provided only consists of a CCTV recording in process, not about the data controller. 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. In other cases, signs merely alter citizens that surveillance is being undertaken, but not its purpose or the identity of the data controller.

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 125000 Euros may be received (Article 28 (2)). In case of a supposed non-compliance between the data delivered to the data subject and the

[16] Translated from French: Arrêt de la cour de cassation n°57/2007 pénal. du 22.11.2007: 3
[17] C.f. Elvinger, A. (2012): 3

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[18]. 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.

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 the similar to those included in the Directive. In the Law of 2 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 2 August 2002 goes even further on 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)).

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 2 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 supervision purposes and supervision at the workplace, which is not treated by the Directive 95/46/EC. As noted in Section 1 above, the Law of 2 August 2002 also gives, unlike the Directive, a definition of 'supervision'.

A further addition compared to the Directive 95/46/EC is found in Article 28 of the Law of 2 August 2002, concerning the right of access. A specification as to how the right to access has

[18] Commission Nationale Pour La Protection Des Données (2012) 'Rapport annuel 2011': 68. http://www.cnpd.public.lu/fr/publications/rapports/cnpd/rapport_activite_2011.pdf (last accessed 07 May 2014).

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 himself or through a doctor he appoints. 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 2 August 2002 since the changes on 27th July 2007. This is now covered in Article L.261-1 of the Employment Law.[19] 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[20].

Surveillance and access rights: codes of practice at national level. (CCTV and credit rating)

The practice of CCTV surveillance in Luxembourg was largely influenced by three different cases: the first one, which was heard at two instances, clarified the roles of the CNPD and the applicant of processing upon authorisation of CCTV. The second (discussed in Section 1), illustrated in what circumstances unlawfully obtained CCTV evidence is eligible in court. The third case concerned whether or not CCTV footage of a criminal offence may be made public. These cases are described in greater detail below.

Revision of the Law of 2 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' (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)). On 27th July 2007, the legislation was changed, leading to the current version of the Law of 2 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 2 August 2002). This therefore allowed CCTV to be operated for the prevention of theft and vandalism. An important point in Article 10 (1) (b)[21] is the phrase 'that makes the processing necessary' (ib.). 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

[19] Code du Travail 2013: 142.
[20] Art. L. 261-1. (1) of the Employment Law
[21] 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, (...).

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).

Case 1 – The permission of the CNPD to interpret the legislation

A judgement[22] from the administrative court on 15th December 2004 and the subsequent appellate judgement[23] from 12th July 2005 confirmed this proceeding from the CNPD. In case N° 17890, a company wanted an annulation 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 no evidence of a high risk to the safety of the customers, nor for the safety of the employees. The company only wanted to install the CCTV for the protection of its goods[24].[25] 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, endowed the CNPD with the task to evaluate the necessity of the processing[26] and that the proof of necessity needs to be made by the applicant.[27]

Case 2 – Usage of illegal CCTV footage in court

As outlined in the opening section above, Case N°2523/2006 illustrated that although under certain circumstances CCTV evidence may be used in court, in cases where it violates the right to a fair trial, (as it did in this case due to being the only available evidence), the evidence cannot be used.[28]

Case 3 - Revelation of CCTV footage in public

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 two more CCTV footages from the train station in Luxembourg City.[29] The appellant argued that firstly, the CCTV processing hadn't been authorised be 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.[30] As such, the appellant demanded the annulation of all his investigative files. 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

[22] Jugement N° 17890 du rôle du tribunal administratif du Grand-Duché de Luxembourg du 15 décembre 2004.
[23] Arrêt de la Cour administrative N°19234 C du 12 juillet 2005.
[24] 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.
[25] Jugement N°17890: 2ff
[26] Ib.: 10
[27] Appel N° 19234 C: 11
[28] For a detailed description of the case, see section 1 of the country report.
[29] Arrêt n°254/12 Ch.c.C.: 2
[30] Violation of the Articles 8 and 35 of the Code of Criminal Investigation.

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'[31]. As a result, the appeal was dismissed by the court.

The changes of the 'Law of 2 August 2002' on the 27th of July 2007 also enabled the creation of security areas via a Luxembourg regulation. Article 17 - 'Authorisation by regulatory means' - describes these security areas as 'any place to which the public has access that by its nature, location, configuration or frequentation presents a greater risk of criminal offences being committed'. Currently there are four security areas in Luxembourg City[32]; the processing of the CCTV data is done by the state prosecutor – or his deputy – and two members of the CNPD, all acting as a supervisory authority. Access to data can only be exercised through the supervisory authority.

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

The CNPD provides on their 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 2 August 2002. Information about how to assert your rights and what to do in case of infringement of your rights is also provided on their 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 (see Section 7) in order to verify if personal data is processed or if a company is registered and thus allowed to process the data.

In cases of infringement of your rights, the CNPD suggests first to 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 complaint to the CNPD. For the latter an online form is available on the internet site, which can be completed online and 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 the 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, the CNPD provided the template form, so citizens could demand the blurring of their premises. According to the CNPD, approximately 500 complaints were made which demanded the blurring of their pictures. Since Google still has not met those complaints, the service still is banned and Google has no permission to take further pictures in Luxembourg.[33] The CNPD also publishes on its website national and international news on data protection on a regular basis, issues statements on important topics, provides brochures about data protection and privacy and writes annual reports about the work of the CNPD.

[31] Arrêt n°254/12 Ch.c.C.: 3
[32] Memorial A – N°231; 3960
[33] See http://www.tageblatt.lu/nachrichten/luxemburg/story/18611439 (Only available in German, last accessed 08 May 2014).

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 the data and how to inform the 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[34] and can be accessed by anyone. The register provides two kind of information. First, the information of the data controller or processor, including the address. In many cases however, the data controller isn't really specified and the address leads only to the head office of the company. The second information available in the register is related the processing of the data. 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 by 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 at the CNPD, by the Law of 2 August 2002 (Art. 12 (2) a-e; (3) a-n), several data controllers are missing on the national register.

[34] http://www.cnpd.public.lu/fr/registre/application/index.html (last accessed 24 June 2013).

LOCATING THE DATA CONTROLLER IN LUXEMBOURG

Introduction

The following country profile summary outlines the attempts of locating the data controller contact details for the research-sites in Luxembourg. The broad variety of sites gives an overview of the good and bad practices of data controllers and the information provided to the citizens concerning the right to access data in Luxembourg, but it has to be noted that they are only chosen examples.

Methodological thoughts

The primary entry point while attempting to locate data controllers' details was the internet sites of the research sites. Particularly for some of the international organisations and companies, this approach was the most successful and the easiest way to locate the data controller details. For most of the national sites in Luxembourg, private organisations as well as public institutions, online privacy policies gave only limited information concerning access rights, sometimes not even information about personal data being processed. For this reason, several of the research sites needed further requests by phone, e-mail or in person. Most of the e-mails sent received a quick response with the requested contact details or at least with further information as to how to proceed to acquire the requested details. Others however, did not reply at all. Phone calls and personal contact were the least chosen entry point, as it often was not clear whom to contact or speak with. Personal contact with staff members was especially needed for some of the CCTV sites. On the phone or in person, staff members often showed little or no knowledge about the data controller and were rather suspicious regarding my questions. Nevertheless, they still tried to provide me with as much information, but due to their lack of expertise on data protection matters, the information was often insufficient or incorrect.

Some of the sites couldn't be completed in Luxembourg at all because those sites are non-existent in Luxembourg, like the automatic number plate recognition or the border-control.[35] For other sites, it was not possible to find any contact details for the data controller even after several attempts including a number of emailed requests. These are considered in greater detail below.

[35] Instead of the border control, this site was replaced with the customs and excise, being thematically the nearest public institution and also doing irregular checks at the borders of Luxembourg.

Overall impressions

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[36]	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

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 even necessary to search for general contact details like an e-mail address or a telephone number, in order to ask for the data controller and how to make a subject access request. Four national sites didn't even have a privacy policy section on their website (the driving licence, the school records (primary as well as secondary school) and the green party).

[36] 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.

Thus to summarize, of the 33 research sites in total:

- 8 sites mentioned the access rights and included at least the contact details for the data controller. (e.g.: banking records; online gaming; internet service provider)
- 10 sites mentioned the access rights but didn't give any details as to how to make a subject access request and failed to give data controller contact details. (e.g.: the Police, the transport company and the bank)
- 8 sites failed to mention access rights at all, or didn't have a legal/privacy section on their website. (e.g.: the political party)
- 4 sites didn't have their own internet site. (e.g.: Local health record, local store)
- 3 sites (deliberately?) mis-interpreted the access rights, blocking every attempt to get the data controller contact details. (e.g.: Facebook, Google)

Most of the problems were encountered at the level of *national* organisations, both public and private. The privacy policies are mostly kept short and important information regarding to what data is processed and how to make a subject access request is often missing (e.g. the loyalty card programme of a large supermarket chain informs about the right to access, including the contact details but without more 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 the internet site and not for other data related to their service as a whole – as for example with the Police or the customs and excise. Finally, what data is processed was also not always very clear, as they didn't explain this in their online privacy policies, nor when I asked about this by mail, phone or in person, thus making it inscrutable for the citizen. For example the website of a credit card provider first stated in their legal section, concerning personal data that '(the company) commits themselves to respect all the legal provisions concerning the processing of personal data in the Grand-Duchy of Luxembourg'. However, the website was later updated and the legal section changed and the data protection section was even more reduced to 'the information received via the Internet'[37]. The customs and excises also didn't give any further information when responding to the e-mail request and only provided the contact details of the data controller. Finally, the mobile phone carrier did not give any information about the data controller, not on the website, on e-mail request or on telephone request.

For my personal health file on the other hand, it occurred also – probably due to the lack of knowledge on behalf of the member of staff who replied to my query – that I was granted access to my personal data by simply writing an e-mail with my address without anyone asking me for any formal request by mail, nor any proof of identity. Even when I asked on the phone if they would need anything else of me, I was told that an e-mail would be sufficient. A few days later, I received by mail my personal health records of the hospital, without anyone having checked my ID. This bad practice may be a result of the lack of knowledge concerning data protection, resulting in a careless handling of my personal health file. At an international level meanwhile, negative practices were experienced when concrete information regarding the access request was deliberately obstructed, making it impossible for citizens to issue subject access request, like for example with Google and Facebook. These instances are described further below.

[37] Quoted directly from the company's official privacy policy.

Still most of the sites showed some effort, especially after I got in contact with staff members, who were mostly willing to help me regarding the subject access request despite their lack of knowledge in a lot of cases. Nonetheless a lot of time and effort could be saved, if citizens could get all the information needed online without having to ask.

Best/Good practice

Best practice examples in Luxembourg are hard to find. However, there are several *good* practice cases which were found whilst researching data protection policies and searching for contact details. Most of the good practice cases were found in organisations operating at an international level. These organisations delivered the highest amount of information, without having to search and/or ask for a long time. The best practice in this case was Interpol. A four minute search on their internet site gave the required information, explaining how to write a request and even providing a template form. As the request is send to the Commission of Control of Interpol's Files (CCF), an independent organ of Interpol specifically tasked with dealing with access requests of personal data, an extensive FAQ[38] is available on their website. Also, the request is free of charge which for an international organisation is rather an exception. Nonetheless the CCF doesn't inform the applicant about the exact waiting times but instead uses vague statements concerning the duration, describing how the request is treated internally. Information about what data is processed by Interpol may also be requested by the applicants but is not available beforehand.

Another example of good practice was found on an international, private level via the online gaming company. On the first view of the legal section of their website, it looked like 'typical' global organisation data protection statement, providing a large amount of legal information concerning data protection without supplying the essential items like the contact details (similar to the approach of Google and Facebook as described further below). The privacy policy of the company is divided in 14 sections, with a large amount of information such as what data they collect, with whom they share the data and outlining that the customer has a right of access to data. Here the main difference to the other companies is the information concerning the right of access, in which it is explained that the company requires a written request and proof of identification. The address of the data protection officer, located in the UK, is also provided. They also mention the administration fee, but do not specify how much this is, nor the waiting periods for the replies. Thus in order to make a complete request, one has to contact them beforehand in order to know about the exact fee, as without it, one will probably not get the access to data. Still – due to the information including the mail address of the data protection officer – the practice of this company is a good example of how to inform the citizens in an extensive, but not misleading way.

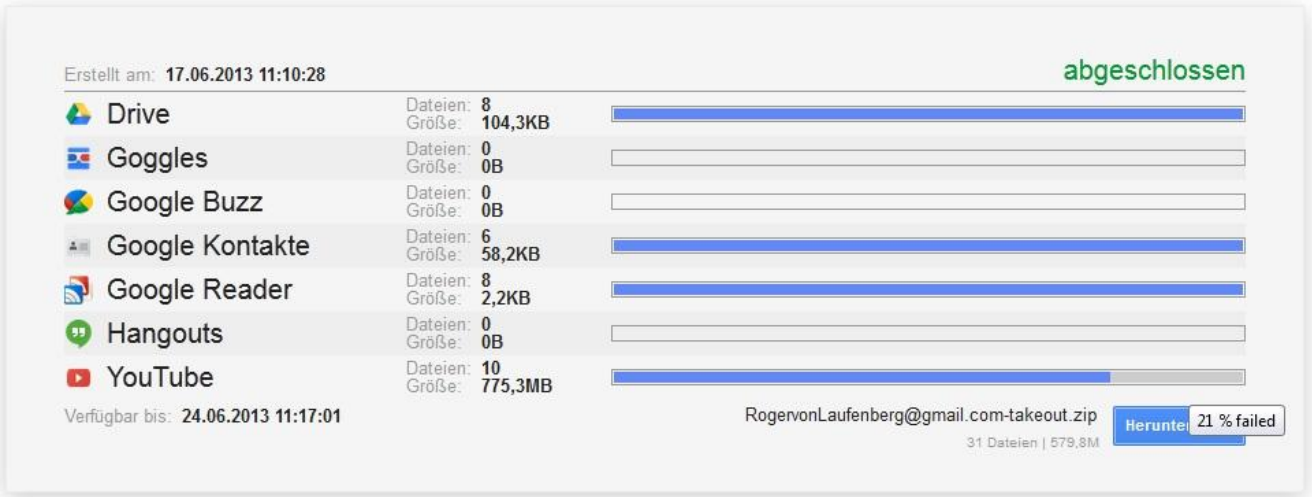
More or less good practices at a national level were demonstrated by the national bank owned by the Luxembourgish government – and by the (private) postal and telecommunications services in Luxembourg. For both sites, the contact details were available on the website and they informed about the written request and the necessary proof of identification. As in Luxembourg requests are free of charge, the absence of a fee was not mentioned in the privacy policies. But they also didn't mention any waiting periods, which may be a result of the vague description of those waiting periods by the national data protection law. They also fail to mention what data is processed by their data controllers, nor specify direct contact details for the data controller, instead instructing users to send requests to the general

[38] http://www.interpol.int/About-INTERPOL/Structure-and-governance/CCF/FAQs (Accessed 30 July 2013).

company address. Still those two sites were identified to be reasonably good practice on a national level.

Bad practice

Similar to the best/good practice examples above, a distinction between national and international sites has to be made here, due to the general gap between both regarding their data protection principles. On the international level, some bad practice cases were found in this research, especially with large internet organisations such as Google and Facebook. Generally speaking, the legal sections are found quickly on their homepages and the information they provide is extensive. Over the length of several pages, users are informed about all the different kinds of data they process and store, how they collect the data, why they process the data and with whom they share it. But regarding the right to access the data, users are informed about their right but not how to exert it – like in the case of Google. Even a more extensive search of the Google Inc. legal section doesn't answer how the right to access can be exerted. Google provides registered users the possibility to access their data when logging in to their dashboard[39] – an overview of all the Google services which provides a breakdown of which of these services are used by the user. Here one can, according to Google, download the personal data processed by Google. However, only a selection of the available Google services from the dashboard is included in the download.[40]



So already here part of my data is not accessible, primarily most of my e-mail data except for my contacts. As Google is also one of my search engines, part of my web history is also stored by Google Inc. So every time I search something on Google – as a registered user – this is processed and stored by them and I should have a right to access that data. As already mentioned above, since Google Inc. doesn't inform users about how to make subject access requests in the case of the web history, the user has to click through several other legal sections of Google in order to get some more information. In this case the necessary (but still incomplete) information is found on the 'Privacy Troubleshoot' section, where registered users are able to view their web history processed by Google[41]. Here, neither an option to

[39] https://www.google.com/settings/dashboard Accessed 07 May 2014
[40] For my personal Google account, there are 14 Google Services listed in the dashboard, from which I can download only 7.
[41] http://google.com/history Accessed 07 May 2014

download your personal data, nor the address of the data controller is available, thus making a subject access request impossible.

When contacting Google Inc. by e-mail and requesting the contact details for the data controller, standardised replies are sent by Google, referring back to the data protection principles of the legal section on their website and the possibility to download the data via the Google dashboard tool, thus completely ignoring the initial request for the contact details. Replying to those e-mails and the sending of new e-mails remained unanswered – thus no contact details were provided and a subject access request is not possible. This strategy of denial by Google may be seen as a deliberate obstructing of the access to personal data and thus is evidently a bad practice.

A similar practice was undertaken by Facebook also, with the same strategy: providing a huge amount of information but leaving out the essential points, like the right to access the personal data and the data controllers contact details. After some more research, the possibility to download your data is mentioned but here again, not all my data is included[42]. When sending e-mails, standardised replies are sent back, ignoring the initial request – any further e-mails remain unanswered. Here again, simply by deliberately ignoring my requests, I am not able to exercise my right of access, which clearly is a bad practice regarding the provision of information.

By contrast on the national level, the bad practices – documented at public as well at private sites – were of a different nature. Often the main difficulty was obtaining any information whatsoever about data protection protocols, like for example at the public agency responsible for driving licences records in Luxembourg. Even after 20 minutes of research on their website, there was no information regarding the data controller and/or data protection, making it necessary to send an e-mail to the general e-mail address. The answer remained unsatisfying, neither contact details were provided, or any other information, except that the only information they hold about me are those I supplied upon registering for my driving licences. My question about how to access my personal data remained unanswered. This is especially concerning given the wide coverage of this type of database – namely all driving licence owners in Luxemburg.

Similar experiences were found with other national sites. School records as well as the national patient health record had no legal sections on their websites and as such no information about their privacy policies was available. For the latter, a new electronic health records system is being introduced which is at the moment in the testing phase and won't be ready until 2014.[43] The process is monitored by the CNPD in order to grant the patients data protection rights.

Three especially bad practices examples – concerning sensitive data – were documented when locating the data controller of my patient health record. On the one hand, for the local patient health record – the researched site was the local dentist – after asking on the phone, my access to my patient health record was obstructed and the member of staff explained to me that I could only have a copy of my dental X-ray but not of my health record. However as she was unsure, she also asked the dentist himself, who confirmed her statement. So I got

[42] According to europe-v-facebook.org, the download form only gives the user 29% of his personal data processed by Facebook. (http://www.europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html Accessed 01 August 2013).

[43] http://www.mss.public.lu/publications/infoletter/index.html Accessed 31 July 2013.

from both the assistant and my dentist the denial of my right to access, as a result of an evident lack of knowledge, obstructing the access to my patient health data. Beside the access to the CCTV records described below, this was the only site where I was personally told that I had no right to access my personal data. The other extreme was documented on the other hand by the hospital, the 'centre hospitalier du nord', already described above. It was sufficient to simply write an e-mail with my name, my Luxembourgish and my Viennese address to obtain a copy of my patient records including a CD with my X-Rays. The lack of knowledge of data protection principles, in this case not asking for any proof of identity, allows for a potential abuse of personal data. Since the personal data in question is sensitive data, it is even more important to be informed about how to process this data and how to handle subject access requests, in order to neither obstruct, nor carelessly allowing the access to data.

The third example was especially double edged, where partly good practice but also bad practice was demonstrated by the Police. Although the privacy policy on their website is not really informative, they nevertheless mention the right of access to data and include a contact e-mail address. After contacting them asking about how to proceed to access my data held by the Police, I received a first reply five days later clarifying the process. The email explained that on the one hand, I could access the data I may have entered on their website (which is what the legal section on their website was intended to cover). In this case I simply would need to write a request to the director of the police. On the other hand, if I want to be informed of my police records – thus my data processed in their documents, I would need to write a request to the state prosecutor, but they could also transfer my request immediately to the designated supervisory authority. After sending a further email to ask for clarification, I was also given the address to which I could send my access request and the confirmation of the transmission of my request to the supervisory authority. So whilst the initial information provided on the website was not very helpful, the personal contact was marked by a high level of expertise, providing me with some of the necessary information. Since this case was one of the few examples, where the communication was characterised by a high level of expertise, this may be seen as good practice. However, since I was forced to actively search for the contact details, only the communication itself was good practice. It would have been better to inform the citizen beforehand on the website of the police, without having to search for it and write some emails.

Reinforcing the bad practice described above was the way the designated supervisory authority handled my request (which was forwarded by the director of international relations at the Police). Although I only mentioned in my initial e-mail that I wished to access my police records and thus needed the contact details of the data controller and only stated my name, one month later I received a letter from the prosecutor. The letter didn't contain my full police records but still mentioned the two recordings in my police records from 2005 and 2009 with specifications in what connections those entries were made. The letter also mentioned that there is no processing of my data in the Schengen and in the Interpol database. It also stated that upon request I could get the copies of the records. All this sensitive data was sent to me, without any proof of identity of my part, not even further specifications upon my person except for my name. This was thus the second case, where I was permitted far too easily and with minimal security checks to access to my data. Both cases of course involved especially sensitive data.

Other bad practices were experienced because some of the websites from the researched national sites had a legal section but sometimes no data protection section, or just simply

stated that their data protection principles comply with the Law of 2 August 2002 – the national data protection law.[44] Thus again, further research was necessary such as writing e-mails or making phone calls. This is insofar a bad practice, as it hinders the request for access, by essentially forcing the citizen to write e-mails and wait for answers, delaying the possibility to write the request and thus also the access to data.

Direct interaction – in person or by phone – with staff members was mostly characterised by a lack of knowledge, providing me most of the time with misleading information, such as that I was not entitled to get the requested information as described in the section of CCTV below and also when contacting my local dentist for my patient health records as outlined above. Especially for the right of access to CCTV data, most of the staff I contacted were rather suspicious, asking about the reason I would want to access my data and informing me that CCTV data is only available for the police when a crime has been committed. This even happened when I was redirected to the responsible person of the CCTV system and thus (in theory) an informed/expert person. Communication through e-mail didn't show this kind of lack of knowledge, but here the problem was more the long waiting times in order to get a reply of the request for information, or even to get a reply at all.

CCTV and signage

The experience of this research found that in Luxembourg, CCTV signage not only provides little information, but is also in some cases hard to locate. Especially in private sectors, the signage was not easily visible, thus failing in its singular purpose to inform about on-going CCTV surveillance. This occurred on visited sites like the large department store, where in the shopping centre as well as in the supermarket CCTV was present but the signage not. This research site presented in its whole a really bad practice, concerning the information provided and the access to data. First, only after contacting a member of staff and being redirected to the security guard, was I shown the signage, hanging in a corner with the view blocked by a poster and a box. The signage informed only about CCTV recording in progress – in English, French and German – and a telephone number for further information was provided, which led to the call centre of the company.

Here the security guard was suspicious and doubtful regarding my request for information. I was told that only the police have the right to access the data and only in case of an incident. Shortly after, he told me that they do some investigations beforehand themselves and check for strange things happening in the store. Since I was unsatisfied with the information, I tried calling the call centre. Here I was redirected immediately to the head of security department of the store. Again, it was explained, with a general suspicion, that I don't have the permission to access my data recorded by the CCTV and that only the police have the right to access the data. The head of security assured me that the CCTV has been authorized and thus is legal, but he could not, or did not want to give me further information about the CCTV processing. He told me that the data protection law was 'probably available at the national data protection office' if I would want more information. Again not satisfied with the reply I got, I contacted the store again, this time by e-mail. Here, I got a reply within a few hours with the necessary mail address – but no further information on how to make the request and what to include, nor what waiting periods I could encounter. Thus on all the three levels

[44] For example on the website of the green party, there is a small section stating: '*Your personal data is processed with the highest confidentiality by the bodies of* 'déi greng*' and will not be shared with others. (cf. law relating to the Protection of Persons with regard to the Processing of Personal Data, 02.08.2002, http://www.cnpd.lu/)*' http://www.greng.lu/demande-dinscription Accessed 29.08.2013.

where I tried to approach them, I was not only given wrong or insufficient information but also twice denied my access right, even from an employee who should have the necessary knowledge of the data protection principles.

In the remaining CCTV sites – CCTV in a transport setting, public space, local store and bank – CCTV signage was clearly visible, often with more than one sign on the premises, informing about on-going CCTV surveillance and in some cases stating the purpose of safety. All the signs were at least bilingual in French and German, in some cases also in English, but further details, especially contact details or phone numbers are rarely provided. So it was necessary to do some extra research, by asking staff members or checking on the website, to get more information in order to be able to access the data. None of the visited sites in the private sector used template forms for their signage, but at least it seems to be a general practice to state on the signage the authorisation reference number of the CCTV by the national data protection agency, the 'commission nationale pour la protection des données' (CNPD) (see Pictures 1 and 2 below). This unique authorisation number is given to CCTV systems which have been approved by the CNPD and simplifies the search for the data controller in the national register should anyone wish to search for the data controller in this way. Although the intention of informing the citizens about the authorisation is good – as the national register should contain the contact details of the data controller as well as information about the data processing – it implies prior knowledge on behalf of the citizen of the CNPD and the national register. Two examples of this practice can be seen on the pictures below, the first one at an international bank, the second one at a local supermarket. It should also be noted that the second signage, that of the local store, is a self-made sign, not using any template and misspelling the German term 'Videoüberwachung'.

Pictures 1 & 2: CCTV signage including CNPD authorisation number (blanked out of picture)

As for the signage in public spaces, a high level of information is provided, all following the same template. But crucially, the signage still fails to provide the contact details of the data controller, as shown in Pictures 3 and 4 below. It is clearly visible who is in charge of the CCTV and for what purpose the data is collected. Those two sites showed the best practice of all the visited CCTV sites, providing the most information, but still missing the contact details. Picture 3 informs the citizens of CCTV on the train station in Luxembourg City,

while Picture 4 informs citizens about CCTV in one of the four "security areas"[45] in Luxembourg City which is operated by the police.

Pictures 3 & 4: Lack of contact details in CCTV signage

As I was already in contact with the director of international relations at the Grand Ducal Police for the access to my police records, I only needed to ask if the address I was given is also responsible for the treatment of the CCTV data, which was confirmed shortly after. But if I hadn't already been in contact with the director of international relations, the research for the contact details would have been much more difficult. On the internet sites of the Grand Ducal Police and of the Police Inspectorate, there is only little information about the CCTV in these security areas and no information at all about access rights regarding this data. So here the same procedure as for the police records would have been necessary, thus contacting the police through a general e-mail address and asking for the contact details.

The same procedure was necessary for finding the contact details for the national railway company, as there was no information available at the train station. On the internet site in the legal section, a large paragraph concerning the protection of personal data is available. Although there is no mailing address provided, they advise citizens to write an e-mail requesting access to personal data. Here also, the information is mainly for the general access to personal data shared on the website of the company and does not mention the possibility of accessing the CCTV data. To date, after sending two e-mails and waiting more than a month, my request remained unanswered. A similar approach was experienced while requesting the contact details of the data controller at the national bank. As the signage provides only little information and no telephone number, it was necessary to search on the website. The legal notice on the homepage also covers the personal data, but doesn't specify how to access the data. So again, an e-mail needed to be send, which similar to the CFL remained unanswered for one month. After sending a second e-mail, where I expressly declared that I wish to know the contact details of the data controller, I got a reply from corporate compliance, stating: *'*[…] *For safety reasons of the clients and employees, our cashpoints are under CCTV surveillance. The CCTV has been approved by the national data protection office, qualified for such cases.* […] *A signage on the cashpoint informs about the CCTV.* […]' Again, my

[45] The security areas are legally described as 'any place to which the public has access that by its nature, location, configuration or frequentation presents a greater risk of criminal offences being committed' (the Law of 2 August 2002). Currently there are four security areas in Luxembourg City, three in the city centre and one around the 'stade Josy Barthel' – the national football stadium. These security areas are processed by the grand-ducal police of Luxembourg.

initial request was ignored, as I did not get the contact details or any other information as how to access my personal data. Not satisfied I wrote a third time, quoting the corresponding legal sections of the Law of 2 August 2002 and asking – *again* – to provide me with the contact details of the data controller. My question was ignored a third time, now with the argument that the CCTV footage is only stored for 30 days and thus the footage of me at the ATM is not available anymore. The deliberate ignoring of my question for the contact details of their data controller, first by not answering at all, then by not answering to my question, showed a particular bad practice and appeared to intentionally block my right to access to my personal data.

Concluding thoughts

Generally speaking, the researched sites as part of this task appear to show several faults, making the possibility of a citizen submitting a subject access request somewhat difficult. Especially for the national sites in Luxembourg, some extra effort is necessary to get the information one expects to get beforehand already, like 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 the information, enough information to actually make a subject access request is seldom available. Only two of the international sites provided (except for the exact waiting periods) all the necessary information and made this information easy to find as well as presenting it in an intelligible way. Good practice like this is missing on a national level; best/good practices in Luxembourg are thus not fully comparable with the practices by international organisations such as Interpol or the online gaming company. On the other hand the bad practices of the big online companies, making their profit with the personal data of the users but hindering the subject access request is very frustrating and endangers data protection principles if these practices are imitated by other organisations. These practices could not be documented at a national level, except perhaps for the national bank, where my right to access personal data also seemed to be deliberate obstructed.

The lack of expertise was probably one of the biggest difficulties concerning the data protection principles and the right to access data on a national level. A lot of people upon contacting them didn't know how to handle these requests (e. g. with my local health records) and therefore gave me the wrong information. The careless handling with my sensitive data (both times from important public organisations) also indicates a significant lack of knowledge in those sectors, where one would expect people with a high level of expertise. Still, this only refers to the experienced sites and doesn't claim to cover all the area in Luxembourg.

The CCTV signage in Luxembourg showed a similar trend as the other national sites, where practices like displaying the national CNPD authorisation numbers are a good intention, but where the effect of informing the citizen has to be questioned alongside the general lack of knowledge of the members of staff. This can result in the potential misleading of citizens and show a lack of interest in data protection principles. Due to the reaction of most of the contacted staff members – by e-mail, phone or in person – one can infer that enquiries regarding the access to personal data are not very common in Luxembourg and thus members of staff did not have the requisite expertise and/or knowledge to deal with them accurately.

SUBMITTING ACCESS REQUESTS IN LUXEMBOURG

Introduction

In this country report, the practice of accessing personal data in Luxembourg is shown by making subject access requests to a range of public and private organisations, situated in Luxembourg but also for international organisations like Interpol and Google.

The analysis covers a wide range of different sites and thus gives an overview of how those requests are treated and what kind of problems citizens might encounter when trying to access their personal data. Since this research is based on different examples, it doesn't claim to cover all the organisations and different practices which might be encountered in other organisations.

Overall Summary

Methodological thoughts

While for most of the non-CCTV sites the choice of the site depended on which might hold data about the researcher or which were easiest to reach, the choice for the CCTV cases was made methodologically. By choosing a central point in the city and taking the closest sites to it, a random sample could be generated. For Luxembourg, the research was started at the 'Place du glacis', the central public parking area, and 'centre Hamilius – rue Aldringen', the central bus stop in Luxembourg City, both equipped with a public CCTV system. From this point in the city the other sites were sampled and documented.

A main issue for the CCTV cases and which probably had the biggest impact on the CCTV data was the distance between the researcher, situated in Vienna and the research field being in Luxembourg. Although part of the research, like visiting the sites had been conducted in Luxembourg, the subject access requests were sent from Vienna creating a time lag due to which some CCTV footage was already deleted. This was especially the case when the data controllers needed further clarification concerning the requests which necessitated more exchange of correspondences and thus a greater period of time before requests could be processed.

Methodological attention also needs to be given to the lack of clarity in the wording in the legal text of the data protection law in Luxembourg – the 'Law of 2 August 2002'[46]. There is a crucial point in the legal text, which had a big impact on how the subject access requests were treated in this research. As the Law of 2 August 2002 does not give a precise timeframe within which the data controllers have to respond to the requests, this resulted in excessive waiting times of up to 75 days between the date of sending the requests and getting an answer, excluding the acknowledgement of the request being processed. In order to have a clearer frame and a better planning of the research, a maximum waiting period of 40 days was agreed between the researcher and the project management team – similar to other countries' waiting periods.

Another methodological issue concerned the language used in correspondences with data controllers. Since Luxembourg officially is trilingual – French, German and Luxembourgian – I could've theoretically sent the national requests in all three languages. But as French is

[46] A detailed outline about the data protection law won't be provided here as this is already available in the legal analysis at the beginning of this report.

the common language in administrative issues, I also used this in my subject access requests. This was not only applied in the national requests but also in the international requests, a practice used by all the partners writing the international requests in their native tongue.

General overview and emerging trends

In total 19 requests have been sent to different organisations of which only four were returned completed within the timeframe. 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, I received in total six *complete* answers, where my personal data was disclosed and all my questions answered satisfactory.

	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

	Public/Private	**Site**
15	Private	Twitter
16	Private	Amazon
17	Private	Facebook Ireland Ltd.
18	Private	Microsoft
19	Private	Google

The highest success rate of the disclosure of data has been achieved for CCTV sites. Although no organisation sent me the actual CCTV footage, I was granted the right to visit the site and view my footage. The main concern regarding CCTV footage in general was the risk of infringement of third parties' privacy, which was stated in some cases. Other concerns and reasons for denial of access were security reasons and vague and unclear legal interpretations, as some organisations (deliberately (?)) misinterpreted the legal ruling concerning the right of access to data. A special case of access to CCTV data has been 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.[47]

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 have to collect the different kind of information necessary to submit the subject access requests. As described in the Locating the Data Controller country report, especially on a national level, the information provided by data controllers concerning how to make a subject access request isn't extensive enough for lay citizens to easily access their data. For instance, there are no templates via which to write access requests – neither on the website of the different sites, nor on the website of the CNPD – and there is often also no real information about whom to address to send a request. This meant that I had to send several requests to the general company addresses with instructions to forward the request to the data controller within the organisation. While no replies have been received from organisations explicitly admitting not knowing how to handle such requests or not knowing to whom they should forward them, some requests sent to general company addresses have remained completely unanswered to date. A lot of time and effort for the data subject could be spared if all contact information and guidance on how to make a request would be available beforehand, either on the specific homepages of the organisations or in the national register of the CNPD – which essentially is the purpose of the national register in the first place.

[47] See the legal analysis report of Luxembourg for the legal regulations and the CCTV section of this report a detailled describtion of the role of the authority of control regarding subject access requests.

Due to the absence of templates, it at times 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, first instance answers provided satisfactory information without the need for extra requests. Most cases needed clarifications after the first instance, 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 which might be a sign that data controllers only seldom handle subject access requests and in any case treat such requests with a low level of priority and importance. A general trend in the response of data controllers, especially for the CCTV sites, was the justification that the surveillance sought to ensure the safety of those visiting the sites in which CCTV is used. Moreover, data controllers often simply referred to the CNPD authorisation number[48] of the CCTV and the presence of the CCTV system in the national register as justification for its deployment. Although in none of my subject access requests the legitimacy of the data processing was questioned, it seems as if a lot of data controllers interpreted my request and my questions about data processing as such.

Involvement in the research also manifested in multiple Google searches for my name from Luxembourg quite shortly after sending the subject access requests at the end of September 2013. As I have an academia.edu profile, the Google-searches linking to my profile also showed up on my academia profile, making it possible to trace the search back to the origin of the IP-address, in those cases to Luxembourg. As Figure 1 shows below, prior to making the requests, there were no searches. After the 10th of October 2013 the searches ceased (only one other access from Luxembourg can be dated to the 13.11.2013).

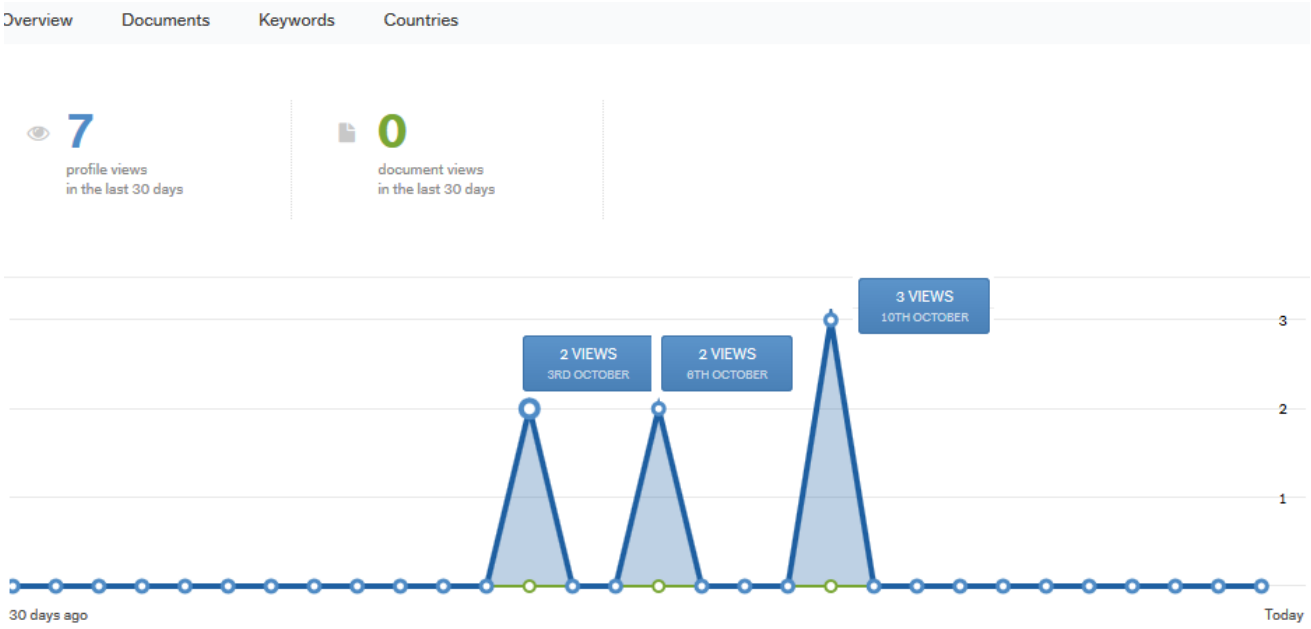
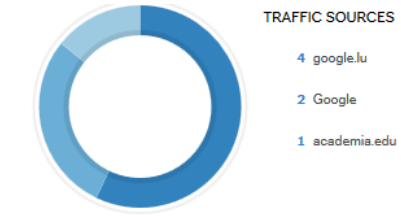


Fig.1: Access on my academia.edu profile in October 2013 - https://univie.academia.edu/RogervonLaufenberg

[48] 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.



RECENT VIEWS

Time / Date	Visitor ID	Page	Refering Site	Keyword	City	Country
10:23 11 Oct	4	Profile	google.com/search?q=&start=0			
10:23 11 Oct	4	Profile	univie.academia.edu/RogervonLaufenberg			
10:21 11 Oct	4	Profile	google.com/search?q=&start=0			
14:58 07 Oct	3	Profile	Google		Hesperange	
14:57 07 Oct	3	Profile	Google		Hesperange	
12:28 04 Oct	2	Profile	google.com/search?q=&start=0			
07:21 04 Oct	2	Profile	google.com/search?q=&start=0			

Luxembourg

Fig.2: Origin of the access on my academia.edu profile - The visitor ID indicates three different users all based in Luxembourg.

Thus one can infer that the subject access requests raised a suspicion or curiosity and some data controllers evidently wished to know a little bit more about the person behind the request. Another case in which this happened was as part of requesting data from two airlines companies. Since several similar requests were sent to the company's data controller by the other consortium partners, the privacy officer of one of the companies discovered our status as researchers for the IRISS project and invited us to a meeting to discuss further details. Despite the revelation, it was insisted that our access request should be handled as a normal request since the right of access is one which is afforded to all data subjects, regardless of academic or other background.

Another problem arose with one part of the legal text concerning the access right, which led multiple times to complications and delays during the request for data. The Art. 28 of 'the Law of 2 August 2002' states that: *"the data subject or his beneficiaries*[49] *who can prove they have a legitimate interest may obtain (...)."* Some of the data controllers 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.

Quantitative data

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%)

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

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*	10 of 13 incomplete cases
Of which no information about third-party sharing*	11 of 13 incomplete cases
Of which no information about automatic decision making*	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

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

Case by case analysis

Public – Facilitative practices

Interpol

The request sent to Interpol was probably the best treated case of all. Being the only site providing an extensive explanation concerning the subject access request and including a template, sending the request itself was easy and quickly done. I sent my request on 06/09/13 to the commission for the Control of INTERPOL's Files (CCF) in Lyon, including a proof of identity in form of a scan of my passport. Although I didn't receive an acknowledgement of receipt, a reply from the CCF was sent back on 06/10/13, 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 me *"that the appropriate checks have been carried out and that there is no information to disclose that is applicable*" to my request.

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

The disclosure of my police records was handled by the authority of control – similar to the open street CCTV. Upon identifying the data controller, part of my records were already sent to me[50], a second request disclosed the remainder of my records – although according to the authority, *"the transmission of the records isn't obliged by the Law of 2 August 2002, but is done with the agreement of the prosecutor (…)."* My records haven't been shared with third parties – including Europol – and regarding the automatic decision making, as the authority isn't the data processor, they can't make any comment about that matter.[51]

Local Authority

[50] For more information, see the Locating the Data Controller country report above.
[51] A more detailed description of 'problems' of the authority of control will be addressed in the CCTV section – open street CCTV.

My request was processed by the municipality within three weeks, disclosing the personal data file they hold about me in their system and confirming that none of the data is communicated with third parties. Unfortunately my questions regarding the automatic decision making was not answered. Due to time constraints within the project, a follow up of this case was not possible and thus remained unanswered.

Public – Restrictive practices

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 my personal data in relation with my vehicle and driving licensing at the 'Société Nationale de Circulation Automobile' (SNCA). Trying to obtain any information whatsoever about the processing of my personal data and who to send the subject access request to remained unsuccessful, despite sending several mails.[52] After getting no information beforehand, I had to try to direct my request haphazardly to the SNCA. On 25/09/13, I sent my request with a copy of my passport. Although for the research I set a necessary response time of 40 days, I got no answer for two month (64 days).

Thus on 28/11/13, I sent a second letter, stressing that they had exceeded the time limit largely and that if I didn't receive a reply within the next 7 days I would file an official complaint to the national data protection commission, the CNPD. This threat triggered a reaction from the SNCA, although not the desired one. On 09/12/13 a reply was received, referring to my initial request from 25/09/13 without mentioning any delays. Although they confirmed my presence in two of their databases[53], they were not able to disclose my 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, which was reflected in the ignoring of my first request. Although we do not know the amount of subject access requests the SNCA receives, they still should be able to handle individual requests like all the other sites. Indeed, this was the only site in the Luxembourgish research which responded that the request could not be handled at all.

In order to grant me my right of access to data however, they gave me the possibility, upon arrangement, to visit them in person at their office so I could – jointly with one of their experts – have a look myself in the databases for my personal data. According to their letter, the time spent by their expert showing me my 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."*

[52] For a more detailed description see the Locating the Data Controller country report above.

[53] 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.

Giving me the possibility to personally check the databases together with one of their experts may be an attempt to try to grant me access to my personal data, but several of the above mentioned points show a very restrictive practice in the disclosure of personal data. Firstly by not answering my initial request, I was forced to send a second request, causing a long delay and additional postage costs. The way my request was handled after my complaint about the delay was not courteous at all, and I 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 2 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[54] *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"*[55]

Due to the above mentioned reasons, particularly the noncompliance with data protection law, an official complaint has been sent to the national data protection authority, which unfortunately remained unanswered until now.

<u>Private – Facilitative Practices</u>

Bank Records

The clearest and most complete response was obtained for my banking records without the need of to and fro sending of mails. 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 requiring me 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 on 24/09/13 to the general office of the bank in Luxembourg City, where it was processed by the legal and litigation services of the bank. A few weeks earlier

[54] 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.

[55] (cf. http://www.mt.public.lu/formulaires/circulation_routiere/immatriculation_controle_technique/ Accessed 27.01.2014).

(on 03/09/13) I'd already sent a request to the bank for my CCTV footage[56] which was also processed by the legal and litigation services, so there had been some cross-referencing in the communication. The reply to my request for my banking records followed on 11/10/13, thus largely within the delay of 40 days.

The response I received was detailed and it was obvious that the data controller was anxious to provide me the requested information. The communication was very respectful – which wasn't the case for all answers I received. The only critique might be that they pointed out twice that I initially entrusted them my personal data at the moment I 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 me in the first place who provided them my data, thus questioning why I'd want to have information about it afterwards. This is only an assumption based on the lack of trust and understanding which I encountered in general during my research in Luxembourg.

The actual personal data they sent me was by far the most elaborate I received from all the national sites. Annexing their reply on my request they sent me a printed 50 page file, starting from my first deposit account in 1993 to the renewal of my bank account in 2011. The received data was clear to understand and seemed complete – although this can't be confirmed for sure as it is almost impossible to know if they process further information. The large amount of data results also from the 21 years of the company being my bank, a period of time where a lot of personal data can be collected.

Alongside this extensive disclosure of personal data, I also got information concerning data sharing with third parties and automated decision making processes. For the first part, it was stressed that for the functioning of my credit card, it was necessary for the bank to communicate my 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 my data was already addressed at length in the reply I obtained concerning the CCTV data on 25/09/13. It was explained that regarding my 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 amount 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. Some improvements might still be necessary, especially by

[56] This case was a bit more complicated as the disclosure of data was not granted and thus shouldn't be dealt with in this section. See more information below in the CCTV section of the report.

informing the data subject beforehand and providing enough information about how to submit a subject access requests.

Microsoft

Of all the multinational private organisations, Microsoft disclosed the most information compared with the other sites. As I have a Microsoft Hotmail (now outlook.com) account since 2002, there should be a lot of data stored by Microsoft. Starting with the search for the Microsoft data controller, the necessary information can be found relatively quickly on their homepage in the section: '*privacy statement'*.[57] Here, Microsoft informs the user about the different ways of accessing the 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*"[58].

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, in the privacy statement as a last point – '*Other Important Privacy Information'* – Microsoft 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 upon three clicks and after a little bit more than five minutes, the address of Microsoft Luxembourg could be found on their homepage[59]. In general therefore, the privacy section – although extensive – is lucid and comprehensible.

My subject access request was sent on 17/10/13 and on 12/11/13 I was asked to confirm my request through email, upon which the investigation of my request was assured. One detailed response was received through email on 10/12/13 and 11/12/13 with the disclosure of my data downloadable on SkyDrive. Similar to the communication with Esprit, although my request was sent in French, the responses I obtained have all been in English – presuming that the data subject understands it. This is insofar interesting as they seemed to understand fully the request and all the details I asked them, as in their response from 10/12/13 they addressed all the points and questions from my request. On a positive note, a second similar answer from Microsoft was received on 06/01/14 by mail, this time in French – for the largest part a translation of the previously received English response and where necessary, some more information and references to the different sections of the privacy statement and products of Microsoft.

Content-wise, although all my questions were addressed, not all of the responses were satisfying. The disclosure of my data was extensive, including headers of my emails dating back to 2007 as well as IP-logging for a period of one year. For my data concerning the conversation with the *'Live Messenger'* I was advised to access it through the site profile.live.com. Automatic decision making in regard with my personal data could not be identified, the same goes for further personal data Microsoft might hold about me. However,

[57] http://www.microsoft.com/privacystatement/en-gb/core/default.aspx for the English (UK) section, or http://www.microsoft.com/privacystatement/fr-lu/core/default.aspx for the French (Luxembourg) section of the privacy statement. (Accessed 26.03.2014).
[58] http://www.microsoft.com/privacystatement/en-gb/core/default.aspx (Accessed 26.03.2014)
[59] http://www.microsoft.com/en-us/contact_fr-lu.aspx (Accessed 26.03.2014)

for the sharing of my personal no specific answer was given to me, except for a reference to the privacy statement.

Thus all in all, the response I 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, but it would be better if the communication would have been in the language of the requester from the beginning. Furthermore the data controller showed an evasive practice concerning the third party sharing – a crucial point regarding data protection. Compared to other similar sites like Facebook and Google, 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.

Amazon

The data controller of Amazon, represented by the legal department answered exactly within 40 days of the submission of my subject access request – disclosing my personal data from my amazon.fr, amazon.de and amazon.co.uk accounts, but not from the US/global account amazon.com. So although it is possible to access amazon.com from almost everywhere in the world and also shop there, legally a separation seems to be done between the European and the US department of Amazon. Since the disclosure of my personal data contained some sensitive data, like my credit card information, the encrypted CD-ROM which contained my data was sent separately from the passwords, which presents a good practice regarding the security of data in comparison to, for example my health data from the 'centre hospitalier du nord'.[60] 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 access to my personal data – as I had asked in my request. Further, according to their response, automated decision making is not used by Amazon, which since it can't be proved otherwise, has to be accepted 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

My request to Twitter was sent on 17/10/13 via mail to the Twitter headquarters in the US, upon which I received an e-mail to confirm my request on 26/11/13 and three days later another e-mail with a ZIP-file attached, disclosing my personal data. My 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 I used. The Twitter legal department also informed me that none of my data has been disclosed to law enforcement agencies, but did not provide me any information about other third party sharing and automatic decision making and thus was also not complete. Also the response was in English although my subject access request was, like for all the other sites, in French. This case remained incomplete, due to a shortage of time within the project.

<u>Private – Restrictive Practices</u>

Mobile Phone Carrier

[60] See Locating the Data Controller country report.

While requesting my personal data processed by my 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[61] for all organisations who registered their data processing – with the goal to inform citizens and make access easier – I 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 I sent my request to the indicated address on 25/09/13, asking for my personal data, including my communication details. As I got no reply at all, a reminder was sent on 28/11/13, indicating that the delay had been exceeded and if no reply was received within 7 days, an official complaint would be made to the CNPD. Since this letter also remained unanswered, I sent an official complaint to the CNPD.

On 24/01/14, my reminder from 28/11/13 was sent back to me 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, making it more complicated for citizens to obtain the necessary information to access their data and thus defeating the initial goal of the CNPD's register. Still it seems strange that my first request, sent to the same address, wasn't sent back but simply remained unanswered.

Probably as a reaction to the complaint I sent to the CNPD, the company finally issued me an answer with the disclosure of my data on 20/02/2014, although the letter itself only arrived two to three weeks later. Although the data controller does not mention any connection to my complaint sent to the CNPD, he apologises for the delay. The disclosure of my personal data was very complete, including personal as well as technical details such as my unique identifier corresponding to my home address, 'disability'[62] settings and 'Roam-NoSMS'[63] settings. Especially for the last two technical settings, I didn't know those were possible, as this wasn't communicated to me when subscribing to Tango Mobile S.A. and thus shows the importance of the access to personal data as a form of providing information.

Another important information I and also the company discovered due to the disclosure of my personal data was that upon subscription, the salesman had written my name wrong – instead of **von** Laufenberg, he had written **van** Laufenberg – which would have been of no big importance if he hadn't also written **van** Laufenberg for my email-address used for the sending of my bills and for my bank account for the direct debit authorisation. Thus I received no bills and my bank never authorised the direct debit due to this. Following my access request therefore, the data controller amended its records upon comparing the personal data I provided with my subject access request and the existing information held about me.

[61] http://www.cnpd.public.lu/fr/registre/index.html Accessed 27.01.2014.
[62] 'Disability' settings relate to whether the user does or does not want to receive welcoming SMS when in roaming mode.
[63] 'Roam-NoSMS' settings relate to whether the user does or does not want to receive SMS when in roaming mode.

Furthermore the data controller provided me information about third party sharing, which mainly included a printing company, an external call centre which has access to all my personal data, as well as their bank, but without specifically mentioning anyone of them. As for automated decision making, the data controller advised that my 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 crucial 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 being unsure whether a request has been received or not. On the other hand, this case also shows one of the reasons why access to personal data is an important right and needs to be granted, as it is a necessary step for the correction of wrongly processed personal data.

Loyalty Card (department store)

Another interesting, restrictive case could be observed when trying to access my personal data stored by a department store in relation to my loyalty card. Since I didn't have such a card in the first place, I applied for the loyalty card program when buying some clothes in their shop in Luxembourg City. A few weeks later in order to be able to send the access request, I searched for the contact details on the homepage of the company's loyalty card scheme. The privacy statement of the company's homepage, only available in English, didn't 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 on 17/10/13, I sent my request and got a reply by e-mail on 05/11/13. Although my initial request was sent in French, the reply was in German stating that they couldn't find me in their system and that for my loyalty card number no personal data was available. As such, they couldn't proceed with my request. They asked me to check my information again and that I could come back to them at any time for further questions. Even though they replied in a respectful manner, the use of German was illogical and can be considered as a way of restricting the citizen's access to personal data. Moreover, it seemed to demonstrate a certain procedural rigidity and inflexibility insofar as failing to reply in French and assuming that I was able to read and understand German. In this case, perhaps only those data subjects capable of speaking German are able to submit an access request.

Nevertheless, I checked if I supplied the correct information and discovered that I simply hadn't completed my online registration after already having filled in the registration form in store. After completing this step, I mailed my new request – again in French – on 19/12/13. The answer arrived promptly a few hours later – again in German – disclosing my name, address, e-mail address and date of birth, but no information about my purchased items and the automated decision making, which was requested in my correspondence to them.

They did however include an answer about third party sharing, advising me that they make use of my personal data only for the loyalty card scheme and don't 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 don’t 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 in the legal department of the company between their official privacy policy 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 service centre my subject access requests denied the use of third party sharing, thus providing misleading information to their customers. Although it can be supposed that this was not a deliberate practise, the misleading communication – including the usage of German – and the missing data in the responses from of the data controller has to be seen as a restrictive way of handling subject access requests. As such, an official complaint has been issued to the CNPD, which is currently treated. To date, the complaint remained unanswered from the CNPD as well as from the company.

Loyalty Cards (air miles)

I sent my 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 my data was processed within less than a week but my questions regarding the third party sharing and automatic decision making weren’t addressed. When contacting the airline a second time and asking them to answer the remaining questions, the status as researcher for the IRISS Project was revealed by the data controller due to the similar requests from other partners. Thereafter, 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

My first mail was sent on 24/09/13 and was unanswered by the airline. Only after I sent a reminder on 28/11/13 was my request was processed. A total of 47 days had passed before I got a first answer. In this response, my flight bookings and my personal data – flight reservations, payment details excluding my 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 my requests.

Facebook

The problems regarding the identification of the data controller have already been described in the above report concerning the location of data controllers’ contact details. My subject access request was sent to Facebook on 17/10/13, sticking closely to the template from europe-v-facebook.org and also requesting details about third party sharing and automatic decision making. Up until now, my request remains unanswered and a complaint has been sent to the CNPD.

Google

My subject access request for Google Inc. was sent on 17/10/13 to the headquarters in the US. An answer was obtained on 04/11/13, mentioning the importance of the data subject’s

control of his personal data online and referring to their download services Google Dashboard and Google Takeout.[64] 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 on 28/11/13 remained unanswered, which led me to send a complaint to the CNPD, which so far also remained unanswered.

CCTV & signage

A wide variety of practices, from very restrictive to accessible practices could be observed in all the steps of accessing the data, from the moment of visiting the site, searching for information regarding signage and the data controller, through to sending the request 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.[65] 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 the access to data. None of the identified signage included a detailed identification of the data controller or any information about the possibility of the subject access requests, although the Law of 2 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 the 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 observed signage could be improved by simple means, such as simply adding one line with the specific contact details of the data controller.

To provide clarification on this issue, more detailed guidance could perhaps be provided from the CNPD, similar to the British Information Commissioner's Office (ICO) which has issued a 'CCTV code of practice' to advise CCTV data controllers of what they may wish to include on signage. This document includes a section about the responsibilities of CCTV operators in regard of informing the data subjects and the right of access to data.[66] The information provided by the CNPD regarding CCTV systems is mainly the one needed to

[64] A description of those services are provided in the Locating the Data Controller country report above. In the meantime, the services have changed slightly: Google Takeout is now responsible for the possibility to download your personal data and further Google Products have been added, although still a lot is missing. Google Dashboard has adopted the function of Google History and thus permits the user to review his search history, but still without the possibility to download any of it.

[65] When visiting the site and despite the large amount of CCTV surveillance, no signage could be identified. Upon contacting the ministry they assured me that five stickers indicating the authorisation number of the CNPD are clearly installed outside on several locations of the ministry. 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, I didn't notice the signage – which makes it questionable if lay people would identify the signage.

[66] Cf. Information Commissioner's Office (2008) CCTV Code of Practice. Chapter 9. Responsibilities, p.15ff, http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf (Accessed 07.03.2014).

issue an application for the installation of a CCTV operating system[67], whereas more detailed information could lead to clearer and better signage which in turn may lead to positive consequences in the form of more informed citizens.

The size of the signage which was observed during this research varied largely from metal signs to a small sticker indicating the video surveillance (cf. Fig. 3 & Fig. 4). 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 Fig. 4 on the entrance door, it is at least in compliance with Article 10 - Processing for supervision purposes, (2)[68] and Article 26 - the data subject's right to information of the Law 2 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, as previously described for the Ministry of Foreign and European Affairs. If the signage in form of a sticker can't 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 German, which proves to be a good practice due to the international setting of Luxembourg City.

Fig. 3 (left): Signage of the CCTV surveillance at the train station in Luxembourg City in French, German and English, including the CNPD authorisation number
Fig. 4 (right): 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)

Case by case analysis

CCTV in a department store

[67] Cf. http://www.cnpd.public.lu/fr/declarer/autorisations/traitements/demande-video/index.html (Accessed 07.03.2014) - Only available in French and German.
[68] "(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)."

Perhaps strangely, the department store holds the same CNPD registration number as the shopping centre within which the store is located). This is despite the two entities being different limited companies.

The already described practice of providing misleading information in the above report on locating data controllers continued throughout the process of the subject access requests. Firstly, upon revisiting the store on 28/09/13, I noticed their newly installed signs informing of the CCTV surveillance. At least at every entrance of the department store, the signage now is clearly visible hanging from the ceiling (cf. Fig. 5). Although it is a big improvement compared to the hidden signage at the earlier stage, 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.[69] 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. Furthermore, signage indicating the CCTV surveillance in the shopping centre couldn't be found during the research, despite the presence of several CCTV cameras. This is insufficient insofar as not every visitor of the shopping centre also visits the department store and thus won't be confronted with the signage installed there. So to resume, although it is an improvement compared to no sign at all, it would be recommended – besides the correction of the erroneous signage – to install further signs at the entrance of the shopping centre, in order to also indicate the CCTV surveillance throughout the shopping centre and to provide contact details of the security manager.

[69] The *'Loi N°95-73 du 21.01.1998 d'orientation et de programmation relative à la sécurité'* in France is one of the laws regulating the surveillance by means of CCTV, more specifically regulating the terms of the installation and usage of the video surveillance systems including the informing of the data subject (cf. http://cecil.resade.1901.org/lececil/spip.php?article45&lang=fr, only available in French (Accessed 10.03.2014)). According to the information brochure about CCTV in commercial surroundings issued by the CNIL (*Commission Nationale de l'Informatique et des Libertés*) – the French data protection office – however, the actual regulation for the video surveillance of spaces open to the public is the code for domestic security (*code de la sécurité intérieur*), more specifically the articles L251-1f., the succession of the by '*Auchan*' mentioned *'Loi N°95-73 du 21.07.1998'* (cf. Vidéosurveillance – Vidéoprotection. Les Commerces. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL_Video_commerce.pdf, only available in French (Accessed 10.03.2014); Code de la sécurité intérieur, Article L251-1. http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000025505406&cidTexte=LEGITEXT000025503132&dateTexte=20120618&fastPos=17&fastReqId=1560864542&oldAction=rechCodeArticle, only available in French (Accessed 10.03.2014).

Fig. 5: New installed 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).

On 01/10/13 I sent my request was by e-mail and postal mail and also addressed the erroneous information on the signage. An answer to my request was received on 14/10/13 from the head of the security department of the shopping centre and department store. In this reply, my right of access was denied with the argument, that *'according to the Article 28 (1) of the Law of 2 August 2002 (…), such a request is subject to a proof of a legitimate interest'* and without such a justification my 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 me 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 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 wasn't adequate, mainly because of the non-disclosure of my personal data and the reason used by the head of security, I sent a second letter on 28/11/2013 asking them for a revision of the answer they provided me. I specified that upon consultation of the Article 28 (1) of the Law of 2 August 2002, '*I don't see a reason to provide a legitimate reason'* for the access to data *'for two reasons: (1) As the data treated by the* (department store) *in regard with the video surveillance, being my personal data and not vice-versa, (2) and furthermore the reference to the legitimate interest in the art. 28 (1) is meant for the beneficiaries of the data subject wanting to access the personal data (…)*. I also stressed that if they still deny my access to data, I would like to obtain an adequate explanation of the reasons of denial, knowing that according to the Article 29 – exceptions to the right of access – the *'controller must state the reason for which he is limiting or deferring exercise of the right of access'* (cf. Art. 29 (4) of the Law of 2 August 2002).

The answer from the company arrived roughly two weeks later on 10/12/13. Compared to the first answer which lacked an official character, the second answer had more the appearance of an official company letter.[70] Content wise however, the second answer didn't differentiate much from the first. Not only was no footage from my visit available anymore due to the automatic deletion of the material, even if the footage was still available, they still wouldn't disclose the requested data, again arguing with the privacy of other 'shopping centre users'. For this reason they would need an adequate reason of my part as to why I should obtain access to my 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 2 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 (deliberate (?)) misinterpretation of the data protection law was the reason for the non-disclosure of my 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, overlooking the whole process from visiting the site, identifying the data controller and accessing the personal data, 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 was incredibly time-consuming and frustrating and caused also extra costs. The general suspicion with which I was confronted from the beginning of my 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 last letter was also sent to the CNPD, I received a reply on 24/12/2013 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 2 August 2002:

1. The viewing of the recordings of the CCTV surveillance are 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

[70] 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.

until the right of access has been executed, in order to prevent the automatic deletion of the footage after a certain amount of time – in this case one month (for some cameras five and eight days).

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 2 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 was very restrictive 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 a good practice (see Fig. 3), although information concerning the right of access isn't mentioned in this case. Upon visiting the railway station of Luxembourg City on 27/09/13 as well as using their parking lot on the same date, I sent my first subject access request on 01/10/13, asking for my personal data in regard with their large amount of CCTV surveillance, having visited several areas of the station.[71]

My request remained – as did my all my e-mails before – unanswered, thus a reminder was sent on 28/11/13, asking for an answer to my subject access request. Since the reminder was also ignored, I filed an official complaint to the CNPD on 10/02/14, advising them of the fact that the data controller had ignored every request I had made to the company and thus the impossibility to access my 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 data controller mentions access rights, ignoring all of my requests gives the impression of a deliberate neglecting of data protection principles by the company. At the time of writing – 09/05/14 – my 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

[71] With the renovation of the railway station in Luxembourg City, the amount of CCTV was increased – in their latest annual report, the company stresses out that in order to increase the safety of the passengers and personal the installation of video surveillance will be continued (cf. Rapport annuel, 2013: 34) and also in the national register, the areas of CCTV surveillance for the railway station of Luxembourg City presents an extensive list (see http://www.cnpd.public.lu/fr/registre/application/index.html (Accessed 13.03.2014)).

controlled by Art. 17 of the Law of 2 August 2002 initiating a Luxembourgish regulation for the creation of security areas in Luxembourg City – which has to be newly delimited every year.[72,73] 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 (cf. Fig. 3) 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 are not available. As I was already in contact with the grand-ducal police for my records in their files, it was communicated to me that the supervisory authority – thus the state prosecutor – is also responsible for the access to data in case of CCTV footage. This is also stated in Art. 17 (2) of the Law of 2 August: "*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 after passing through some of the security zones when visiting other sites on 27/09/13, I sent my subject access request to the supervisory authority on 01/10/13 and asked for further specifications on 11/11/13. The first answer was received on 08/10/13. This response did not disclosed my personal data, but it corrected some of the information I had previously been given. First of all, although the first regulation from 01/08/07 states that recordings are deleted at the latest after two months if the footage isn't 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" *isn't* "as such" *identifying'.* Another point is that the law doesn't specifically grant the right of direct access of the data.

The second answer, responding to the questions about automatic decision making and third party sharing was sent on 15/11/13. This mainly informed me that the supervisory authority does not use any automatic decision making and it doesn't 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, it also couldn't give me specific information on those 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 isn't directed to provide the data

[72] The Minister of Interior confirmed and thus extended with latest regulation the current security in areas in Luxembourg City for another year until 07/11/2014. (cf. 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 14.03.2014)).

[73] Except for the security area E, the *'quartier du Kirchberg'*, surrounding the conference centre of the European Union, a fifth security area added via the ministerial regulation of the 25th April 2012, which has no annual expiration date (cf. http://www.legilux.public.lu/leg/a/archives/2012/0086/a086.pdf (Accessed 14.03.2013)).

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 2 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 isn't sufficient and moreover is 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 trough supervisory authority, (which is only able to rectify data and inform the data subject) it would be crucial to provide those 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[74], preventing the massive surveillance of the 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 on 03/09/13 to the legal department of the bank to which I received a reply one week later. Besides the justification as to why they have CCTV and the indication of the authorisation of the CNPD of the surveillance measures, my access was denied with a reference to the article 29. Exceptions to the right of access of the Law of 2 August 2002 and additionally since I didn't mention a legitimate reason for my access to data. Demanding a revision of the way my request was treated and a specification of the denial of my right of access – since I don't need to provide a reason for my access to data – the 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 my personal data regarding the video surveillance could not be disclosed. Moreover, the data controller assured me that none of my data was shared with third parties and except for the automatic deletion of the footage after a specific period of time (without mentioning the exact period), no other automatic decision making processes are used in the CCTV surveillance.

CCTV in government building

[74] E.g. see Wort.lu (26.09.13) "Videoüberwachung um ein Jahr verlängert" http://www.wort.lu/de/view/visupol-videoueberwachung-wird-um-ein-jahr-verlaengert-52447881e4b0ca64e0e520aa (Accessed 14.03.2014), or Lessentiel.lu (27.09.13) "Videoüberwachung sorgt weiter für Debatten" http://www.lessentiel.lu/de/news/luxemburg/story/31961736 (Accessed 14.03.2014) for Media responses, or a debate from the Luxembourgish town council from the 30th September 2013 about the VISUPOL project http://www.vdl.lu/Politique+et+Administration/Conseil+communal/Questions+pos%C3%A9es+par+les+conseillers+communaux/Conseil+communal+du+30+septembre+2013/VISUPOL.html (Accessed 14.03.2014). The local council of the cities of Esch-sur-Alzette and Ettelbrück disapproved the concept of an open street CCTV surveillance in public areas.

My subject access request was sent on 27/09/13 and the response of the ministry arrived already five days later. In the first instance, the data controller denied the third party sharing of the CCTV footage and used this as a reason not to be able to disclose my personal data – for data protection reasons. When I responded to the data controller that this would not be a valid reason to limit my right of access, he surprisingly answered that I have indeed a right of access to my recordings, but they are 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 ten days – even though they have the right to store the footage for one month – the footage from my visit did not exist anymore. Besides the automatic deletion of the footage, no other such processes are applied to the CCTV surveillance. Thus in the second instance my right of access was acknowledged by the data controller but it was by then of no use anymore since the footage was already deleted. This makes the first answer look even more like a deliberate refusal for the disclosure of my personal data and potentially a delaying tactic to ensure the footage was erased.

Concluding thoughts

Overall in Luxembourg, both for the CCTV as well as the non-CCTV data, trying to access one's personal data, as is granted by the Law of 2 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 for lay citizens more than difficult to execute their rights. A coherent guideline regarding the subject access requests 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 the data subject is so persistent in asking for the personal data. Also it makes the actual goal of the right of access to data complicated to achieve – only six of all the visited sites provided comprehensive and complete answers to my requests and only twelve disclosed my personal data.

Still it is not to say that all the data controllers in Luxembourg show restrictive practices, obstructing the right of access to data. Moreover some goodwill has been experienced throughout the research, although it might not have had the intended effect, like e.g. the replacement of the signage in the department store.

Regarding CCTV surveillance, an obvious difference between public and private practices can be concluded, although not in the way subject access requests are handled but in the amount of CCTV surveillance. Especially for the open street surveillance of public areas, ubiquitous CCTV surveillance does not seem to be the intended goal in Luxembourg. 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, facilitative as well as restrictive

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

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 should be approached proactively by an information campaign from the CNPD. Especially in regard with the way the CNPD reacted concerning the complaints – although the handling time of those concerns seems rather long with more than two 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 2 August 2002.

SIGNIFICANCE OF FINDINGS - LUXEMBOURG

In Luxembourg, the 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 in 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 is not very efficient when informing 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 organisation's 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 about whom to contact in case of data protection questions. As a result, any person requesting information would be able to - sooner or later - locate it.

Regarding the right of access to data, the trend of a general lack of knowledge can be further observed. Incomplete replies from data controllers were more often received. From time to time, requests were even completely ignored, although the observed cases also showed the necessity of subject access requests in cases where personal data might be erroneous. Not only was the disclosure of the personal data difficult to achieve, 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 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 to it in an satisfactory manner.

Finally the role of the data protection authority, the *'Commission nationale pour la protection des données'* – 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 the department store *'Auchan'* was resolved rather quickly, speaking in favour for the data subject regarding the access to data resulting from CCTV footage, other complaints remained unanswered after more than two month. Not even a notice about the complaints being processed or the like arrived, which somewhat tempers

the good practice shown beforehand. This is especially so since in their role as the supervisory authority, the CNPD should be providing the necessary help for both the data controller and the data subject.

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

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 09 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 09 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 09 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 09 May 2014

Centre d'études sur la Citoyenneté, l'Informatisation et les Libertés (2010): Loi N°95-73 du 21.01.1998 d'orientation et de programmation relative à la sécurité. http://cecil.resade.1901.org/lececil/spip.php?article45&lang=fr Accessed 09 May 2014

Code de la sécurité intérieur, Article L251-1. http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000025505406&cidTexte=LEGITEXT000025503132&dateTexte=20120618&fastPos=17&fastReqId=1560864542&oldAction=rechCodeArticle Accessed 09 May 2014

Commission Nationale de l'Informatique et des Libertés, (2012): Vidéosurveillance – Vidéoprotection. Les Commerces. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL_Video_commerce.pdf Accessed 09 May 2014

Commission Nationale Pour La Protection Des Données (2012) 'Rapport annuel 2011' http://www.cnpd.public.lu/fr/publications/rapports/cnpd/rapport_activite_2011.pdf Accessed 09 May 2014

Commission Nationale pour la Protection des Données: Régistre Nationale. http://www.cnpd.public.lu/fr/registre/application/index.html Accessed 09 May 2014

Commission Nationale pour la Protection des Données: Vidéosurveillance. Demande d'autorisation. http://www.cnpd.public.lu/fr/declarer/autorisations/traitements/demande-video/index.html Accessed 09 May 2014 – Latest update 10 January 2014.

Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data modified by the Law of 31 July 2006 the Law of 22 December 2006 the Law of 27 July 2007. http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf Accessed 09 May 2014

Déi Gréng 'Demande d'inscription' http://www.greng.lu/demande-dinscription Accessed 07 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 07 May 2014

Europe v Facebook (2013) 'Get Your Data – Make an access request at Facebook' http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html Accessed 09 May 2014

European Court of Human Rights (2010) 'European Convention of Human Rights' http://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed 09 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:31995L0046:en:HTML Accessed 09 May 2014

Google Dashboard https://www.google.com/settings/dashboard Accessed 07 May 2014

Google History https://history.google.com/history/ Accessed 07 May 2014

Information Commissioner's Office (2008) CCTV Code of Practice. Chapter 9. Responsibilities, p.15ff, http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf Accessed 09 May 2014.

Interpol FAQs http://www.interpol.int/About-INTERPOL/Structure-and-governance/CCF/FAQs Accessed 09 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

Lessentiel.lu (27.09.13): Videoüberwachung sorgt weiter für Debatten. http://www.lessentiel.lu/de/news/luxemburg/story/31961736 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 09 May 2014

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

Ministère de la Sécurité Sociale 'InSight SantéSécu' http://www.mss.public.lu/publications/infoletter/index.html Accessed 09 May 2014

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

Ville de Luxembourg – Conseil communal du 30 septembre 2013: VISUPOL.
http://www.vdl.lu/Politique+et+Administration/Conseil+communal/Questions+pos%C3%A9es+par+les+conseillers+communaux/Conseil+communal+du+30+septembre+2013/VISUPOL.html Accessed 09 May 2014

Wort.lu (26.09.13): Videoüberwachung um ein Jahr verlängert.
http://www.wort.lu/de/view/visupol-videoueberwachung-wird-um-ein-jahr-verlaengert-52447881e4b0ca64e0e520aa Accessed 09 May 2014.

List of Abbreviations

CCF – Commission for the Control of Interpol's Files

CNPD - Commission nationale pour la protection des données

ECHR – European Human Rights Convention

ICO - British Information Commissioner's Office

SNCA – Société Nationale de Circulation Automobile

SNCT – Société Nationale de Contrôle Technique