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

NORWAY COUNTRY REPORTS

PEACE RESEARCH INSTITUTE OSLO, NORWAY

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN NORWAY – ROCCO BELLANOVA, J. PETER BURGESS & MARIT MOE-PRYCE

LOCATING THE DATA CONTROLLER IN NORWAY – MARAL MIRSHAHI, ROCCO BELLANOVA & J. PETER BURGESS

SUBMITTING ACCESS REQUESTS IN NORWAY – STINE BERGERSEN, ROCCO BELLANOVA & J. PETER BURGESS
MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN NORWAY

Introduction

The aim of this country report is to provide an overview of the main Norwegian legislation and practices concerning data subjects’ right to access their personal data.\(^1\) The scope of the right of access is rather wide in the wording of Article 12 of the so-called European Union (EU) Data Protection Directive (DPD),\(^2\) as it includes not only the mere access to personal data but also the possibility to erase, block or rectify the same. Due to the limited scope of this analysis, when studying the Norwegian legislation we have kept a rather ‘restrictive’ reading of Article 12, limited to the provisions of Article 12(a) DPD granting the right to “obtain” information.\(^3\)

Whenever possible, we have quoted the most relevant sections of the legislation, using the English versions available on the website of the Datatilsynet.\(^4\) When no ‘consolidated’ translation is available, we have provided ad hoc translation as well as exhaustive references to the original version.

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

---

\(^1\) In particular, we focus on the relevant Norwegian primary and secondary legislation on data protection, with special attention to the provisions concerning data access. We also take into account the information and the advice provided by the Datatilsynet, the national Data Protection Authority (DPA), on its website. Furthermore, we also integrate both academic and practitioners’ publications on the topic, as well as information received during exploratory interviews with lawyers of the law firm DLA Piper, and with Ann Setan Rudinow, Professor at the Norwegian University of Science and Technology and member of the Personvernmnnda, the Norwegian Privacy Appeals Board. We have organized informal meetings with officials of the Datatilsynet to receive advice on the specifics of the Norwegian data protection legislation. Finally, we have used two handbooks offering an overview of Norwegian legislation and case law to better orientate our research in its first phases: cf. Hafskjold, Christine, Lee A. Bygrave, Tobias Mahler, and Thomas Olsen, “Norway”, Privacy International, London, 2010. Available at: https://www.privacyinternational.org/reports/norway/i-legal-framework (hereinafter: Hafskjold et al.); and: Gronlie, Nils Arne, Håvard Kjærstad, and Stine Baumann, “Data protection in Norway: overview. Data Protection multi-jurisdictional guide”, Practical Law Company, London, 2012. Available at: http://uk.practicallaw.com/5-520-1543#. The authors would like to thank all their informants for the precious advices provided. Obviously, the authors remain the sole responsible for any error or misunderstanding.


\(^3\) Art. 12(a) DPD states that:

Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1).

\(^4\) http://www.datatilsynet.no/English/Regulations/
First of all, it is important to note that Norway is somehow a special case among the countries selected for this coordinated international research exercise. It is the only one that is not a member of the EU, but it has implemented the DPD. Second, Norway has a rather long legislative tradition in the field of data protection: its first dedicated regulation has been adopted in the same period in which few other European countries (or autonomous regions) were enacting similar pioneering laws (e.g. France and Hessen). Therefore, Norway can be largely compared to other EU member states when it comes to the ‘translation’ of the DPD. Yet, it should also be acknowledged that it has introduced specific original provisions and that there are evident differences in terms of its ‘institutional participation’ to EU debates on data protection. For example, the Norwegian DPA has no seat in the so-called EU Article 29 Working Party, but only an observer status.

The main legal instrument that translates the Data Protection Directive (DPD) in Norway is the Personal Data Act (PDA),\(^5\) which is complemented by the Personal Data Regulations (PDR),\(^6\) both of 2000. In terms of data protection principles and key definitions, the PDA can be considered substantially in line with the EU framework. Norwegian data protection legislation can be even considered more advanced in specific fields, for example when it comes to the “use of personal profiles” and of “automatic decisions” (cf. Sections 21 and 22 PDA). As mentioned below, the right to access data (\textit{innsynsrett}, in Norwegian) is largely mirrored in Section 18 PDA (among many), and it is partially granted not only to data subjects but also to “any person” (cf. the wording of Art. 12(a) DPD quoted in footnote 3). It is important to highlight that Norway had already enacted legislation on the protection of data back in 1978: the Personal Data Registers Act.\(^7\) As mentioned above, this legislation was among the first enacted in Europe. The 1978 law was ‘completed’ by a series of regulations in the following years, and also established the Norwegian DPA – the Datatilsynet –, which became active at the beginning of 1980. The Personal Data Registers Act already included a provision on the right to access data (cf. Paragraph 7), which shared many of the basic features of the current definition. Finally, it should be noted that while no specific protection is granted to privacy in the Norwegian Constitution (1814), “the Norwegian Supreme Court held that there exists in Norwegian law a general legal protection of “personality”, which incorporates a right to privacy” in a ruling of 1952.\(^8\)

At present, the PDA sets the general framework of data protection legislation, while the PDR provides for regulations in specific fields, including credit information services (chapter 4) and video surveillance (chapter 8).\(^9\) Furthermore, sector-specific laws govern key relevant databases/registers, such as health, police, population, the Schengen Information System, etc.\(^10\)

\(^{5}\) Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act). Available at: http://www.datatilsynet.no/Global/english/Personal_Data_Act_20120420.pdf. Hereinafter: PDA.

\(^{6}\) Regulations on the processing of personal data (Personal Data Regulations). Available at: http://www.datatilsynet.no/Global/english/Personal_Data_Regulations_20100215.pdf. Hereinafter: PDR.


\(^{8}\) Hafskjold et al.

\(^{9}\) Video surveillance is also the subject of specific attention in the PDA, where a full chapter (VII) introduces a specific definition and different layers of requirements.

\(^{10}\) An overview of the evolution of Norwegian data protection law in relation to surveillance practices can be found in section 4.3.5 of the IRISS Deliverable D2.3: The Legal Perspective, available at: http://irissproject.eu/wp-content/uploads/2013/04/Legal-perspectives-of-surveillance-and-democracy-report-D2.3-IRISS.pdf.

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
None of the most important recent case law discussed by Hafskjold et al. concerns the right of access to data as such.\footnote{Hafskjold et al. refer to three recent cases that touch upon disclosure of the identity of an internet user linked to a specific IP address, the disclosure of personal information of relatives in the framework of literature works, and the possibility to retain control over her own image. See Hafskjold, Christine, Lee A. Bygrave, Tobias Mahler, and Thomas Olsen, “Norway”, Privacy International, London, 2010. Available at: https://www.privacyinternational.org/reports/norway/ilegal-framework} Such a finding was confirmed in the informal meeting and exploratory interviews held with academics, lawyers and DPA officials. However, it is interesting to note that the Personvernnemnda, the Privacy Appeals Board, has dealt with some ‘administrative’ cases concerning the right of access.\footnote{The Privacy Appeals Board is a sui generis institution in data protection law, because it is an “independent administrative body subordinate to the King and the Ministry” that “shall decide appeals against the decisions” of the Datatilsynet (Section 43 PDA).} For example, in a recent case (December 2012), the Personvernnemnda decided upon the case of denied request of access advanced by an employee.\footnote{Cf. PVN-2012-13 Innsyn i personalmappe. Klage på Datatilsynets vedtak vedrørende nektet innsyn i personalmappe. Personvernnemndas avgjørelse av 18. desember 2012; available at: http://www.personvernnemnda.no/vedtak/2012_13.htm.} The main issue at stake was the possible application of a specific clause of exception to data access requests, namely the exclusion of data “which are solely to be found in texts drawn up for internal preparatory purposes and which have not been disclosed to other persons” (Section 23(e)). The facts concerned the non-disclosure of a series of files concerning the data subject and stored by the employer. When the lack of access was brought to the attention of the Datatilsynet, the authority had endorsed the claim of the employer and accepted the invocation of the clause of Section 23(e). With its decision, the Privacy Appeals Board partially reversed the position of the DPA, arguing mostly on the basis of the application of the Administration Act and of the general principle of transparency.

Another relevant case concerns a request of access advanced by an employee of the airline SAS concerning his insurance premium.\footnote{KLAGESAK PVN-2005-02: Klage på Datatilsynets vedtak om å avvise sak om innsyn i innbetalt forskningspremie Personvernnemndas avgjørelse av 9.8.2005 ; available at: http://www.personvernnemnda.no/vedtak/2005_2.htm.} SAS forwarded his request to the insurance company, but the latter refused access, arguing that insurance premiums are only in part based on information linked directly to an individual. The case is particularly interesting because it touches upon the limits of the definition of personal data, as the insurance company submitted that insurance premiums are not personal information given the way in which they are calculated. This line of reasoning was endorsed by the Datatilsynet, but this interpretation was reversed by the Privacy Appeals Board, which required the disclosure of the requested data to the data subject.

Finally, even if it does not concern the right of access, it is worth mentioning what can be considered one of the most important cases in the jurisprudence of data protection in Norway. The case concerned the legitimacy of the decision to dismiss an employee (a driver) based on the cross-check of different registers, and in particular the data of the GPS system installed in the driver’s vehicle.\footnote{Cf. Surveillance/monitoring HR-2013-00234-A (2012/1334). Stikkord: gps, personopplysningsloven § 49.} The driver and his trade union lodged a complaint to the Datatilsynet, arguing that the company had used his location data for a purpose different from the original purpose of the GPS system (which had been installed for safety reasons). The DPA supported...
the employee’s claim, as did the Privacy Appeals Board. Interestingly, the courts, including the Supreme Court, recognized that the use of GPS data was not legal, but that the resulting records could be accepted as evidence, and thus the dismissal of the employee was fair.

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

The main provision concerning the right of access to data is Section 18, chapter III, of the PDA. The Section 18 PDA states that:

“All any person who so requests shall be informed of the kind of processing of personal data a controller is performing, and may demand to receive the following information as regards a specific type of processing:

a) the name and address of the controller and of his representative, if any,

b) who has the day-to-day responsibility for fulfilling the obligations of the controller,

c) the purpose of the processing,

d) descriptions of the categories of personal data that are processed,

e) the sources of the data, and

f) whether the personal data will be disclosed, and if so, the identity of the recipient.

If the person requesting access is a data subject, the controller shall inform him of

a) the categories of data concerning the data subject that are being processed, and

b) the security measures implemented in connection with the processing insofar as such access does not prejudice security.

The data subject may demand that the controller elaborate on the information in the first paragraph, litra a-f to the extent that this is necessary to enable the data subject to protect his or her own interests.

The right to information pursuant to the second and third paragraphs shall not apply if the personal data are being processed exclusively for historical, statistical or scientific purposes and the processing will have no direct significance for the data subject”.

Therefore, Section 18 PDA provides for a rather comprehensive right of data access. Indeed, the first paragraph establishes a de facto obligation for data controllers to provide - to both data subjects and other individuals (“any person”) – a wide array of information on the processing operations. Therefore, it provides for both a sort of ‘general’ right of access and a ‘individual’ right of access to information. The scope and quality of access of these two kinds of right of access to information is different. In line with the EU directive, data subjects can require more detailed information, their own personal data as well as information on the measures taken by the data controller to ensure the security of the processing. This last kind of information is, however, restricted in case of a specific security measure that would be undermined by revealing its detailed operations. Section 18 PDA establishes also a more general limitation on the right of access of data subjects: limiting the scope of the information to be made available if the processing has “historical, statistical or scientific purposes” and if it has “no direct significance for the data subject”.

---

16 As mentioned in the Section 6, the distinction between “generelt innsyn” (general access) and “individuelt innsyn” (individual access) is drawn from the website Personvern på nettet operated by the University of Oslo (cf. [http://personvern.info/verktøy/krev-innsyn/](http://personvern.info/verktøy/krev-innsyn/)).
Section 22 PDA is also particularly relevant, as it translates the part of Article 12(a) of the Data Protection Directive concerning automated decisions. Section 22 PDA states:

“If a decision has legal or another significant effect for the data subject and is based solely on automated processing of personal data, the data subject who is subject to the decision may demand that the controller give an account of the rules incorporated in the computer software which form the basis for the decision.”

Other elements of the ‘wider’ right of access to data as provided by Article 12 DPD, such as rectification, erasure, blocking and notification to third parties (Art.12(b) and (c)) can be found in Section 27, concerning the “rectification of deficient personal data”, and, to some extent, in Section 28, on the “prohibition against storing unnecessary personal data”.

Sections 16 and 17 PDA are also of particular interest for the scope of this overview. Section 16 PDA sets specific time limits for the data controllers: they “shall reply to inquiries regarding access or other rights pursuant to Sections 18, 22, 25, 26, 27, and 28 without undue delay and not later than 30 days from the date of receipt of the inquiry”. In case of “special circumstances”, the reply can be “postponed”, but “the controller shall give a provisional reply stating the reason for the delay and when a reply is likely to be given” (Section 16 PDA). However, the PDA does not provide any specific criteria to define legitimate “special circumstances”. Conversely, the time limits are rather clear and well defined, as is the question of the possible costs of a data access request as Section 17 of the PDA states that “[t]he controller may not request compensation […] for meeting demands of the data subject pursuant to Chapter IV [which includes the right to access]”. While the use of “may” in English could be interpreted as including an element of doubt, the original text in Norwegian is very clear, confirming that no compensation shall be requested from the data subject.17 Finally, Section 24 PDA states that “information may [be] requested in writing from the controller or from his processor”, and also that the data controller “may require that the data subject furnish a written, signed request”.

Beyond the ‘law in the books’, Datatilsynet can provide support to individuals that have not received a response from the data controller. In particular Datatilsynet can open a case in their case handling system and contact the data controller demanding that they respond to the request. If there is no reply from the data controller, the Datatilsynet can decide about possible fines for the data controller. Besides this, the Norwegian DPA has launched some initiatives to facilitate the right of access, even if this task is not explicitly mentioned in the PDA (cf. Section 42, 3rd para). We discuss the most relevant ones in Section 5 below. Finally, it is important to note that both the Datatilsynet and the so-called Privacy Appeals Board, enjoy a sort of specific right of access. Among their inspection and decisional powers, they “may demand any data necessary to enable them to carry out their functions” (Section 44 PDA).

**National exceptions to the EU Data Protection Directive and to the right of access to data**

A series of general limitations to the right of access to data can be found in Section 23 PDA:

---

17 “Den behandlingsansvarlige kan ikke kreve vederlag for å gi informasjon etter kapittel III eller for å etterkomme krav fra den registrerte etter kapittel IV” (§17 PDA).

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
“The right to access pursuant to Sections 18 and 22 and the obligation to provide information pursuant to Sections 19, 20 and 21 do not encompass data:

a) which, if known, might endanger national security, national defence or the relationship to foreign powers or international organisations,
b) regarding which secrecy is required in the interests of the prevention, investigation, exposure and prosecution of criminal acts,
c) which it must be regarded as inadvisable for the data subject to gain knowledge of, out of consideration for the health of the person concerned or for the relationship to persons close to the person concerned,
d) to which a statutory obligation of professional secrecy applies,
e) which are solely to be found in texts drawn up for internal preparatory purposes and which have not been disclosed to other persons,
f) regarding which it will be contrary to obvious and fundamental private or public interests to provide information, including the interests of the data subject himself.

Data pursuant to the first paragraph, litra c, may nonetheless on request be made known to a representative of the data subject when there are no special reasons for not doing so.

Any person who refuses to provide access to data pursuant to the first paragraph must give the reason for this in writing with a precise reference to the provision governing exceptions.

The King may prescribe regulations regarding other exceptions from the right of access and the obligation to provide information and regarding conditions for the use of right of access’. This latter rule confirms the King as the head of state, and establishes that in case of any exceptions (apart from those stated in § 23 a- f) to the rules, the stake is very high as only the head of state can issue such exemptions.

Section 23 is not only interesting for the list of exceptions, which remains rather ‘traditional’, but also because it establishes a sort of indirect access when it comes to data “which it must be regarded as inadvisable for the data subject to gain knowledge of consideration for the health of the person concerned for the relationship to persons close to the person concerned” (Section 23, para 1(c) PDA). Furthermore, the same Section 23 obliges the data controllers to provide a written response for denying access including the reason for the denial.

Compatibility of national legislation with Directive 95/46/EC

As mentioned above, the main legislation (both the PDA and the PDR) implements the DPD. So far, no major issues concerning the (lack of) compatibility of the national legislation with DPD have emerged. No relevant debate or discussion has been raised on the specific provision of the right to access data or the compatibility of the Norwegian system with the one established by the DPD. As mentioned above, Sections 18, 27 and 28 PDA largely translate the full scope of Article 12 DPD.

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

No specific codes of practice have been developed so far. As mentioned above, the PDR provides regulation in several specific fields, including both CCTV and credit ratings.
Chapter 4 PDR concerns “credit information services”, and Section 4-4 focuses on the “right of access of and information to the data subject”. The second and third paragraphs of Section 4-4 PDR state:

“[first para]
The right of access of legal persons follows from Section 18 of the Personal Data Act. The data subject may also demand to be informed of what credit information has been provided about him in the last six months, to whom it was given and where it was obtained.”

While the second paragraph recalls the general provision of the PDA, it is interesting to note that the third paragraph grants further rights of access to the data subject, tailored on the specific ‘social’ functioning of credit ratings.

Chapter 8 of the PDR concerns “video surveillance”, and Section 8-5 focuses in particular on the “right of access”. Section 8-5 states:

As regards image recordings to which Section 37, second paragraph, of the Personal Data Act applies [“video surveillance that must be assumed to be of significant importance to the prevention and solving of crime”], the provisions regarding right of access pursuant to Section 18 of the Personal Data shall apply. In other cases, the subject of the image recording may demand access to the parts of the image recordings in which the subject appears, if the image recordings are stored for a period exceeding seven days.

Right of access pursuant to the first paragraph, second sentence, shall not apply to image recordings that are in the possession of the police, or image recordings that may be of significance for the security of the realm or its allies, other vital national security interests and the relationship to foreign powers.

The first paragraph of Section 8-5 PDR is divided in two parts, establishing two different regimes of data access on the basis of the purposes for which the CCTV is operated. If the video surveillance is “assumed to be of significant importance to the prevention and solving of crime” (Section 37 PDA), then the regime of data access is that established by Section 18 PDA. If not, the scope of data access is reduced, and the data subject can only request access to her own images, and only if they are stored for more than a week. Further restrictions are in place regarding access to CCTV footage, including cases where the images are already “in possession of the police”, or they concern national security. In such instances, no access at all is possible (Section 8-5, 2nd para, PDR).

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

Even if the promotion of the right to access data is not a statutory key function of the Datatilsynet,\(^\text{18}\) it is interesting to note that the DPA has devised a few related activities.

\(^{18}\) According to Section 42, 3rd para, of the PDA, [the Data Protection Authority shall]
1) keep a systematic, public record of all processing that is reported pursuant to Section 31 or for which a licence has been granted pursuant to Section 33, with information such as is mentioned in Section 18, first paragraph, cf. Section 23.
IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
According to information obtained during an informal meeting with official of the Norwegian DPA, the Datatilsynet is considering drafting a standard template for data access requests, to be posted on the website.\(^{19}\) Currently, the most relevant initiative is a dedicated page of the Datatilsynet website,\(^ {20}\) listed among a group of informative pages on the basic rights guaranteed by data protection (http://www.datatilsynet.no/personvern/). In the page focusing on the right to access, the DPA provides a short presentation of the scope of this right (e.g. what people can request from data controllers), a list of possible related questions, and a template to require access to the information collected by the employer.\(^ {21}\) It is interesting to note that, in the same page, the DPA refers also to Section 21 PDA, concerning the “obligation to provide information in connection with the use of personal profiles”. The Datatilsynet publishes an annual report of its activities (available only in Norwegian). Unfortunately, the report does not specify the number of complaints concerning data access that have been received and processed by the DPA.

In addition to the information published on its own website, the DPA also handles and promotes a website called Slettmeg.no, which means ‘delete me’, providing support for individuals “who find offending material about themselves on the Internet” but also that “have published this information themselves, but regret it and want this information removed”).\(^ {22}\) The website is managed by the Norwegian Centre for Information Security, but according to Hafskjold et al., it is the responsibility of the Datatilsynet.\(^ {23}\)

Similarly to the DPA, the Personvernmmnda has no statutory responsibility for promoting access rights, as its main function is to “decide appeals against the decisions of the [Norwegian] Data Protection Authority” (cf. Section 43 PDA). Still, the website of the Privacy Appeals Board advises citizens to consult the web-pages of the Datatilsynet and of an ad hoc website of the University of Oslo to obtain background information on data protection policies and rights. The latter website, called Personvern på nettet (Online Privacy Policy),\(^ {24}\) is particularly interesting for the scope of this overview because it devotes an entire subsection to the right of access.\(^ {25}\) Under the motto “Krev innsyn” (“Claim access”), the

---

\(^{19}\) Informal meeting held on the 4th September 2013 in the premises of the Norwegian DPA.

\(^{20}\) http://www.datatilsynet.no/personvern/Informasjonsplikt/

\(^{21}\) http://www.datatilsynet.no/verktøy-skjema/Skjema-maler/Innsyn-i-personalmappe-brevmal/

\(^{22}\) http://www.slettmeg.no/English

\(^{23}\) Cf. Hafskjold et al.

\(^{24}\) http://personvern.info

\(^{25}\) http://personvern.info/verktøy/krev-innsyn/
Personvern på nettet website provides both theoretical and practical information on the general and the individual right of access. These include, inter alia: a short description of the rights of individuals and data subjects with explicit reference to the kind of information that can be accessed and to the most common exceptions applicable, links to relevant legislation (e.g. Section 18 PDA), functional advice concerning the procedure of a data access request (e.g. who should be contacted and the eventual need to send a written request), and examples of possible situations in which individuals or data subjects can find themselves.

**Role of national DPAs in ensuring that data controllers allow citizens to exercise their access rights**

In general, the duties and powers of the Datatilsynet are established in chapter VIII of the PDA. In particular, it should be noted that the DPA, as well as the Privacy Appeals Board, “may demand any data necessary to enable them to carry out their functions” (Section 44, 1st para, PDA). However, while the DPA has a general duty to “verify that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies are rectified” (Section 42, 2nd para, (3), PDA), no special provisions concern data access.

As mentioned above, the Datatilsynet can intervene if a data controller does not respond to the requesting subjects, or if a data subject lodges a complaint. Apart from that, no specific large-scale investigation concerning data access has been carried out in the last few years.
LOCATING THE DATA CONTROLLER IN NORWAY

Introduction

This country profile report on Norway is based on the experiences encountered whilst attempting to locate data controller contact details of several everyday surveillance sites. In particular, the main purpose of this preliminary ‘ethnographic’ research was to assess the level and quality of accessibility to data controller information, simulating the perspective of a ‘lay person’ attempting to approach various institutions and agencies. Given the specific methodology followed, as well as the scope of this research, the observations below are illustrative of the researcher’s experiences and do not claim to reflect the practices of all data controllers in Norway. Nevertheless, this exercise can highlight some general trends, and permits to identify some examples of good and bad practices encountered during the course of this research.

Methodology and limitations

The adoption of a coordinated research design is aimed at enabling a transnational comparative analysis, which is presented in the following sections. However, it should be noted that, given the very nature of the ethnographic-inspired method adopted, the use of the shared protocol has been adapted by each team at the level of the ‘micro-managing’ of the research.

The bulk of the research was carried out during July 2013. The report has been drafted and revised in the following period. The chosen sampling approach for this phase of the study is a ‘non-probability convenience’ sampling. Similar to the other country cases, we used this approach to include cases were personal data of a ‘lay person’ would be held. The cases selected for this study were the following: locally held health records; locally held primary school records; locally held secondary school records; banking records; insurance records; credit reference checks; entry/exit system at work place; HR/personnel files at work place; membership to sports club; loyalty card for a national supermarket; loyalty card for a private company; internet service provider; mobile phone data; e-mail data; social network website; online gaming; search engine data; CCTV in transport setting; CCTV in public space; CCTV in department store; CCTV in local store; CCTV in bank; membership to national children’s charity organisation; membership to trade union; membership to political organisation; membership to NGO; electoral roll; driving license records; automatic number plate recognition (ANPR); border control; passport service; police records; and Interpol.

Together with the task leader and the other research teams, we have categorized these kinds of sites under the following domains: health; work place; education; finances; leisure; communications; consumerism; civic engagement; security; and transport/movement.
The following three sampling strategies were defined by the task leader: websites browsing, telephone contact, and personal visits. The researcher in charge of the bulk of the field research was requested to use the most convenient strategy to collect information, due to time and resource constraints. In practice, this implied opting for sites that were familiar, geographically nearest or the most important or relevant in the national market. For most of the cases a combination of these means of sampling were used. For example, in many cases the researcher used the online website to obtain the contact information of the selected site, and then contacted it by telephone or visit to the site itself.

Another key element of the shared methodology is the decision to not inform the interview subjects about the scientific nature of the request of information, and to not provide them any personal information of the researcher carrying on the interviews (e.g.: name and place of residence). The main reason of not revealing the researcher’s personal and professional identity was two-fold. First, the choice of not communicating the researcher’s personal details aimed at safeguarding the researcher’s privacy. It should be noted that, given the sampling criteria chosen, many of the sites under research can easily become part of the everyday life of the researchers themselves, even if the selection was carried out so to blur the personal preferences of the researchers. Second, the professional identity of the researcher was withheld to avoid a skewed experience than that of a ‘lay person’.

While opting for this ‘lay person’ approach, we do acknowledge that the persistence, time and resource capacity of a researcher may be greatly different than that of a so-called ‘lay person’. Furthermore, a ‘lay person’ may not have sufficient (if any) information about her data protection rights. This may result in hesitation when asking for information, or simply accepting declines and insufficient responses. Thus, the challenges in obtaining personal data from data controller may even be greater for a ‘lay person’ than for a researcher specifically trained to conduct this kind of study. On the other hand, we cannot make only ‘negative’ assumptions of the resources, skills or capacity of a ‘lay person’. For example, the factor of motivation of a ‘lay person’ pursuing information about a data controller may in fact exceed that of a researcher. Therefore, these reflections should be read as a crucial caveat to the possible generalization of the research insight of this preliminary study, and they are included to highlight a possible limit of the research itself.

In practically all the cases the use of websites was required to find the contact details of the site. As most websites did not provide information about the data controller, at least not at first sight, the researcher approached the sites by telephone in order to obtain information about the data controller. The researchers opted for this choice, because it reflected the ‘lay person’ approach, as it seemed to be the most immediate way to obtain specific information.

In the cases where data controller’s information was obtained at the first attempt through several channels, this has been counted as a ‘first round of visit’ success. In the cases where contact through several channels was necessary, this has been counted as ‘second round of visit’ success. The cases that have not provided sufficient data controller’s information have been deemed as ‘unsuccessful’.

---

26 In retrospect, this impression was somewhat modified. See next footnote for further explanation.

27 This involves the cases in which telephone inquiry was used to obtain information, whilst the same information was available also online. Finding the same information several places has thus been registered as “first attempt”. This was not due to the lack of information on the website, but rather that the telephone was a more convenient channel for the researcher. In these cases, although we regarded such use of two channels as ‘a first attempt success’, we do acknowledge in retrospect that it could in fact be easier for a lay person to retrieve information online, rather than being on the telephone (due to time and cost restraints).

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
When collecting data by the means of telephone, the interviews were ‘semi-structured’. In cases where the informant provided limited answers or simply denied answering, the researcher followed up with probing questions, highlighting the legislation on personal data access. In some cases, the probing questions led to better facilitation. In other cases, the probing made the informant more hesitant in answering. In some cases poor facilitation was due to lack of information or understanding of the question. This confusion occurred due to the fact that the researcher did not provide any personal information, making the informant reluctant to answer. In these cases, the researcher had to state that the question of obtaining personal data access was rhetorical, and that the aim of the inquiry was to identify the data controller if one was to obtain personal data access. In all cases concerning CCTV systems personal visits were required.

The operationalization of the quality of information, i.e. data controller’s details, has been divided into two categories: ‘successful’ and ‘unsuccessful’. ‘Successful’ cases imply results in which the data controller details are identified. In this category, we have chosen to include cases in which the data controller details are somewhat vague, i.e. the process of identifying and locating the specific office or entity within a large institution. Recognizing that this may lead to a time-consuming and complicated process for the ‘lay-person’, and although being on the borderline of ‘successful’, such cases may still provide information which enables access to personal data. The cases that have been categorized as ‘unsuccessful’ are those in which the data controller is not identified. Such unsuccessful cases are characterized by either a complete lack of information of data controller, or where the ‘lead’ information requires the involvement of a third party in order to access the data controller (e.g. the police).

Finally, it should be noted that at this stage of the study the researcher did not attempt to control whether the contact information of data controller actually would lead to obtaining access to personal data information. The aim of this preliminary study was to locate the contact information of the data controller, and to assess the quality of this information in terms of accessibility, and not in terms of effective ‘usability’ of the same information. Thus, when rating the quality of information, we have chosen to take the data controller contact details obtained as correct.

Overall impressions

At the beginning of the research, 35 sites were identified as relevant for the study. At a preliminary stage we discovered that two of these sites (nationally held health records and ID cards) were to be considered ‘non-existing’ in Norway. Thus these sites were removed from our selection. Out of the remaining 33 sites, we obtained some data controller information for all sites. The quality of and accessibility to this information, however, varied greatly. In this section we will provide the overall impressions of the research process, highlighting few particularly good and bad practices we encountered. The 33 sites consisted of 10 public sector agencies and 23 private sector companies. None of the 33 sites expressed the requirement of service cost for providing personal data.

Out of the 33 ‘explored’ cases, the data controller contact details of 22 sites were successfully identified after the first attempt. Out of these 22 cases, 7 sites belonged to public sector agencies. Five of these public sector sites provided limited information about the data

---

28 In Norway, the right of data access is provided for in Section 18 of the Norwegian Personal Data Act (PDA).
29 Primary school records, secondary school records, border control, passport service, ANPR, Interpol and police records. The data controller information for the last five sites mentioned here were rather vague; as we were requested to contact the police for data controller’s details. However, we have considered these cases as IRISS WP5 – Norway Composite Reports

Final Draft
14/05/14
controller, but were deemed as successful because a general data controller was identified. For these sites, the data controller that was identified was the police. These sites required a visit to the local police station with a valid photo ID for further information. For these cases it was not clarified whether the contact information of the data controller would be provided, or if the inquiry would be considered at the convenience of the police.

The remaining 15 private sector sites provided rather comprehensive contact details of the data controller such as telephone contact, per e-mail or by login with personal username and password on the website of the company/organization.

Three private sector cases, namely the internet-based cases of the social network website, the search engine and e-mail provider, did not provide sufficient information about the data controller and were therefore categorized as ‘unsuccessful’ after the first attempt. At three public sector sites, namely health records, driving license records, electoral rolls, we were requested to visit the office that applied to us (the office of caller’s medical practitioner, the local traffic station, the city hall of the area of residence). This information was considered as ‘successful’, because although the details of the data controller were not given as such, a personal visit to the establishment would lead to obtaining information about the personal data. However, due to the requirement of a second round of visits, we have categorized these sites as successful after second round of visits.

For the remaining 5 private sector cases, a second round of visits was required. The second attempt did not provide sufficient data controller information. The informants of these sites explained that data controller information could only be obtained through the police. The police was thus said to be the sole authority for requests of data access. Furthermore, this would imply that the only legitimate purpose of data access would be for investigation of a criminal act. These cases were categorized as unsuccessful, because we regarded the option of contacting the police inherently different for the private sector than that for the public sector cases. The difference between these two categories was the following: in the public sector cases the police can, as such, be reasonably identified as the data controller. In the cases of CCTV and entry/exit system at work place, the data controller would be rather implied to be the relevant private companies and the police ‘only’ a third party with the sufficient mandate to access to data, and not the data controller itself.

### Table summarizing the main results of the research

| Data controller contact details successfully identified in first round of visits | 22 of 33 cases (73%) |
| Data controller contact details unable to identify in first round of visits | 11 of 33 cases (27%) |

successful, because although the specific office or entity at the police was not mentioned, the institution itself is understood as the data controller.

Border control, passport service, ANPR, Interpol and police records.

We judged the requirement to go to a police station with a valid photo ID to inquiry on the possibility to lodge an access request for several sites as both very intrusive and disproportionate, both at the level of a ‘lay person’ and of a preliminary research activity. For this reason, we decided not to visit the police station.

Human resources at work place, banking records, insurance records, credit reference, membership to sports club, online gaming, internet service provider, mobile phone data, CCTV in local store, loyalty card for national supermarket, loyalty card for private company, membership to national children’s charity organization, membership to trade union, membership to political organization, membership to NGO.

Entry/exit system at work place, CCTV in bank, CCTV in department store, CCTV in public area, CCTV in transport setting.

IRISS WP5 – Norway Composite Reports

Final Draft

14/05/14
| Total number of data controller contact details successfully identified after second round of visits | 25 of 33 cases (76 %) |
| Total number of data controller contact details unable to identify after second round of visits | 8 of 33 cases (24 %) |
| Contact details identified via online privacy policy | 3 of 25 (successful) cases |
| Contact details identified after speaking to member of staff on phone/via email | 20 of 25 (successful) cases |
| Contact details identified after speaking to member of staff in person | 2 of 25 (successful) cases |
| Average rating given to visibility of privacy content online | 2 – Adequate |
| Average rating given to the quality of information given by online content | 2 – Adequate |
| Average rating given to visibility and content of CCTV signage | 1 – Poor |
| Average rating given to quality of information given by staff on the telephone | 2 – Reasonable |
| Average rating given to quality of information given by staff in person | 1 - Poor / 2 – Reasonable |

The private sector companies which provided particular services scored highest for good practice. In most of these cases, the informant had broad knowledge about the data controller contact details, and the information was provided rapidly and without hesitation. The quality of information was high because these companies provided several specific means to contact the data controller. Furthermore, these companies seemed to understand the inquiry without further explanation. This implied good accessibility for the average citizen/lay person.

On the contrary, the internet-based sites – social network, search engine and e-mail provider – scored lowest in terms of accessibility and quality of information. We found no specified contact details of data controller, and the means of any communication with these sites were rather generic in addition to requiring member login.

In 4 of the 5 cases concerning CCTV system we were told that access to data controller could only be obtained through the police. Only in the case of CCTV in a local store did we find the contact information of the data controller. However, even in this case, it was also mentioned that this would only enable us to view the CCTV footage, and that for acquiring the footage we had to contact the police. Thus, in our evaluation, we have only considered the CCTV in local store site to count as a successful case of obtaining data controller details.

The quality and accessibility of data controller details among the public agencies was intermediate. Although information about the data controller was to some extent obtained, the respondents seemed unsure and hesitant. This hesitation seemed to be due to lack of information about the data controller as well as the purpose for such inquiries.

In sum, based on the observations for this study, we found that private companies holding personal data of the member/client were better at providing accurate information about the

34 Technically the mobile phone company and insurance company also fall into this category, because the information was both obtained on the phone, and later also found on their website. As explained in the methodology section, the use of telephone was the first means of collecting data due to practical reasons.

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
data controller. In the cases where the personal information was recorded footage, the details of the data controller were not obtained (except for the local store). In public sector, the access to information was not very easy, and once obtained not very precise. Internet-based sites scored lowest on accessibility and quality of data controller details.

Public sector

Approaches of facilitation

In general, it should be noted that we noted poor ‘facilitation’ in the handling of our requests and questions by public sector sites. For example, out of the 10 agencies belonging to the public sphere, the informant of primary and secondary school records was the only one providing accurate information about the type of data that was held and how to access the data controller. For the cases of obtaining local medical records, driving license records and electoral rolls, we encountered facilitation on an intermediate level. More specifically, these sites requested us to visit our local agency of concern (such as the office of caller’s doctor, the local traffic control office and the local city hall). So, while identifying the type of institution that would serve as the data controller, the contacted sites did not specify where to find the data controller.

As for the remaining 5 sites, a similar trend of facilitation was observed. The informants’ response to all of these cases was that we had to contact the police for more information. So, albeit some facilitation was provided, we did not obtain specific information about the data controller. We consider these responses as successful finding, because the police are the overarching data controller. However, we do note that this information is somewhat insufficient because the informant did not specify the department/section within the police to contact, making the data controller details rather unspecific.

Our general impression of facilitation in the public sector is that personnel in the public sector do not have access to accurate information about the data controller as such. In all cases except for electoral rolls and school records, the tone and wording of the informant showed lack of interest for facilitation. Furthermore, although the various agencies identified the police as the relevant authority for obtaining access to personal data, it is unclear/arguable whether this was an elusive tactic to avoid the researcher’s question due to lack of information on the matter.

Approaches of Denial

As indicated in the previous section, in most of the cases concerning public agencies the process of obtaining data controller details was vague. We found that a factor leading to
denial was the fact that the researcher did not provide her name, date of birth and place of residence. As a result of this, the informants said that they could not provide the precise location and contact number of the data controller without having the basic information of the caller. This request can be considered, if not intrusive, at least disproportionate when compared to the wording of the Norwegian data protection legislation. Indeed, the Personal Data Act grants to “any person who so requests” (and not only to relevant data subjects) the right to get information “on the name and address of the controller and of his representative, if any, [and on] who has the day-to-day responsibility for fulfilling the obligations of the controller” (Art. 18 PDA, 1st paragraph, litra a and b). Furthermore, although providing information about which agency to approach, informants were not particularly helpful in providing information about how to locate such agencies. In all cases we were requested to search online for the location of the local agency that applied to us rather than the informants themselves looking up this information on our behalf. The only information that was clear was that a request of access to personal data could be lodged at the local agency with a valid photo ID.

When requesting the data controller information for medical records and driving license records the respondents seemed confused and hesitant in answering. Furthermore, the inquiry seemed to annoy the informants, and they were rather impatient when answering. For instance, the receptionist at the medical center said “I do not understand what you are asking for. I am busy; I have to take the calls from other patients now” and hung up as the researcher was still specifying the inquiry. Such responses seemed to be due to the lack of expertise/knowledge on the matter. This observation leads us to believe that denial could be a result of lack of preparedness for such inquiries, and hesitation due to lack of awareness of citizens’ rights to access personal data.

In the cases where the police was identified as the ‘lead’ to obtaining access to personal data, the informants were inquisitive to why we were curious to this information. Particularly in the cases of border control and Interpol, the request to contact the police seemed more as a redirection than a facilitation to obtain data controller details. Thus, the overall impression of approaches of denial concerned mainly the lack of interest when responding, the inability to provide detailed information without the caller’s personal ID, as well as the ambiguity as to why police contact is necessary for further information.

**Private sector**

**Approaches of facilitation**

In most of the cases concerning private actors, the access to data controller and personal data information appeared relatively clear and uncomplicated. For example, the information about the data controller for online gaming, sports club, mobile phone company and internet service provider was obtained in under 10 minutes for each respective case. Furthermore, all of these sites also provided insight into personal data through a member login on their website. This accessibility is regarded as a positive feature for obtaining access to personal data. However, this assumes that one is a client/member of the company. If the only way of accessing personal data was through member login, this could be a breach to access rights, because a regular citizen has the right of obtaining data controllers’ details without being a client/member. However, we did not observe the member login feature as a barrier, because other means of facilitation were also offered in all these cases.

In the case of CCTV in a local store, the site allowed direct access to data (review of footage) if there was a ‘sound’ reason for this. The store manager did not specify what such reason
might be, and when asked again, he mentioned that access request could be made through the police.

In general, the private sector agencies offered good facilitation through providing a number of ways to access the data controller. However, the case of CCTV in a local store was somewhat unclear. Although we have categorized the case of CCTV in local store as a successful case, due to the immediate response of the store manager, this case does bear some similarity to the other CCTV sites that will be discussed in the section below.

Approaches of Denial

The private sector agencies that denied access to data controller details were 4 of 5 CCTV system cases and all three online service providers. The former consisted of CCTV in a public area, CCTV in a bank, CCTV in a department store and CCTV in a transport setting. The latter were the social network (Facebook), the e-mail provider and search engine (both Google).

In the cases of CCTV systems, the informants were very hesitant in providing information about the data controller, and also very inquisitive to why we were making the request. Furthermore, apart from the bank, it was rather difficult to locate anyone at these sites that knew who we could contact for a lead to this question. In the cases of CCTV in public area and the department store the assigned security company would not offer any information whatsoever, and said that only the police could obtain the data acquired by the CCTV systems. Furthermore, these sites were very defensive and limited in their response. The informers of the bank and for the transport setting however informed us about the duration to which the data would be held, and mentioned that this data could be accessed through the police. Although all 4 sites referred to the police as the “lead” for further information about the data controller, the latter two sites were more open about the reason for this procedure. They emphasized that a prominent reason to access such information was if it concerned a criminal act. It was puzzling to why these CCTV sites were so hesitant to allow access to the footage, when the local store site allowed this in particular cases having a “sound reason”. However, as mentioned earlier, the local store manager also referred to the police when probing for more details of access to data.

In the cases of the social network, the e-mail provider and the search engine, we did not find any details about the data controller. The means of which we could contact the sites were through various online requests and through online content download. The findings for these sites are explained further in the following section.

Online content

Although internet browsing was important for conducting this preliminary research, this mostly enabled us to obtain the telephone numbers of the relevant sites. On the one hand, this choice was made as it provided a methodological advantage due to time constraint; the opportunity to interact with an actual person was more time-efficient and allowed direct questions about the data controller contact details. However, this choice was also made due to the general impression of (lack of) availability of data controller information on the websites of most sites.

Out of 33 cases, two private companies, namely the insurance company and mobile phone company, provided sufficiently detailed information about the data controller and the

---

38 Please note that the site we contacted for obtaining information about CCTV in public area was a center with cameras also covering public area.
procedure of obtaining personal data information online. For the cases that concerned
domains of the web, such as the social network website, the search engine, the online gaming
and the e-mail provider, only the online gaming website provided several means of contact in
order to obtain data controller information. For the remaining sites we found contact
information for general contact, but no contact information specific to that of a data
controller.

Some sites, such as the site for banking records, specified the scope and use of personal data
on their privacy policy page. However, it was not specified whom to contact for more
information on this matter. Furthermore, a number of websites provided only general
information about their privacy policies. However, this information was primarily related to
the privacy policy of accessing the webpage, and not specifically linked to the entire scope of
services provided by the organization. An example of this may be seen on the website of the
public transport service, in which we tried to obtain the contact information of data controller
of CCTV footage. Their privacy policy page highlights the use of cookies on their website
and outlines the privacy policy related to electronic transportation tickets but fails to mention
how to access CCTV footage. Another example of a privacy policy page outlining privacy
with regards only to web access and cookies was the national children’s charity website.

In the cases of the social network, the search engine and the e-mail provider, we did not
manage to locate ‘satisfactory’ contact information of the data controller. For the social
network (Facebook) we only found an online query form (in Norwegian), and the option to
download all personal data (defined as all information one has on a Facebook account) after
login to the website. In the cases of the search engine and the e-mail provider (both Google)
no data controller information was found. The only means of communication as such was a
“trouble-shooter” option in English, with fixed categories of “problems” that could be
submitted. However, in order to use this option, the website required personal login. Due to
this, we did not pursue the search for data controller information.

In these three cases we noted two particularly interesting findings. Firstly, there were no
means of direct communication with the data controller, as the query form and trouble-
shooter were not designed for this purpose. Secondly, member login was required in order to
obtain personal data or to enable communication at all. Thus, in a best case scenario, one
could obtain personal data information, but not actually get hold of the responsible party
controlling the data. Furthermore, in all cases where personal data could be obtained through
member login, we found that such requirements shift access rights of a lay person to that of
being a client/member. Thus, a lay person may not have the public right to check the details
of the data controller prior to becoming a member/client.

It must be said that these websites had an extensive privacy policy page compared to other
sites visited. Although these sites provided such a wealth of detailed information about legal
concerns and rights, this information was far from being clear when it comes to the relevant
contact information of the data controllers.

CCTV and signage

In Norwegian data protection legislation, proper CCTV signage is to be considered a basic
requirement. More specifically, this implies that the data controller draws “clear” attention to
all CCTV systems by means such as signs (or other) of the area that is under surveillance;
whether the surveillance includes sound recording; and the identification of the data
controller (cf. the Norwegian Personal Data Act (2000), Section 40). By clearly informing
citizens of the ongoing collection of personal data, the enterprise promotes transparency and
upholds legal requirements. Unfortunately, in the cases dealing with CCTV in Norway, the findings have been rather poor.\textsuperscript{39}

In all cases concerning CCTV, including CCTV in a transport setting, department store, local store, bank and public area, there have been few (if any) CCTV signs (cf. pictures below). Furthermore, the locations of the signs were, in general, not optimal, causing poor visibility due to disturbing background or located at remote places far from the actual CCTV cameras. Finally, all CCTV signs that were found were small in size and contained no contact information about the data controller. It should be noted that there is no standard template for CCTV signage, and that signage is generally provided by the company installing the system or operating it.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{image1}
\caption{CCTV signage at local store: Unfit background causing poor visibility of sign.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{image2}
\caption{CCTV signage at department store: poor visibility due to the size of signage, the sign location remote from the actual camera and in a place where few customers pass.}
\end{figure}

\textsuperscript{39} When we shared this finding with the official of the Datatilsynet during an informal meeting, they acknowledged the poor status of signage implementation, and told us that several citizens had previously contacted them concerning the issue of signage. In the recent past, the DPA has carried out controls in the main streets of the capital to ensure that all shops using CCTV were doing so according to law. So far, the policy of the DPA is to insist on the acquisition of good routines at the level of companies rather than in the enforcement through fines (informal meeting held in the premises of the Datatilsynet in Oslo, 4\textsuperscript{th} September 2013).
Pictures 4 and 5 – CCTV signage at public transport – metro stop: lack of data controller details, and too small considering the size of the surveillance area.

Picture 6 – CCTV signage at public transport – bus: This single sign for an extended rush-hour bus consisting of 4 doors. Although quite visible, it was only apparent to those in the front section of the bus, and the sign lacked data controller details.

Sensitive Personal Data

During our interactions with data controller representatives, it was sometimes possible to discuss with the members of staff which kind of data is collected by specific sites. Although not conducting a comprehensive research on this issue, it became apparent that sensitive personal data are (potentially) collected in sites that would not be deemed, *prima facie*, as sensitive.

For example, while it is obvious that a general practitioner is, per se, a sensitive site, given that she manages medical records, a primary or secondary school is generally not considered automatically a sensitive site. However, the interview regarding school records revealed some interesting points about the processing of sensitive personal data. Speaking about the

---

40 According to the Norwegian Personal Data Act (2000, section 2) sensitive personal data is described as: “information relating to a) racial or ethnic origin, or political opinions, philosophical or religious beliefs, b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act, c) Health, d) Sex life, e) Trade-union membership.”

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
information stored in school records, the interview subject reported that these also contain notes about disabilities/illnesses as well as information about exemption from particular classes. The former is regarded as sensitive personal data as it contains information related to personal health. An example of the latter could be exemption from classes such as *Norwegian Nynorsk* or what was formerly known as *KRL*. Exemption from these subjects would imply that the student is of a minority background and has a different religious belief than Christianity. Thus, schools in fact control and process data that may be regarded as sensitive personal data.

Furthermore, there may be other less apparent incidents where sensitive personal data is processed or controlled. In such cases such a processing is not necessarily regulated by the specified legislation concerning handling of sensitive personal data. In particular, data collected by CCTV could be a source of exposure for sensitive personal data. For example, a CCTV camera in a sex-shop or a pharmacy could indeed expose personal data about a subject that is defined as sensitive. Furthermore, CCTV cameras in public areas capturing footage of a subject entering politically affiliated institutions or religious sites do capture sensitive personal data. As explained in the previous sections, it has been challenging to obtain access even to the details of the data controller of CCTV footage. In most cases, the request for obtaining access to such data must be redirected through police authority. This makes it difficult for the data subject to access personal data, and to understand whether the data collected are potentially sensitive.

**Concluding remarks**

To summarize, this ethnographic-like research exercise highlights the following trends:

- The average approach of public agencies is one of denial, or at least lacking facilitation. The staff seemed to be uninformed about data protection regulation, and either hesitant or lacking appropriate information about the data controller.

- The public agencies categorized under the domain of security imply a rather time consuming and bureaucratic procedure for identifying the specific information about data controller. This is due to the fact that ‘the police’ are mentioned as the general data controller, in which no detailed information is given about the office or entity particular to each respective case.

- The average approach of private agencies was, with the notable exceptions of CCTV and internet-based site, much more facilitating. The staff seemed more prepared to answer questions concerning data protection and could provide information about the data controller.

- When it comes to CCTV sites, the claimed need to contact the relevant police office raises some concerns as to the facility to identify the responsible data controller. It should be acknowledged that the text of the PDA risks triggering misunderstanding and unduly limiting the right of access of data subjects. However, if access to the information concerning the relevant data controller is only to be obtained through police, this should be considered as a sort of denial tactic.

- Online sites, such as social network, email provider and search engine, have a somehow frustrating approach: while they all provide some sort of interaction with

---

41 Cf. [http://www.human.no/Livssynspolitikk/Religion-og-livssyn-i-skolen/?index=2](http://www.human.no/Livssynspolitikk/Religion-og-livssyn-i-skolen/?index=2)

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
the data subject or concerned person (e.g. via online forms or trouble-shooters), they provide little satisfactory information in terms of contact details. Furthermore, the possibility to interact with them is limited via membership, so that only registered users can log-in to require further information.

- Establishing too high barriers to access one’s own personal data could have a negative effect on the capacity of everyday users to assess whether their sensitive data are collected in sites that are, apparently, not sensitive (shops, public spaces, etc.).

Finally, it should be noted that the Datatilsynet maintains a register of all the data controllers, which is publicly accessible. However, Chapter VII of the Personal Data Regulations establishes a very long list of types of processing that are exempted from the duty of notification to the DPA, and it is possible to assume that all data processing systems that should be notified are, de facto, registered. Therefore, a potentially helpful tool to improve the ability of data subjects to locate and contact data controllers is strongly weakened.
SUBMITTING ACCESS REQUESTS IN NORWAY

Introduction

This country report reflects the experiences of submitting subject access requests to 15 organizations and institutions operating in Norway. The selected data controllers are either physically located in the country or, at least, providing services in Norway. They include both the public and the private sectors. The methods used to get in contact with the data controller have varied, and so has the quantity and quality of the responses (if any) received and of the relevant personal data disclosed.

This exercise has no ambition to provide an exhaustive assessment of the effective practices of data controllers when it comes to responding to data access requests. However, this case study permits us to identify and analyze some specific features of these practices, and to note some recurring challenges for data subjects attempting to exercise one of their key data protection rights.

Methodological remarks

The methods used in the case study were mostly drawn from the overall protocol designed by the project coordinators. The ethnographic procedures proposed by the University of Sheffield were adjusted in the course of the research, so to be responsive to the specific conditions in which it was carried on, to the interactions with the data controllers themselves, and to the specificities of the country.

In practical terms, different solutions were used in the process of getting in contact with data controllers, both to identify the most relevant contact and to submit the data access request. They ranged from phone to company websites, from email communication to online chat with customer services, to visits to the data controller site. The research team opted for the easiest choice when it came to getting access to the relevant contact. Then, the team used the seemingly most adequate channel of communication to send a formal subject access request. The text of the request was based on a common template originally drafted by the project coordinators, and was both fine-tuned to reflect national legislation and translated in Norwegian. The most common way of sending the initial request was by normal mail (nine cases), and by email for the rest (six cases).

The research team selected the data controllers to be contacted following general indications from the project coordinators in terms of categories (types of services offered; national/multinational; public/private). Whenever possible, the research team approached data controllers that play a key role in their specific sector.

The bulk of the research was carried on between September 2013 and March 2014. Field notes were taken all along the experience. They constitute, together with the formal replies from the data controllers, the main material at the base of this report.

---

42 The full list of the 15 case studies carried on is provided below. The list includes the name and type of data controller addressed. For each case study, a case file has been drafted, consisting of an exhaustive summary and some further annexed documents, e.g. the data access requests and relevant copies of the interactions with the data controllers.

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
The division of the different sections in this report seeks to highlight the dominant traits identified during the process of making a subject access request and analyzing the content of the answer. Reference is made to the specific sites throughout this report, and further detailed information can be found in the case-by-case summary below.

<table>
<thead>
<tr>
<th>Public/Private</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Public</td>
<td>CCTV in open street</td>
</tr>
<tr>
<td>2 Public</td>
<td>CCTV in a transport setting (metro station)</td>
</tr>
<tr>
<td>3 Private</td>
<td>CCTV in a bank</td>
</tr>
<tr>
<td>4 Private</td>
<td>CCTV in a department store</td>
</tr>
<tr>
<td>5 Public</td>
<td>Local authority</td>
</tr>
<tr>
<td>6 Private</td>
<td>Banking records</td>
</tr>
<tr>
<td>7 Private</td>
<td>Loyalty card (air miles)</td>
</tr>
<tr>
<td>8 Private</td>
<td>Loyalty card (supermarket)</td>
</tr>
<tr>
<td>9 Private</td>
<td>Advanced passenger information</td>
</tr>
<tr>
<td>10 Private</td>
<td>Mobile phone carrier</td>
</tr>
<tr>
<td>11 Private</td>
<td>Amazon</td>
</tr>
<tr>
<td>12 Private</td>
<td>Twitter</td>
</tr>
<tr>
<td>13 Private</td>
<td>Facebook</td>
</tr>
<tr>
<td>14 Private</td>
<td>Google</td>
</tr>
<tr>
<td>15 Private</td>
<td>Microsoft</td>
</tr>
</tbody>
</table>

**Overall summary**

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
Language

All the initial subject access requests were drafted and sent in Norwegian, even to entities not formally based in the country. It should be noted that the researcher who acted as the data subject in this research was neither Norwegian nor able to speak Norwegian. As the other two members of the team are fluent in Norwegian, this enabled us to explore in some detail the issue of language.

Significantly, all the data controllers of multinational sites replied to the request in English rather than in Norwegian. This is particularly interesting in the case of Microsoft, where the initial response came from the Norwegian branch and was signed by an officer with a Norwegian-sounding name, but the response was still written in English. It may be that they were trying to be helpful as they recognized that the name of the data subject is self-evidently not Norwegian but they did not have the courtesy to check that we could understand their English response.

Though the automatic switch of language probably does not pose a problem for many Norwegians, the technicalities of data protection legislation and the use of legal terminology may also transform the use of English into a potential barrier in the exercise of data access rights. In particular, the switch to a foreign language may inhibit the full understanding of the response, and may not facilitate possible follow-up questions and exchanges.

For example, in the case of Advanced Passenger Information records, the officer to whom the researcher communicated in the online chat forum for customer service enquiries responded in Swedish and not in Norwegian. This is not so an uncommon experience in Norway and, for the most part, Swedish is a language close enough to Norwegian to be approximately understood. However, when it comes to specific terminology, the possibility of misunderstandings cannot be ruled out, as many common Norwegian and Swedish words are very different. In this specific case, even if the researcher strived to keep the language used as simple and clear as possible, despite the fact that the conversation revolved around something as technical and “challenging” as a subject access request, the chance that the officer did not understand completely what the data subject was asking for remains very high. The potential feeling of being “lost in translation” is further reinforced in the cases where the communication does not take place with somebody clearly trained for responding to data access requests, and when no direct access to the relevant responsible person is made easily available.

In several other cases, the use of English proved to be successful, and this seems due to both the language competences of the research team and the direct contact with more trained staff. From this perspective, we could consider the possibility to switch towards a different language as a good practice whenever this does not hamper the communication with the data subject and when it facilitates the contact with the most relevant offices of the data controller. Indeed, it could be speculated that continuing to use Norwegian when the response to the subject access request was in English would probably have further slowed down the process.

At the same time, it should be noted that the identification of the data controller details through websites in Norwegian or on CCTV signage in Oslo would have been difficult without knowing the language. Little information relevant to the lodging of a data access request was available in English, making it natural to expect a subject access request to be sent in Norwegian and imposing a high barrier to non-Norwegian speaking data subjects.
Public (space) versus Private (space)

This study covers only three sites that are formally identifiable as public authorities: the Skattedirektoratet (the Norwegian Tax Authority), the Oslo metro system, and the CCTV system located in an open public space. Among these, it should be noted that the Oslo metro system is a semi-public authority. This small sample is largely due to the fact that the data subject/researcher, whose personal data we sought access, had not lived in Norway for a very long time. This excluded some potential data controllers (i.e. vehicle registration) and, in general, made the administrative history of the data subject in Norway quite thin.

The approaches and responses of the three entities were very different from each other. The worst case was the CCTV system located in an open public space: no appropriate signage was present next to visible cameras, fostering a feeling of uncertainty concerning the relevant data controller and the effective use and aim of the cameras. Based on our general knowledge, the research team had to assume that the relevant data controller is the Oslo Politiet (Oslo Police District). Not only did the team receive no footage, but also the interactions with the Oslo Police District were not very smooth. The Oslo Police District seems to have no specific staff dealing with this kind of requests, which increases the possibility of misunderstanding and hampers the communication with the data subjects. For example, the Police Inspector who dealt with our request insisted we use the generic email address of the Oslo Police, rather than communicating directly with him.

The other two cases turned out to be more positive experiences, but still not particularly smooth. In the case of the local authority (the Tax Authority), the final response was quite exhaustive, even if not always easy to interpret and fully understand, and the interactions with the relevant office were professional and polite. However, the full response was obtained after many delays and took a very long period punctuated by excuses. Given the key role of this public authority in both social and administrative terms, a more reactive response would have been expected.

Finally, the overall assessment of the CCTV system of the metro can be considered the most positive among the public sites. The research team received no footage because images were deleted (according to the information provided by the data controller) seven days after recording, as it is generally required by the relevant legislation). The information about the functioning of the system and the relevant specific legislation applying to it can be considered satisfactory. The same data controller also stated that the disclosure of the footage would have put at stake the privacy of other data subjects. Furthermore, the quality of the interactions with the data controller was both professional and attentive.

If a general conclusion can be drawn from this small sample is that the existence of specifically trained and responsible staff can make a positive difference in the approach to data subject requests. This is especially the case since there are no formally recognized and simplified channels to lodge a data access request, and that the Norwegian Data Protection Authority has put no official template at citizens’ disposal. Therefore, the impression is that each data access request is very time-consuming for both the data subject and the data controller.

The same general insight seems to be valid also when it comes to the private sites. In these cases, it is even more difficult to establish consist trends, despite the wider sample.
Leaving aside the cases of some multinational companies (discussed in the following section 2.3), there is little information at disposal for data subjects interested in lodging a data access request. In some cases, it is extremely hard to either identify the relevant data controller (e.g. in the case of the CCTV system in the large department store) or to directly contact the seemingly most relevant office or department. However, the private sites that were more responsive (despite some delays) were those that seemed staffed with properly trained personnel, or where the front office was finally able to identify the relevant colleagues within their own organization.

For example, the best practice was found in the case of Norwegian. Even if the research team needed to send a reminder, the response was rather complete and included relevant personal data. The website was rather clear and accessible, with information on how to contact the data controller. Still, the address provided was a general one, and this created some delays in the response of the data controller, as the request had reached the wrong office. However, the offices were able to fix this error and come back to the data subject with a rather exhaustive response.

The worst experiences were the cases linked to the Norwegian bank. The data subject/researcher lodged both a request to access his bank records and the footage relative to a visit to an agency of the same bank. It was not possible to find proper information on the website relating to data subject access request, and not even on the office dealing with data protection questions in general. Before contacting the general postal address of the bank, the researcher spoke with the personnel of the bank agency and checked the signage next to the CCTV system. While the employees were polite and professional, they were not trained to address data protection questions, so that the conversation did not facilitate the exercise. The signage stated that the data controller was a specific branch of the bank. However, this information is far from satisfactory because the signage carried no relevant information enabling to contact the data controller. Furthermore, when we attempted to identify the contact details of this specific branch of the bank by other means, we were not able to find any specific contact. Both cases were quite radical failures, with practically no follow up to the data access request (apart from a short phone call regarding CCTV footage).

In the case of the CCTV system operated by a large department store in the city centre of Oslo, the experience was pretty similar. Despite the evident presence of several cameras, signage is mostly designed to inform of the presence of the CCTV, but does not provide proper information on the data controllers. At the end, the only solution for the research team was to rely on the website of the department store, which provided no specific information about CCTV but only a generic address. This address refers to a manager within another branch of the company. The manager replied to the follow up request, but without providing any footage or explicit explanation about this decision, and only stating that the CCTV system in the department store is registered and approved by the Norwegian DPA.

While the last two cases concern private companies (actually the same private company –the bank – but two different branches), they can hardly be considered merely private sites. They both have a strong public dimension. The city center bank’s CCTV system also covers open public space used by many people throughout the day. Similarly, the CCTV system located within the other branch of the bank covers a space that is private but of key public relevance. Indeed, as in many other European countries, opening and maintaining a bank account with a ‘national’ bank is not only needed for strictly economic purposes, but also for many other social reasons, including relations with public authorities. Then, even if the bank is a private
entity, physical interactions (such entering into their premises) have also a public dimension for many data subjects.

In sum, the private/public divide seems to have little impact on the attitudes of data controllers. What seems to be the main criterion is rather the existence of properly trained staff, the existence of internal channels with the organization to distribute the requests to the apposite offices, and the clarity of the information provided to the data subjects on how to contact the relevant services.

On the contrary, some data controllers seem to deploy dodging strategies, which hamper the possibility to successfully obtain the required information, or to even properly lodge a data access request. These strategies are not of pure denial, but they rather discourage the request (their submission and their follow up) and are premised on the absence of proper information or a clear channel of communication. For example, in the case of an airline company, it was not even possible to lodge the data access request because all communications had to pass through a customer-service chat (the phone service being de facto impossible to use).

Finally, given their relevance for the public dimension of data subjects’ lives of some private sites, the inability to properly and steadily follow up on data access requests should be considered a particularly negative trend.

**Multinational companies**

All the multinational companies somehow responded to the subject access requests, even if they were not all responsive in the same manner nor they all provided the personal data requested. Still, some common features can be drawn from this experience.

According to the Norwegian Data Protection Act (DPA) § 24, the data controller can claim a signed consent form from the data subject prior to disclosure of information. The first general finding is that none of the 15 data controllers we contacted asked for such a form, except from Twitter and Amazon who both requested a further confirmation of ownership to the data. Facebook and Microsoft acted similarly and requested confirmation of ownership of the email address, and not the identification.

As mentioned above, all multinational data controllers switched to English instead of responding in Norwegian, and without asking permission to the researcher/data subject. While the shift to English was not a challenge for the research team, it highlighted a more implicit challenge: the clarity of the language used to respond to the data access requests and to explain the type and quality of the personal data provided (if any). Indeed, even when personal data were provided (e.g. in the case of Facebook and Twitter), it was not always easy for the researcher/data subject to ‘make sense’ of the data received, or to properly assess how the personal data at stake are effectively used by data controller. For this reason, it should be noted that the choice of a specific language can make a big difference, and that even if data subjects are fluent in a foreign language, their understanding of the response can remain only partial. Then, to some extent, data controllers’ initiative to switch to English may become a more or less intentional strategy of inhibition.

---

43 Obviously, the ability to ‘make sense’ of the disclosed data is not only linked to the use of a more or less familiar language, but also to the clarity of the information provided as explanation by the data controllers, the very content of the data and the format chosen for storage and disclosure of the requested data. On these aspects, cf. the paragraphs below.
Another common trend that emerged in the cases of multinationals is that the interactions with data controllers were, in general, more structured and required several interactions. For example, Facebook, Google/Gmail and Microsoft provide some sort of online forms which are supposed to channel data protection or privacy related questions or requests. On the one side, this may facilitate interactions with data subjects, but, on the other side, it generally pre-empts the proper lodging of a more extensive data access request. The Facebook solution resulted in the most adequate in relation to the kind of request the researcher/data subject wanted to submit, especially compared with the other two systems.

In the case of Amazon and Twitter, the communications were structured not through the existence of a specific online form, but by the procedure set in place by the office responding to the requests. The procedure initiated by Twitter was clearer to follow from the beginning, and appeared a standard routine. In the case of Amazon, the communication was de facto lost between the relevant departments. The researcher/data subject received a further email in April 2014. The email was sent from a potentially relevant department at Amazon, and provided the password to access the “documents attached to the previous e-mail”. However, no “previous e-mail” with attached documents had been previously received.

In general, the availability of a structured procedure can be considered a facilitating strategy, especially when compared to the cases mentioned above where it is difficult to communicate with the data controller and their representatives. However, the effective way in which the procedure is structured can either further facilitate or inhibit specific questions. This is particularly evident when it is not possible to upload or send the data access request as the data subject has drafted it. In other words, the design of the channels of communication already function as a strategy of data controllers to sift and tune the data access requests. The potential risk is that specific questions of the data subject – even if based on legitimate data protection claims – are excluded or marginalized from scratch.

The force of the design is also evident in the two cases in which personal data were disclosed: Facebook and Twitter. The two companies provide these data in very different formats, and with a different amount of ‘meta-information’ about the signification and role of the data disclosed. While this may seem a marginal issue, when the data subject is faced with a rather large amount of information, it becomes necessary to be able to inspect the disclosed data in way which enables the data subject to understand it, not least to understand if the data-set is complete.

Finally, even in the cases where no personal data were disclosed or no proper response was provided, the interactions with multinationals were in general pretty time consuming. They often implied several email exchanges, the submission of further information on the data subject and even the use of multiple channels of communication (such as fax, email and online forms). Again, this is a rather ambiguous insight: on the one side, the back-and-forth between the data controller and the data subject had a reassuring effect: attention was dedicated to the dossier and it was possible to further clarify some points. On the other side, the need to invest so much time may prevent data subjects from properly follow up or even repeat the exercise in the future.

Process and content
When analyzing the different sites, it became evident that at least two different aspects of the data controllers’ responses had to be assessed: the process and the content. We understand by content the effective response that was, or not, delivered by the data controller, and by process the practices of the data controllers as emerging in the interactions, or lack of, with the data subjects.

Both in the case files and in this report, this differentiation has proved fruitful, as one of the insights gained from the subject access-exercise was that the process of contacting the data controller could be regarded as positive whilst the actual disclosure or quality of the disclosure could be negative. Furthermore, the disclosure of data was positive in some cases, even though the process of obtaining the data from the data controller could be considered negative.

Regarding process, several issues can be highlighted. First, both in the case of Google and Microsoft, it should be noted that no specific employee or department seems to be designated to respond to subject access requests. In the case of Microsoft, this became especially clear as the subject access request was sent back and forth between many customer service officers, and the data subject was copied in to correspondence between the employees of customer service, giving instructions on what to write to the data subject. Apart from being unnecessarily comprehensive and perhaps a bit clumsy, the process of contacting Microsoft was also the least smooth of all the sites.

Second, a few data controllers, after establishing the initial contact, promised to send the data subject a response or additional data, but failed to do so. This was the case for the mobile phone carrier, who promised to forward the location data, and the CCTV data controller in the bank, who after calling the data subject, promised to get back to the researcher/data subject neither of whom did so.

Third, when evaluating the success of the process of obtaining the personal data, not only the process of locating the data controller and making the initial subject access request must be taken into consideration, but also the continuation of the process. This means that the facilitation of making follow-up questions is also important for a process to be successful and complete. Where follow-up enquiries are necessary, it is greatly facilitative to have a named and dedicated officer dealing with our request rather than having to start again with a new and anonymous entity. This was the case in our request to Twitter from whom we got an answer from a named officer who was able to respond to our follow-up questions with ease.

A mechanism that could ease the process of both making and processing a subject access request is the use of a common template. It should be noted that in May 2014 (shortly after the end of the empirical phase of this research, the Datatilsynet introduced a template for subject access requests (“Datatilsynets innsynsmal”))44. Given the recent release of the template, a detailed analysis of this template is out of scope for this study. However, some broad features of the template can be highlighted. First, the template of the DPA specifies the right to access general information about the processing of personal data by the company at stake, and also the right to access the personal data of children under the age of 15 or other individuals by the power of attorney. Second, the template gives data subjects the option of requesting access to either all their personal data held by the company, or to specify their own request (e.g. data gathered within a certain time period, data stored in a special system etc).

44 The template can be found online at: http://www.datatilsynet.no/Global/04_skjema_maler/Innsynsmal.pdf.

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
As the template does not mention CCTV explicitly, this would be where one would specify requests linked to disclosure of CCTV footage. Third, the template also describes the right to access information about "the security measures relating to the processing of your personal data" ("sikkerhetstiltak knyttet til deres bruk av personopplysninger om meg"). Finally, the template gives the option of receiving the information by email, but leaves it up to the company at stake to decide if this method is justifiable. The second part of the template is a full page describing the rights and duties regarding data access, with multiple references to the relevant national legislations.

In the cases where a template was available on the websites of the data controller, they were less than facilitative for the making of a subject access request. This was the case for Microsoft, where an online form had to be used, which did not fit the scope of the full text of the subject access request. This leaves a room for misunderstandings and delay caused by the fact that the information is not complete. For instance, there are no contact details for the data controller and no explicit procedures outlined to follow when making a subject access request.

As mentioned above, although lacking a template for subject access requests, several of the companies provided downloading tools or log in options as an alternative route to gaining access to one’s personal data. This was the case for Facebook and partially also the Norwegian Tax Authority. In the case of Facebook, the initial response from the data controller stated that there are several ways of accessing your personal information, and one of them is “from your account (ex: on your timeline or in your activity log)”. However, given that personal data on Facebook is more than the sum of what is posted and uploaded to a single account, this suggestion is not satisfactory.

Another similar example was the case of Google, where the initial acknowledgement of receiving subject access request included the sentence “[b]efore you contact Google Inc, however, you may wish to note that you can access most of your own data via your Google account. This saves you the trouble of going through the steps to address a separate subject access request to Google”. As the subject access request that was sent to Google specifically asked for “my personal file, [and] copies of all data relating to email exchange between 5. - 8. July 2013”, this suggestion too is not satisfactory as it would not answer the stated request. Furthermore, one could even argue that the suggestion to “just log in to see” is somewhat misleading, as the information revealed would not be complete in most of the cases.

Regarding content, a few points should be highlighted. First, apart from the data controller of CCTV public transport, none of the data controllers stated that data had been erased due to the legal time limits of storage. Second, and partially related, none of the data controllers notified that the requesting data subject had further rights in relation to the stored personal data. For example, according to both European Data Protection Directive (Article 12 (b) and (c)) and the Norwegian Data Protection Act (Sections 28 and 29), the data subject has the possibility to request erasure, rectification and blocking of the relevant information.

Third, there were occasions when the quality or quantity of the content disclosed somehow ‘exceeded’ the expectations of the data subject/researcher. This was the case for both Trumf - the loyalty card for the large supermarket - and partially for Facebook. In the Trumf case, the data controller was particularly exhaustive in defining what kind of personal data was stored about the data subject, and the final response included a list of the time, the place and the sum of transactions made using the loyalty card. The list also specifies which stores the purchase
has been made within, and how many “bonus points” the specific purchase generated. While this information is considered to be quite exhaustive, the lack of clarity from the data controller in addressing other related issues such as the use of “customer profiles” and whether the company gathers and stores information about the specific products purchased by the data subject (which we can assume would be linked to the creation and use of “customer profiles”, where the data subject gets special offers based on the history of purchases) is evident.

The disclosed data from the data controller of Facebook included pictures that the data subject had uploaded to his personal profile, and these included the meta-data, such as the information about the model of the camera or smart phone use, as well as the date where the photos were taken (although these were not correct in several cases), the “upload IP address”, etc. The presence of this kind of information provided an insight on the existence of data related to the data subject that would not have been available merely by accessing one’s data via the online download tool. However, it was surprising to note that no information was provided about other personal data that would be easily accessible through login, such as the pictures in which the data subject is ‘tagged’ (which most probably contain personal data).

In the case of Twitter, a lot of meta-data were disclosed, but the quality of the content was very hard to understand for the data subject/researcher. Decrypting the meaning and function of the information disclosed would require technical competence, which exceeds what can reasonably be expected from the average individual.

“Why do you want the data?”

In several of the cases where the research team communicated with the data controller by phone (mobile phone carrier) or entered the premises of a store to obtain information about the CCTV data controller (CCTV open street city center), one of the first questions raised concerned the motivation of the data subject request or interest. Rather than providing information about the relevant office handling data protection requests, the question was: why does somebody may want the information? This was not the case in any of the communication by email with the data controllers. Furthermore, the researcher was met with a great deal of skepticism, as several employees in stores visited (to clarify ownership of the CCTV cameras outside) assumed that the researcher was from the police, and even asked if they had to close the store, assuming that a crime had happened outside of their premises. This example illustrates in practical terms the reasoning behind the use of CCTV in public spaces as set forth by the data controller for CCTV public transportation: the use of CCTV is founded in a security-logic, both a proactive and reactive one.

In only one case the data controller contacted the researcher/data subject by phone: in the case of the CCTV in a bank. After receiving the subject access request, a member of staff from the bank called the researcher/data subject asking why the information was requested. The researcher/data subject stated that this was a right put at disposal by Norwegian data protection legislation, as stated in the written request. The conversation had no follow up from the data controller, although the researcher/data subject sent a follow up- request. Such lack of response is particularly strange for two reasons. First, the contact had been clearly established between the data subject and the data controller, and the data subject assured the data controller that processing of personal data was something that was important. The data subject was a member of the bank which information was requested from, making the answering of a subject access request important both from a legal and commercial
perspective. Second, the call in itself was strictly not necessary. The subject access request contained all of the information needed for processing the request, something implicitly confirmed by the data controller who did not ask for any further formal information during the call.

What is possible to sketch in these cases is a sort of strategy of inhibition. The aim seems to oblige the data subject to make extra efforts to justify the need and the relevance of the data access request, and pre-empt the lodging of a request. This brief research cannot tell if the data controllers are deliberately trying to thwart citizens or if the strategy is a sort of perverse effect of the lack of trained staff or internal awareness about data protection legislation. However, the final effect may be pretty far-reaching, as it risks install a sort of suspicion on the intentions of the data subject.

Addressing the question of sharing with law enforcement authorities

In several cases, and without the researcher/data subject having asked for it, the data controller explicitly mentioned law enforcement’s access or relation to the data at stake. This was the case for both the CCTV system operated in the public transportation and Twitter. In the former case, the data controller stated that the reason for denying access to the footage was erasure due to the fact that no criminal incident had been registered within the timeframe of the footage requested. In the latter case, the data controller simply stated that the personal data has not been disclosed to law enforcement.

The rationale behind both of these statements can signal the growing relevance of personal data for security related activities, even of personal data initially collected for other purposes (e.g. in the case of Twitter). Regarding the CCTV public transportation the security-aspect was even prompted as the main reason for the surveillance in itself. Other data controllers mention the possibility of disclosure to law enforcement, as one of the possibilities of third party sharing, i.e. the mobile phone carrier.

The use of emails

The research team noted that some differences emerge in connection with the ways in which the researcher/data subject contacted the data controller. The working assumption was that the use of email was the easiest and most facilitating practice for contacting the data controller. This assumption was largely validated in practice, as in many cases responses were received on the same day in which the subject access request was sent, i.e. in the form of an acknowledgement. This practice is potentially reassuring for the data subject, and leaves a substantial trace that the data controller has well received the request. In none of the cases where the subject access request was sent via mail, did the researcher/data subject receive an acknowledgement via mail. The data controller always responded via email, making this the best option for both getting in contact with, and keeping contact with, the data controller.

This, of course, goes both ways. Also for the data subject (in most cases) the method of sending an email is less time consuming both in terms of sending and receiving, and also cheaper than using traditional mail. Another obvious advantage of using email is the fact that the replies came faster than by using traditional mail.

This also brings back the question of the format of the response, including its material dimension. On the one side, receiving a file (pdf or other format) with the disclosed
information reduces the cost of the overall data access request procedure. It can also permit specific forms of consultation that the paper version of the same information would partially hamper (e.g. searching function of key words). On the other side, it also multiplies the sites where the data disclosed are stocked. For example, receiving via email a file with personal data implies that these data are now retained also by the email provider, etc.

Obviously, this assessment is based on the specific competences of the researcher/data subject, who has regular access to internet and IT devices. Unfortunately, the design of the exercise left no room to verify alternative, less computer-dependent, systems to carry on the data access request and obtain personal data.

**Third Party Data Sharing and Automatic Decision Making**

In most cases the issues of third party data sharing and automated decision making processes were addressed too vaguely and in too general terms. According to the Norwegian Data Protection Act (DPA) (cf. Section §22), the data subject is entitled to information regarding automated decision making if a decision fully based on automated processing is of legal or other significant meaning to the data subject, in which case information regarding the logic employed behind the automated decision making can be requested.

In several cases where full personal data was not disclosed, the data controller nonetheless addressed these issues. This was for example the case for Microsoft. Data controllers addressing third party data sharing in particular were for the most part very generic in the descriptions of this practice, but there were some exceptions.

Even though it is less than perfect, the best practice regarding disclosure of information regarding third party data sharing was found with the loyalty card - air miles - data controller. The data controller included a table in the response to the subject access request, with a description of which companies the personal data was shared within one column, and information about why the data was shared in another column. The same data controller also addresses automated decision making, stating that the data controller “makes some automated decisions based on your personal data for the purpose of customer communication”. And further, that “no automated decisions are taken that are of legal or other significant meaning to you”. The response regarding automated decision making processes is less satisfying in this case, but there are data controllers that address this in a very direct way as well. This was the case for the data controller for CCTV public transportation, where the letter we received as a response from the data controller clearly states that no automated decision making is used.

**Case-by-case analysis**

**Public – Facilitative Practices**

*Local city/municipality authority*

Every individual living or working in Norway comes into contact with the country’s tax authority at some point, as part of the mandate of this authority is to administer the population register. The register forms the basis for the tax census, electoral roll and population statistics. The information in the *Folkeregisteret* (Population register) includes e.g. names, information about child custody, records of the deceased, citizenship and changes in marital status.

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
The initial data access request was in Norwegian, and was sent by mail on the 09.10.2013 to the address listed on the website of the administration as the relevant one if you have a request or question regarding privacy. The website also states that the data subject has the right to get access to his or hers personal data. Regarding the Skattedirektoratet being the data controller for the website, the research team also assumed that this is the case for the processing of personal data at large by Skattedirektoratet.

The data controller replied by email on the 15.11.2013, over a month after our initial request, by acknowledging the receiving of the subject access request, and apologizing for the delay in answering. The data controller informed the data subject that the case was currently being processed and stated that the reason for the delay was caused by the large scope of the request and the lack of staff in the department that usually handle these kinds of requests. Finally, the email stated that the data subject would be informed about the progress. The email was signed with a name, but no title or department to the individual was visible.

No further response from the data controller was received, and on the 10.01.2014, the research team sent a follow up request (also in Norwegian) to the same address as the initial request. On the 17.01.2014 the researcher received another email from the same address, referring to our follow up request, which was received by the data controller on the 15.01.2013. The data controller stated that a preliminary response has been sent via post to the address the data subject listed in the subject access request. Another email was received from the data controller on the 31.01.2013, with an update stating that the data controller assumed that a response would be provided to the data subject “early in the following week”. The data subject responded politely, and also asked if it was possible to receive the information via email, by attaching the information in a pdf file. The data controller responded 11.02.2013, apologizing for the information not being sent the previous week as promised, and stating that the information had now been sent from the data controller. Further, the data controller informed us that they have no possibility to send the documents to the data subject via email, and referring to several sections in various laws concerning professional secrecy, confidentiality and postal mail containing national identity numbers.

The researcher responded on the same day, thanking for the information and stating that the information would be analyzed when it arrived, and that further follow up questions may be necessary. The data controller replied almost immediately, in a very friendly manner, signaling that the data subject was very welcome to ask further questions, and also listed the direct phone number to ease the contact.

The researcher/data subject received the information from the data controller about a week later (approximately the 20.02.2014) – four months after the initial request. The response included a letter from the data controller, summarizing some of the main points from the subject access request, and also summarizing the information in the three annexes to the letter. The first annex is an overview of the processing of personal data according to the first paragraph of § 18 PDA, and includes information about messages regarding the processing of personal data by Skattedirektoratet and the local tax offices. Regarding the second paragraph of § 18 PDA, the data controller states that information about the data subject is stored in the population register, and “in our system” to estimate the tax card. Annex 2 and 3 contains this information. Further, the data controller addresses both profiling and automated decision-making by stating that neither is used here. The use of “here” is interesting, and could serve
as an indication of the fact that it does occur in other contexts. Further, the data controller addresses third party sharing by stating that third parties (e.g. banks, employers, insurance companies etc.) are obliged to report to them. This information is used to create the data subject’s tax return form. This is distributed annually. Finally the data controller apologizes again for the long processing of the request. A senior tax lawyer from the legal department and the officer from the previous email communication signed the letter jointly.

Most of the information provided by the data controller does not contain the personal data of the data subject, but it rather concerns the forms of the processing and of the administration of data in general. Of the three annexes sent by the data controller, annex 1 is a general description on categories of data processed, while annex 2 and 3 disclose the data that the tax authorities is actually keeping and processing about the data subject. The second part of annex 1 refers to the second paragraph of § 18 PDA, and the information is divided between Arkivering (filing), Merkeradiavgift (tax), Folkeregistrering (Population register), Ligningsforvaltning (tax assessment), Arv (inheritance), Nettbasert behandling av personopplysninger, herunder personopplysninger knyttet til skatteetaten.no (Online based processing of personal data, i.e. personal data connected to skatteetaten.no). This information is general, meaning that no personal data related to the data subject is included. It is annex 2 the one that includes personal data, concerning: national identity number, gender, full name, address, citizenship, where the data subject moved to Norway from, country and region of origin and marital status. The “DSF” is mentioned as the source of these data, but the data controller do not explicitly explain what the acronym stands for. Later we learned that is an abbreviation for the central population register (Det Sentrale Folkeregister). Annex 3 is entitled “Forskuddsystemene har registrert følgende for [data subject]” (“The advance systems has registered the following on [data subject]”). The information contains tax- and income information for the previous year, and the current year. This includes e.g. date of tax card being issued and to which address it was sent, tax class, percentage of tax being paid, estimated income.

The overall assessment of the practice of the data controller in responding to the data access request can be considered partially positive and partially negative, both in relation to the process and the content. Concerning the process, the research team quite easily located the address of the data controller on the website of the administration. However, the research team had to send a follow up request after some delay from the data controller. The data controller kept the data subject updated on the progress of processing the subject access request, but there was some delay also in this case (the data controller clearly did not send the response, as claimed in the email, on the 17.01.2014, since the data subject received it about a month later). The data controller was professional and friendly in communication with the data subject, and the data subject was invited to ask further questions and was provided with a direct phone number in order to do so.

Concerning the content of the information received by the data subject, the overall assessment can only be considered as partially positive. Automated decision making is addressed, and so is profiling (even though the subject access request did not include questions on profiling), but when it comes to third party sharing, the response is a bit unclear. The data controller states e.g. “personal data may be disclosed to public institutions which might have use for it”. The full meaning behind this statement remains unclear to the research team.
Regarding some parts of the disclosed information, the descriptions are more specific than for others and the data controller is seemingly more specific in listing the possible third parties to which the data subject’s information may have been shared, but neither of the categories provided by the data controller addresses the issue of third party sharing specifically enough. The general impression of the research team is that the data controller has listed every possible option for each of the categories, and not taken the specific personal data of the data subject into consideration.

The experience of getting in contact with the data controller was partially negative. The researcher used the website of the Skattedirektoratet for locating the data controller, but no response was received for the subject access request within the legal timeframe of 30 days. However, the data controller followed up on the data subject, by informing and updating about the processing of the request. Even though there was some delay, the data subject could feel relatively reassured that an answer would be received. The delay could also be interpreted in terms of the first apology in the email from the data controller, namely the fact that the lack of staff being able to handle the request is an indication of Skattedirektoratet taking the subject access request seriously and wishing to respond in a rightful manner. When contact was finally established with an officer from Skattedirektoratet, the response was rather positive and friendly, and the data controller responded to all of the emails sent by the data subject. Even though this experience was the best in terms of apologizing for delay, and for following up on the delay, the final response from the data controller, containing the personal data requested, did not arrive until four months after the initial request was sent.

Public – Restrictive Practices

Although no significantly restrictive practices in the public sector were found in this research, the above case concerning an access request to the tax authority included several facets of both facilitative and restrictive practices. As such, this case should be considered as representing both positive and negative features and cannot be categorised as being completely facilitative or restrictive.

Private – Facilitative Practice

*Loyalty card (air miles)*

The data subject can register to a loyalty card system through the airline’s website. At the time of booking a flight, the data subject can log in with the loyalty card account and the reward points related to the booking are attributed to the data subject profile.

The initial data access request was sent on the 07.10.2013 by post to a general customer service address located on the organisation’s official website. As per the guidance on the organisation’s website, a copy of the passport of the data subject was attached to the request. The data controller responded after a reminder from the data subject. The response was exhaustive and touched upon each specific request advanced in the data subject letter. Notably, this included:
- the purpose of the data processing;
- the name of the office in charge of fulfilling the daily responsibility of data controller (IT direktør);
- description of what kind of personal data is being processed by the loyalty card system: Kundedata (customer data), CashPoint-transaksjonsdata (CashPoint – transaction data);
- the sources of information;
- the recipients of part or all personal data stored by the loyalty card (especially data processors);
- information about Automatic Decision Making: “(the loyalty card scheme) performs some automatic decision making based on your personal data for the purpose of communication with the customers, but it does not perform any automatic decision making that has legal or other significant effects”;
- the list of personal data used for marketing purposes;
- the list of personal data stored and processed by the system (Profilinformasjon and CashPoint-transaksjoner).

The overall assessment of the practice of the data controller in responding to the data access request can be considered positive. Despite the need to send a reminder (10.01.2014), the responsible office was very polite and professional, and keen in responding within the shorter delay.

The website of the company was clear and accessible to the potential data subjects, with clear advice about how to contact the data controller. However, it should be noted that the address provided in the webpage is the general one, and not the one of the office that is formally in charge of handling requests. A possible effect is that data access requests are not channeled to the competent office upon arrival at the general address (which was the case with the request at stake). As mentioned above, the response was exhaustive and clear, addressing all the questions mentioned in the request.

Twitter

The initial data access request was sent in Norwegian on the 21.10.2013 via email to the privacy-related queries address provided on the company’s website. An automated reply from the supposed data controller was received on the same day. This response stated that we must reply to the mail “to open a ticket for review”. We responded to the email 27.01.2014, making the request again to the same address, this time in English. This request was sent two or three times by responding to the previous message received from the supposed data controller, and to the message automatically generated by sending a new request. On the 27.01.2014, a response was received from the data controller, acknowledging our request, and asking for a statement authorizing disclosure of the information being requested, the data subject’s Twitter name, the email address for the data subject’s Twitter account, and a scanned copy of a valid ID. The same day, the research team responded to this, by sending the requested information, and also opted for sending the subject access request via fax.

---

45 The delay between the initial request and the reminder is due to internal constraints of the research team.
After having “opened a ticket for review” as the data controller asked for, the data controller responded by email on the 27.01.2014. The email was signed by “Twitter, Trust & Safety”, and included an acknowledgement of receiving the subject access request, and asked the data subject to confirm the ownership of the email address by responding to this mail from it. The researcher confirmed this via email the same day and received a response with a number of files containing personal data on the 29.01.2014 (19 files: 17 .txt and 2 .jpg). In the body text of the same email, Twitter Trust and Safety Team provides a brief description for each file (e.g. “USERNAME-email-address-history.txt: Any records of changes of the email address on file for your Twitter account”). The files included, *inter alia*, all tweets and direct messages published by the data subject, the name of the accounts that the data subject was following and accounts that were following the data subject at the time stated in the initial request.

The questions regarding automated decision making or third party sharing were not directly addressed. However, the Twitter Trust and Safety Team stated that “(n)o records were found of any disclosure to law enforcement of information about your Twitter account”. The data controller also acknowledged that “(w)e have not provided all information that may be related to you because of the difficulty of providing it, or because it may not be specific to you or may reveal the nonpublic information of another user or of Twitter”. Finally, a further implicit response concerning sharing with third parties: “(o)ur Privacy Policy at [http://twitter.com/privacy](http://twitter.com/privacy) describes the information that Twitter may collect and use and the limited circumstances in which your private personal information may be shared”.

On 30.01.2014, the data subject acknowledged reception of the files sent by Twitter, and asked again about automated decision-making practices and more specifically about third party sharing (possibly specific examples).

On the 12.02.2014, the data controller replied from the same work address and the same Twitter Trust and Safety team. It stated that “Twitter does not process any personal data about our users without first obtaining their consent through agreement to our Terms of Service and Privacy Policy”. Furthermore, the reply addressed Automated Decision Making, by stating that “We do not engage in any automated individual decision-making about our users that produce legal effects or significantly affects them, as set forth under Article 15 of the EU Data Protection Directive”. Regarding the sharing of data to third parties, the data controller stated that “(…) Twitter does not disclose your private personal information to third parties except in the limited circumstances described in our Privacy Policy (…)”. And more specifically, that “We may share or disclose the user’s information at the user’s direction, such as when they authorize a third-party web client or application to access their Twitter account”. Other circumstances where third party sharing can also happen are also listed in the response, including disclosure to service providers, and disclosure necessary to comply with a law, regulation or legal request.

The overall assessment of the practice of the data controller in responding to the data access request can be considered rather positive, both in relation to the process and the content. Concerning the process, the main problem was establishing a first contact. The research team had to send several emails and a fax. However, as soon as the fax was sent, a first reply was sent within the same day. Since then, the email exchanges with the Twitter Trust and Safety
followed smoothly, with replies sent without any significant delay. The overall process was rather easy to follow and the request for further information (copy of a passport and authentication of the request sent) may be considered appropriate measures to safeguard the security of the data required. There was a clear effort from the side of the data controller to respond to the specific requests advanced by the data subject, especially when the questions were re-iterated. The general feeling is that the Twitter Trust and Safety team was able to further tune a template reply to the expectations of the data subject.

In terms of content, it should be noted that – finally – most of the questions raised in the request were addressed. The data sent by the data controller cover the relevant period, and contain a wealth of information, including meta-data. Somehow paradoxically, such an amount of information (especially keeping in mind that the data subject used sporadically his account) may be problematic for the data subject. Indeed, it is not always clear to the data subject (and probably to many other Twitter users) the meaning and function of the meta-data put at disposal. Furthermore, only little instruction on how to read the data is made available by the data controller.

This experience was quite smooth but still very time consuming, both in terms of email exchanges and analysis of the data received. As mentioned above, the data about the Twitter profile and the use of the same were abundant and included a wealth of meta-data. While this is very positive, it also raises question concerning the readability and usability of this wealth of information for many data subject. It also underlines that data access requests are not very meaningful, unless they are calibrated to specific needs of the data subject.

Private – Restrictive Practice

Banking records

Given that the researcher was already a client of the bank in question, he asked for the contact details of the relevant office during a regular meeting with the bank advisor. The advisor asked a supervisor, who took note of the request, sent an internal message to another office – without providing the contact details to the researcher – and assured the researcher that he would receive further information to his email account. No contact details were received, so the research team decided to use the general address available on the website. As a result, the initial data access request was sent on the 07.10.2013 by post.

The data controller did not reply to either the first data access request (07.10.2013) or the follow up reminder (10.01.2014).

The overall assessment of the practice of the data controller is particularly negative, as no response at all was received. The research team is quite sure that the data controller received the first data access request. Indeed, a different request, concerning access to the footage of CCTV camera operated inside one of the bank’s offices, was sent to the same address on the same day, and was acknowledged by phone (although no response was received thereafter in this case also – see further details below).

Loyalty card (Large supermarket)
The data subject can register to a loyalty card system through the website of the company or by filling and sending via post the paper form available in the supermarkets of the association. In the latter case, the prospective member receives a temporary card and then a proper card carrying the name of the member and the same member number of the provisional card. Then, the member can scan the card at the moment of the shopping. Points are attributed to the member profile, which is also available online through login. Furthermore, membership can be linked to a specific credit card, so that when the credit card is used in a relevant shop, the points are directly attributed without the need to scan the card itself.

As no specific address for data protection related question is provided on the company’s official website, the research team used the general customer service email address which is available online to the general public. The initial data access request was sent on the 07.10.2013 via email and concerned the data connected to the temporary card.

The data subject received data access, but only after a series of email exchange. The data controller responded the same day of the first request, acknowledging reception of the request. The next day (08.10.2013), the data controller stated that the card number mentioned in the request was not linked to a registered card and so stated that it had no information about the data subject on the system.

After receiving and using the definitive card (which has the same number of the provisional one), the researcher submitted a follow up request, via email on the 27.01.2014. The letter also mentioned the fact that points should have been also collected at the time of the temporary card, and required further explanation about this process.

The response to the follow up request was delivered by email, and was divided in two parts. In the attachment, the data controller provided registrerte kundeopplysninger hos (information about the registered customer), e.g. first name and surname, email address, mobile phone number, and medieprofil (media, or customer profile, the meaning of which is not self-evident), etc. The attachment also lists all the occasions in which both the temporary and the definitive cards had been used. These data include date, time and total amount of each purchase, name of the supermarket chain and of the specific stores, etc. This list confirmed that the temporary card had been already used before the first data access request.

The second part of the response is drafted directly in the text of the email. It addresses some of the other questions advanced in the access request. This part of the response mostly refers to, and quotes from, the privacy policy of the loyalty card system. It adds little specific information about the effective processing of the specific data requested. In relation to third party sharing, the list provided includes all the stores that participate to the company’s consortium as well as other branches of the parent company, but it remains vague as to the precise entities that have received the subject’s data. Furthermore, the text says that the data that can be shared include also “informasjon om handlet beløp, (loyalty card)-bonus, produkter, dato og hvor kjøpet er foretatt” (information about the amount paid, the loyalty card bonuses, the products, date and where the purchase has been made). However, the document attached to the reply (mentioned above) does not list which products had been
purchased. Notably, this response does not address the question concerning automated decision making.

The overall assessment of the practice of the data controller in responding to the data access request can be considered only partially positive. The answers to both requests, and to other emails, were quick, and the use of email smoothed the entire process (e.g. no postal costs involved). However, the first response seems to be partially inaccurate as for the existence of data linked to the temporary card. No exhaustive explanation was provided in the second row of email exchanges.

The final response is partially exhaustive as for the presentation of the specific data stored about the subject, but not always clear when it comes to specific categories (e.g. medieprofil). The response to the other questions raised is too vague and too general, with paragraphs copied from the general policy or legislation, and not always related to the questions raised by the data subject. In general, it is not always easy to follow for the data subject.

The website of the loyalty card system provides only little information about the privacy and data protection policy, and it explicitly suggests that one should contact the customer service for any related queries.

**Google – Gmail**

The first data access request was sent on the 21.10.2013 by post and was written in Norwegian. The request was sent to the Norwegian headquarters of the company, the address of which was located online.

The reply from the data controller (Google Norway) was received by email on 24.10.2013. The response acknowledged reception of the request in English. A Receptionist replied on behalf of Google Norway stated that “Google Norway AS does not process any data in relation to Google services, nearly all of which are provided by Google Inc a US incorporated company whose address is given in the Google privacy policy [link]”. The message also noted that “[b]efore you contact Google Inc, however, you may wish to note that you can access most of your own data via your Google account. This saves you the trouble of going through the steps to address a separate subject access request to Google. And it helps to protect your privacy by ensuring that only you as the authorized account holder, will obtain access to the information in the account”. Finally, the same message also mentions the need to pass through a “Dashboard” from the account.

The research team opted to contact directly the Headquarters of Google Inc. (via fax, as no specific email address was available on the website). No further response from Google Inc. has been received since then.

The overall assessment of the practice of the data controller in responding to the data access request can be considered negative. While Google Norway responded to the initial request in very short time, Google Inc never provided a response. There is little information on how, and to which specific office or department, the data subject can submit a data access request.
that does not fit Gmail standard procedure. The standard procedure itself – the so-called Dashboard – is not a proper tool to obtain full access to personal data. Its user-friendliness and the availability of data to be downloaded are very poor (also compared to similar tool put at disposal by other multinationals). Furthermore, no information about alternative ways to obtain the data, or even start a proper data access request, is available on the website. The “privacy troubleshooter”, which is the only way the website suggests to contact them, is of no real use in case of data access requests.

To fax the request again (and in English) to the US Headquarters seemed the most adequate option, but had no success or even feedback at all. Finally, the decision of the Google Norway to address the data subject directly in English (while responding to request formulated in a different language) made little sense (especially since Google Norway is based in Oslo, Norway).

Apart from the lack of response, it should be noted that, while polite and professional, the initial response of Google Norway was not fully satisfactory. While it is very probably that Google Norway is not the relevant data controller, the information about the possibility to obtain data access by login into Gmail are, at best, partially correct. Indeed, only little information beyond the everyday access to the account is finally available. The online tools put at disposal, either the Dashboard or the Privacy Troubleshooter, are far from satisfactory. They do not really permit to submit a proper data access request, nor to easily obtain the relevant data. There does not seem to be an ad hoc office or department dedicated to the handling of data access requests.

Amazon

The first data access request was sent on the 21.10.2013 by postal mail and the request was made in Norwegian. The request was sent to Amazon’s Luxembourg address as per the details provided on the company’s official website.

The reply from the data controller was received by email on 20.11.2013. The data controller responded within one month after the initial request was sent, and so within the 30 days provided by law). The response by email acknowledged reception of the request and stated that they “would be happy to provide you with the Personal Data that we hold about you in accordance with our data protection obligations”. The same email also noted that “before we start gathering the information, so as to protect our customers’ data, we are required to confirm your identity”, and required that “a copy of your passport or driving license or other official identification, and a copy of a utility bill” should be sent to via email, fax or post to the Legal Department.

It should be noted that this first response was directly in English, despite the fact that the initial request was sent in Norwegian. Furthermore, the email was sent not from the offices of the Legal Department but from those of the Executive Customer Relations.

The research team provided the Legal Department, copying the Executive Customer Relations into the response, with the required information via email on the 27.01.2014. Given
that the email exchange was now been carried on in English, the research team also attached a new version of the data access request (in English, and with the possibility for the data controller to focus on more recent data). Given that the Executive Customer Relations (which was only in copy) insisted on the need to contact the Legal Department (via email, sent on 28.01.2014), the data subject opted to also send the required information via fax. No further response from Amazon Legal Department was received several months later. On 04.04.2014, the Legal Department sent an email to the researcher/data subject in which it provided the “password necessary to access the documents attached to the previous e-mail”. However, the researcher/data subject had received no relevant previous email, and thus no relevant documents.

The overall assessment of the practice of the data controller in responding to the data access request can be considered negative. While it is true that the data controller responded to the initial request in due time, the reply required further information about the data subject (including information not strictly relevant to assess his identity, such as the utility bill). This part of the procedure was not clearly stated on the website, and came as a surprise to the data subject. Furthermore, it is not clear to the data subject why further information should be sent to a different department, and why it is not directly the Legal Department the one that replied to the initial request.

The lack of follow-up from the Legal Department left, de facto, the data subject with no access to his data, and even further exposed to the data controller (who now has passport and a partially redacted copy of the utility bill data). While the data subject may have further contacted the Legal Department after more than 30 days without response (as stated in the reply from the Executive Customer Relations), the research team considers the continuous need to follow up as a shift of responsibility from the data controller to the data subject, which further delays or inhibit the enforcement of data access.

Finally, the decision of the data controller to address the data subject directly in English (while responding to request formulated in a different language) is not self-evident (even if the data controller is not established in Norway).

Apart from the lack of response, it should be noted that, while polite and professional, the initial response of the data controller largely shifted the responsibility on the data subject. First, the further data required to identify the data subject are not all particular relevant to this purpose, and still pretty intrusive. Second, the data subject is called to control if any response at all is received: “Please contact us by e-mail if you have not received a response from us within 30 days from providing us with your proof of identity and address”. It is also interesting to note the lack of clarity in relation to the multiple use of the pronoun “us” in the same sentence: do they refer to Amazon.co.uk in general, or to the Executive Customer Relations or to the Legal Department?

Facebook
The initial data access request was sent on the 21.10.2013\textsuperscript{46} via postal mail and was made in Norwegian. The request was sent to the company’s Ireland headquarters address provided on their website.

The reply from the data controller was received by email on 21.11.2013. The data controller responded almost exactly one month after the initial request was sent (just one day after the 30 days time provided by law). The response by email included a link to the online tool that allows Facebook registered users to download their account data.

In the response, the data controller states that there are several ways to access your data on Facebook, either via just logging in to your account or by using an online tool provided by Facebook. In the former case, data access is exactly the same that is permitted when using Facebook for whatever other purpose. In the latter case, the online tool permits to download an offline copy of the data linked to the account. A link to this tool was given by the data controller, along with a step-by-step guide on how to use it. Furthermore, this comes with a warning that the downloaded material can eventually contain sensitive information, so that precautions should be taken when using the tool: “you should keep it (=the downloaded information) secure and take precautions when storing, sending or uploading it to any other services”.

In the end, the data subject decided that the use of the online tool was the best solution available, and clicked on the link available on the first reply. Then, Facebook, on 27.01.2014, sent a second automatic email, announcing that the Facebook data of the user were available for download. The data subject followed the link included in the message and downloaded the data.

The overall assessment of the practice of the data controller in responding to the data access request can be considered partially positive as to the process, and partially negative as to the content. For what concerns the process, it should be noted that the first response was sent mostly within the timeframe established by law. The message was clear and the options at disposal rather easy to understand. However, the reply did not touch upon the specific requests advanced by the data subject, but only referred to standardized practices of the data controller. The download operation was rather smooth and the .htm format of the files received allows search operations.

For what concerns the content, the assessment of the practice is less positive. The data controller response does not address explicitly the questions of the sharing of data with third parties and of the use of automated decision making. It also seems difficult to obtain a non-standard message in case of further follow up. Furthermore, the first response tends to equate the mere login to the profile with data access.

While the online tool permits users to download data that would not be available through the mere login, some kinds of data are still missing: for example the pictures uploaded by other users where the data subject has been tagged and further metadata concerning the use of

\textsuperscript{46}Interestingly, the delayed submission of the first request was not an issue in the exchanges with the supposed data controller.
personal data by third parties. Finally, it is not very clear how the access rights of a data subject that has never been a user of Facebook (but whose data are stored and processed by Facebook) can be enforced.

This experience highlights several interesting aspects of the practice of handling data access requests. First, the messages from Facebook were signed by the “Facebook Data Access Request Team”, which highlights how the multinational has created an office to handle this kind of requests. Attention to data access seems to be confirmed by the existence of a standard procedure and an online tool. Once the researcher opted for accepting to use the tool, the access to data was a rather smooth and easy operation. However, this practice points out some important limits of the use of template and standard forms. While data were rather easy to obtain, no response was given on questions that ‘did not fit’ the procedure: e.g. third party sharing and automated decision making. Therefore, the use of standard procedure has a strong channeling and morphing effect on the way in which data access rights may be enforced. Finally, it should be noted that the Facebook Data Access Request Team used English since their first message, even if the data access request was formulated in Norwegian.

Advanced Passenger Information

The research team began by visiting the company’s official website in order to locate contact detail via which to submit an access request. Using the “contact” link on the main website, a phone number and opening hours for the company’s Customer Service department appears, along with a search function and a list of frequently asked questions. None of the questions relate to privacy at all, and when doing some random searches for relevant terms relating to processing of data (e.g. personvern, personopplysninger, data, = privacy, personal information, data) no relevant hits appear. There is also a list of online contact forms for various specific needs, but none of them are related to questions regarding privacy or personal data. When the research team clicked on the link to get the contact information for the company’s Customer Service department (which appeared to be the most relevant way to channel the subject access request), none of the links or headlines addressed privacy or questions relating to the processing of data. As the research team was not able to locate any specific details regarding the processing of personal data by the company on the website, and privacy is not mentioned at all on the site, the research team chose to call the general telephone number for the Customer Service department listed on the website. The results were negative, as the researcher had to wait in line for a very long time, and eventually had to give up because the exercise was too time consuming. The researcher tried again on at least one other occasion, but also this time, the results were negative, and no contact with an officer from the company’s Customer Service department was established. Further, the research team chose to use the postal address the company suggest on their Customer Service website in the section entitled “if you need to send a letter by post”. As a result, the initial data access request was sent in Norwegian by mail on the 07.10.2013 to this postal address.

No response from the data controller was received, and on the 10.01.2014, the research team sent a follow up request (also in Norwegian) to the same address as the initial request. No response was given to either of the subject access requests.
The research team chose to use the “chat-service” that is available through the main contact-website of the company. The service is presented in connection to the search-function and is described as following: “Use our search function! If your question is not answered, you can ask for personal service through a chat-function”. A search for “personvern” (= privacy) was conducted. No hits were found and the option to open a personal service via chat popped up. The full chat log is translated below.47

You are speaking with Tim
Welcome to the Travel Centre
- What can I help you with?

You wrote: Hi! I’m wondering about where I can send a request to get access to my personal data?
Tim: What exactly do you mean now?
You wrote: I have a general request concerning the processing of personal data at (the airline company), and I’m wondering where I can send my request?
Tim: In that case you are going to have to go through me, and I’ll send your information to the right department.
You wrote: Can’t you give me an email-address or a postal address where I can send it?
Tim: No, such a thing doesn’t exist. It is only through this chat or through our telephone support at 05400 where you can make such claims.
You wrote: OK. So there is no address where I can send a formal request (as I am entitled to according to § 18 of the Personal Data Act)?
Tim: No, there is unfortunately no such address as I said.
You wrote: Can you give me the name of your Data Protection Officer?
Tim: I’m sorry but we cannot give out the names of people working with the company.
You wrote: Ok. I understand, but I am just wondering which department that has to do with privacy/Processing of personal data?
Tim: In that case, it is me who needs to pass this information on to my supervisor who can send it to the right department. I cannot give any more information than this.
You wrote: A lot of companies list this kind of information on their websites, but I could not find it at your site.
Tim: No, that is because there is no such official information available, everything is handled internally concerning issues of improvement and so on.
You wrote: My request does not fit in this format, and I would like to send it via email or post. This is about my personal data, and I do not want to give out these details in this chat.

47 The name of the Customer Care Officer has been changed by the research team. As mentioned above, the languages used in the chat were Swedish (from the side of the data controller) and Norwegian (from the side of the research team). It should be noted that, under Norwegian legislation, “any person” is entitled to obtain from a data controller several information, including those concerning “the name and address of the controller and of his representative, if any, [and] who has the day-to-day responsibility for fulfilling the obligations of the controller” (cf. Section 18, para 1, PDA).
IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
Tim: As I said, this is not possible; it is only possible on this chat or at phone number 05400.
You wrote: If you cannot provide me with an address (to the department that handles this kind of requests) I will ask the Data Protection Authority to assist me in making this request. I do not wish to receive this kind of information through phone or in this chat.
Tim: Like I said, it is only through chat or phone that you can send in this.
Tim: Anything else you are wondering about?
You wrote: Ok. Thanks. I will contact the DPA, and get back to you.
Tim: Ok, I wish you a nice day!
You wrote: Thanks, the same to you!

The overall assessment of the practice of the data controller in responding to the data access request can be considered particular negative both in relation to the process and the content. Concerning the process, the research team tried three options to contact the data controller. First, the research team tried calling the general number of the company’s Customer Service department on several occasions, but no contact was established as a result of this exercise. Second, a formal subject access request was sent to the address available on the website of the company’s Customer Service department to be used in those cases where a customer needed to send an inquiry by mail. No response was given, and a follow up request was sent. No response was given to this neither. Third, the research team chose to use a more untraditional method of getting in contact with the data controller, by using the chat function connected to the search field available on the website of the company’s Customer Service department. The conversation with the Customer Service Officer proved to be unsuccessful as well, and the research team considers the overall practice of obtaining information about the processing of personal data in this case as negative.

The Customer Service Officer did not provide the data subject with any useful information in order for the data subject to make the request, and did not make an effort to put the data subject in contact with colleagues that could have helped. The overall message from the Customer Service Officer was that the only way to make a subject access request was over the phone or via the chat- dialogue, leading the research team to believe that the officer maybe did not understand what a subject access request was.

When asked about the name of the Data Protection Officer, as it might be right that the company does not have one (according to the website of the DPA)\(^{48}\). Although, when the researcher asked for the relevant department for inquiries regarding privacy/ processing of personal data, the response from the Customer Service Officer was that “there is no such official information available”, which is not a satisfying answer.

Furthermore, it should also be mentioned that the denial of the existence of a post address or an email address where a subject access request can be sent, further strengthens the research team’s suspicion that at least the particular Customer Service Officer did not know what a subject access request meant.

\(^{48}\) [http://www.datatilsynet.no/Personvernombud/Virksomheter-med-ombud/#Andre%20virksomheter](http://www.datatilsynet.no/Personvernombud/Virksomheter-med-ombud/#Andre%20virksomheter)
Finally, the lack of information on the company’s websites is also particularly negative. As several methods proved unsuccessful, the last option of using the chat function on offer on the company’s Customer Service website, was positive in terms of process (the research team got through to a Customer Service Officer immediately, and the officer was responsive), but negative in terms of content, since the research team did not obtain any personal data, nor the relevant address of the data controller.

**Mobile Phone Carrier**

The company in question is one of the most common mobile phone carriers in Norway. The research team began by calling the organisation to ask for an address to which they could send an access request. The researcher did not have to wait in line for a very long time before getting through to an employee of the company’s Customer Service department, and asked in a polite way where she could address a subject access request. The Customer Service Officer laughed gently and replied saying that that was a very good question. After some silence from the Customer Service Officer, he asked what the request exactly was regarding, because “we have several departments”. The researcher replied that she had a general request relation to the processing of personal data undertaken by the company. The Customer Service Officer responded that the best thing would be to send an email to the generic Customer Service address, and that an executive officer would forward the inquiry to the right individual. Being an employee of the same department, the researchers found it difficult to understand why the Customer Service Official we were already communicating with could not answer the question of a specific address. As a result, the initial data access request was in Norwegian, and was sent by email on the 07.10.2013 to the general customer services email address.

A first reply from the data controller was received on the same day (07.10.2013). The response was merely a statement thanking the data subject for the subject access request, informing the data subject that the request had been forwarded to the right department, and wishing the data subject a great day. This email was sent from the working email of another official of the Customer Service.

On the 14.11.2013 the final response from the data controller was received by email. The email was sent from the working address of an official from another department and not from the department of Customer Service as the first email. The response did not include any attached files, but only the body text of the email.

The data controller states that the data subject’s claim for disclosure of personal data is met for the last period (01.09.2013- 30.09.2013) due to the fact that the data is not being stored for more than three months. The data controller states that this information will be sent by post to the registered address of the data subject. The rest of the text of the email states that the company are licensed for storing personal data about their customers “med formål fakturering, mm...” (for the purpose of billing, etc…). This information is not very clear, since there is not any additional information on what the rest of the purposes are. The information is stored for three months for the customers who receive monthly bills, and for as long time as it takes for the bill to be settled for the rest of the customers. The data controller does not specify if there is any maximum limit for the storage of data. The data controller
further states that after the relevant period, the traffic data (dvs hvem og når vedkommede har ringt til, sendt sms til mm” = “who and when the data subject has called and texted etc”) is deleted. In this case as well, the use of “mm” or “etc” is not very reassuring, as there clearly is information and specifications that the data controller does not provide. According to the data controller, where the conversation was started (which base station) is also stored for three months, because of regulations from the Norwegian DPA and the license that the company has.

Furthermore, the data controller states that the daily responsibility for fulfilling the responsibilities of the data controller is “leder for CO avdelingen” = head of the CO department”. Exactly who this individual is, or what the “CO avdelingen” means, remains unclear to the research team. The data controller further lists the types of data that is being stored: subscription data (“normal” customer register), data traffic, which phone numbers is connected to ingoing and outgoing calls, where the conversation started (base station), how long the conversation lasted, and eventual customer inquiries. The information is gathered from the registration of the data subject and from generated traffic data. The data controller further states that “vi bruker ikke automatiserte avgjørelser ved” = “we do not use automated decision making by”. The rest of the sentence is missing from the response from the data controller, so regarding automated decision making, one can only assume that automated decision making is not being used. The data controller also refers to “ekomloven” (“Lov om elektronisk kommunikasjon” = “Electronic Communication Act”) and “konsesjonen” (“the license”), when stating that the employees of the company are under professional secrecy, making sure that information is only disclosed to the registered data subject. Police Authorities can, when certain conditions are fulfilled, get personal information disclosed, either by court ruling to set aside the professional secrecy, or that the post- and telecom agency does so. One last possibility for disclosure is that the data subject agrees to disclosure. The last possibility is not very clear to the research team, since the data controller does not state if this possibility includes agreeing to terms and conditions, or if it is to be considered as a separate possibility. Furthermore, the data controller states that “Vi utlewer ikke personopplysninger” (= “We do not disclose personal data”), which seems a bit like a contradiction in terms with regards to what the data controller wrote in the previous sentences. And further the data controller has “(…) en plikt til å levere ut kundeprosjoner til (telefonkataloget/ opplysningstjenesten), men dette kan man også reservere seg mot, ref. abonnementsvilkårene våre” (= “(…) a duty to disclose personal data to (the telephone directory/ “yellow pages”), but you can object to this, referring to our subscription conditions”). Finally, the data controller thanks the data subject for making an interesting request, which brushed up on a good deal of knowledge.

The overall assessment of the practice of the data controller in responding to the data access request can be considered partially positive in relation to the process, but rather negative in relation to the content. Concerning the process, the research team had to call customer service to get the relevant address of the supposed data controller. This did not take much time, but should not have been a necessary step in order to locate the data controller’s address. The research team contacted the data controller via the general address of the customer service. The acknowledgement of receiving the request was given from the customer service the same day. The data controller finally responded one week past the 30-day timeframe, and no follow up request was sent.
The data controller partially addressed the questions on third party sharing and automated decision-making. Regarding the latter, the question was addressed, but the sentence was clearly incomplete, making the statement difficult to understand. Regarding third party sharing, the response from the data controller is unclear as well, given that a statement is made that “we do not disclose personal data” following a section describing the exceptions.

The research team’s largest concern however, is the fact that no additional information regarding traffic data or other personal data was received by mail, as the data controller claimed would happen. The result is that the data subject did not receive any of the personal data requested, but only a body email text describing some of the other traits with the processing of personal data by the company. However, the communication and the process of contacting the data controller were quite positive. Despite the fact that the researcher had to obtain the relevant address to the data controller by the use of phone, the conversation was pleasant, and the officer did provide a quick answer to the data subject. The data controller addressed the questions raised in the subject access request, but no personal data was disclosed.

*Microsoft*

The initial data access request was sent in Norwegian on the 21.10.2013 via email to the email address located on the *Microsoft Norge* section of the company’s website. A reply from the supposed data controller was received on the 23.10.2013. This response included a link to the Microsoft Privacy page, and stated that if we have any further questions we should channel these via an online form, to ensure that our request would end up with the relevant department at Microsoft. The data subject responded on the 27.01.2014 by using the suggested online form, even though it should be noted that it was not possible to insert the full text of the initial request in this form. However, the slightly modified version of the request was sent again in English on the 27.01.2014.

A response was received by email from a representative of the data controller on the 29.01.2014, and this included another acknowledgement, and also asked the data subject to confirm ownership of the email account, to provide information of “(…) the Country/region to ensure that we escalate this request to the appropriate contact” and also confirm that the data subject was requesting access to the personal data. The researcher responded via email on the same day, with the requested information. On the 30.01.2014 another email was received from another Microsoft Customer Service Representative, informing the data subject that our request was being processed, and that they usually resolve such issues within 24 to 72 hours, depending on the complexity of the request. This email also states “if you have not received a reply within 3 business days please respond back to this email for follow-up”, which can be considered a shift of responsibility from the data controller to the data subject to provide the information requested, after the necessary additional information from the data subject is provided to the data controller. The researcher acknowledges this email on the same day. On the 31.01.2014, within the timeframe promised by the data controller, another email was received from a third Microsoft Customer Service Representative, thanking us for the request, and asking the data subject again to confirm the email account from which data is requested, by responding to the email from it. It should be noted that an original email

---

49 https://support.microsoft.com/contactus/emailcontact.aspx?scid=sw;no;1310&wsi=1prcen

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14
containing what looks like instructions for internal use at Microsoft was included in this email. The email is sent from a Microsoft Customer Service Representative and to altogether four recipients appearing to be representatives of the Microsoft Customer Service as well. The original email includes a status update of our request, and also states that “all contact with the customer must be channeled through this e-mail alias, and I will act as your escalation point for this e-mail”. However, the researcher responded and confirmed as per instructions on the same day. Later on the same day, another email was received from the same address of the Microsoft Customer Service Representative as the last one, informing again that they are working on the issue, and that they usually will respond within 24 to 72 hours. Also, again the data subject is asked to contact Microsoft again if no answer is received within 3 business days.

The data subject received another email on the 04.02.2014. In this email, communication between one Microsoft Customer Service Representative and another employee from the “Design Laboratory Inc” was included, and the Microsoft Customer Service Representative (which had already been in contact with the data subject) is asked to help providing an answer to the customer. The data subject responded on the same day, asking how to further authenticate the email address and also stated the country of origin. An email confirming that no further action was required from the data subject was received on the 06.02.2014, followed by an update stating that the data controller is processing the request on the 14.02.2014. The latter email includes several original emails going back and forth between Microsoft Customer Service Representatives.

Yet another email was received on the 26.02.2014, which also included email exchange between Microsoft Customer Service Representatives. This email informs that “(…) we have completed our search of databases within Microsoft for the unique personal information you’ve provided with your request, and did not locate any records”. The data controller also inform that the process of conducting searches for information related to the O365 profile is not finished, and that the data subject will be contacted when this search is finished. The data controller addresses third party sharing rather vaguely, by stating that “(…) Microsoft uses and shares information in accordance to our Microsoft privacy Statement”. Regarding the use of automated decision making, the data controller states that “(…) we conducted a search for the information you provided in your request could not locate any such data”. The latter statement is regarded by the research team as especially unsatisfactory. On the 05.03.2014 the data subject received the final email from Microsoft. This email stated that “(…) we were unable to locate an O365 Home Premium subscription associated with [email address of data subject]”. Furthermore, the data controller states that “If you are requesting data stored in an O365 account provided to you by an organization, please direct your request to the individual department at the organization responsible for administrating the 0365 subscription”.

The overall assessment of the practice of the data controller in responding to the data access request can be considered rather negative, both in relation to the process and the content. Concerning the process, the first problem was finding the relevant address of the data controller. The research team eventually chose to contact Microsoft via the general address. Furthermore, the research team had to channel the subject access request via an online form that did not fit in our request. However, as soon as the request was sent via the form suggested by the Norwegian Customer Service, a first reply was sent within the same day,
and the first non-automated response was received within two days of sending the initial mail.

Since then, the email exchanges with the Microsoft Customer Service Representatives were very extensive, and included several email exchanges between Microsoft Customer Service Representative that were not really necessary for us to receive, and which served as a disruptive element in the process of accessing the data. However, there was a clear effort from the side of the data controller to respond to the specific requests advanced by the data subject, and follow up emails were sent to the data subject to inform of the status of the process. The general feeling is that the procedures to handle this kind of requests mostly rely on internal communication in order to facilitate a reply to the data subject.

In terms of content, it should be noted that – finally – most of the questions raised in the request were not addressed. No data was sent by the data controller, except from the information in body text of the final two emails regarding automated decision making and third party sharing. And even in this case, the information received from the data controller is less than satisfactory. Especially in the latter case regarding the use of automated decision making, when the data controller states that “(…) we conducted a search for the information you provided in your request could not locate any such data”. However, the communication with the various Microsoft Customer Service Representatives went quite smoothly, in terms of politeness and willingness to reply to our email.

**CCTV and signage**

CCTV footage was not disclosed in any of the cases, and there are different explanations that can be contributing to this fact. The data controller for CCTV public transportation was the only one who explicitly addressed the concerns for other individuals captured on the footage, when denying access to the footage requested. This must be considered as a good practice and awareness, given the fact that the official cause for denial from the data controller was that the footage had already been erased due to the lack of security related “incidents” at the requested time.

The data controller of the CCTV in the large department store responded with a disclaimer, which can be interpreted in terms of a shift of responsibility, by stating that the technical equipment used for CCTV in the department store were installed and approved by the Norwegian Data Protection Authority. And further, that if the data subject had any further questions that the queries must be addressed to the Datatilsynet. This shift of responsibility leads to believe that the data controller did not comprehend what the subject access request asked for, and by good will, this do not necessarily mean that the data controller would not disclose the data if further information was given. But, at the same time, the subject access request specified that the Datatilsynet should be consulted if the data controller normally does not handle these kinds of requests. The result is that the data controller showed bad practice, even when advised by the data subject on how to eventually proceed.

Other data controllers for CCTV sites simply did not respond at all to our subject access request. This was the case for both CCTV in a bank and partially for CCTV open street city center. In the latter case, the data controller claimed to not having received the request and did not know what kind of request we were referring to in the follow-up request.
**CCTV Public/mass transport (Oslo Metro)**

The Oslo metro operates six metro lines in Oslo, and carries approximately 80 million passengers every year. *Jernbanetorget* is one of the main stops, connecting several lines, and it is located near the Oslo Central Station. There are many visible CCTV cameras in the underground station area of Jernbanetorget. The research team visited the location twice. The first time, we saw no signage, neither by the entrance nor within the premises of the metro (e.g. on the platform). This led the research team to assume that the metro lines operator would be the apparent point of entry for a data access request, and this assumption later proved to be correct. However, when visiting the site later, the research team used a different entrance (leading to the same area under CCTV exposure), and on this side two signs were visible by the entrance. One sign was mounted on a column on the sidewalk next to the stairs leading down to the platform area, and one on the wall at the bottom of the stairs (See Pictures 1 & 2 below). Despite being quite large, neither of them is very visible: they are mounted high up on the wall, and they are not immediately within the field of vision of by-passers. These signs have the same text: “SMIL! Området er fjernsynsovervåket. Oslo Politidistrikt”, which translates into “SMILE! The area is being surveilled. Oslo Police District”. They do not provide any other relevant information such as the address or contact point of the data controller, or reference to the applicable legislation.

One possible explanation of what does initially seem like two data controllers controlling the same area, could be that the scope of surveillance of the public areas carried out by the police, ends at the bottom of the stairs, and that the metro lines operator is actually the data controller for the CCTV surveillance within the premises. In either case, it is fair to conclude that the practise regarding signage is very poor and confusing.

*Picture 1: Signage on the street by the stairs leading down to the metro*
The researcher first sent the request in Norwegian by email to the email address available on the Norwegian website of the metro lines operator (a communally owned company which operates the metro, busses and trams in Oslo), on the 09.10.2013.

A reply from the data controller was received on the 13.11.2013. This response included an attached pdf file with a letter signed by the Drifissjef (daily manager) of the operator and a lawyer. The body text of the email included a statement that if the data subject wished to receive the response by mail, a more accurate postal address was required, which can be explained by the fact that the initial data access request did not include a city zip code. The letter refers to the request to disclose or be able to view CCTV footage / information for the five minute period specified in the subject access request. Furthermore, the data controller addresses each of the questions listed in the subject access request. This includes the name of the data controller, and that the processing of data is in accordance to legislation. Also, the data controller addresses the purpose of the processing by rephrasing the question to “det antas at spørs målet er hva som er formålet med kameroevervåkningen”, meaning that the data controller assumes that the relevant question to be answered is what is the purpose of the CCTV cameras. Furthermore, the response to this is that the CCTV surveillance is focused on safe and secure departure from the platform, replacing the mirrors that were previously mounted on the old trains. The purpose is also to keep an area under supervision, and this is stated as important in order to help individuals or to take action if unwanted situations should occur. Furthermore, the data controller states that the point of the CCTV surveillance is also a proactive one, and states that “hvis det gjøres kjent at området er overvåket, vil dette gjøre at risikoen for uønskede situasjoner reduseres”, meaning that if citizens are made aware of the fact that there is CCTV surveillance in the area, the risk for unwanted situations will be reduced. Although it remains a bit unclear as to what an “unwanted situation” is, it does not seem to connect directly to the previous purpose of facilitating safe entry and exit to and from
the platform. The proactive logic seems to be more connected to crime prevention, and this is later explicitly stated in the response from the data controller, where the proactive purpose of the CCTV surveillance is summarized as “forebygge kriminalitet og straffeforfølgning”. This can be translated into “preventing crime and criminal prosecution”.

In sum, the purpose of the CCTV surveillance can be seen as twofold: on the one side as a reactive measure, to facilitate necessary intervening action if something is out of order. And on the other side, the purpose can be seen as a proactive logic, where the goal is to prevent such disorder by creating awareness of the CCTV surveillance, making citizens withstand from such actions. The latter purpose can also serve as an explanation as to why most of the camera in the area where the data subject’s exposure took place, were very visible. The cameras were mostly quite large, and had the traditional shape in contrast to other CCTV sites visited by the researchers, where the spherical shaped cameras seems to be the dominating variant.

Furthermore, the response from the data controller addresses the question raised in the subject access request on where the information is gathered from and what kind of personal data is being processed. The data controller states that the personal data is gathered via CCTV surveillance, and that there are very strict rules connected to the processing of these personal data. The recordings are sent immediately to the Driftssentrale, the Control Center, and here the data is stored automatically on a hard drive. Furthermore, the routine is that no one views the recorded images in this process at all. The data controller states that the recordings are deleted after 7 days, and presents this as the reason for denying the disclosure of the data subject’s data. And further, the data controller also states that even if recordings would be possible to disclose, our request would still be rejected, on the basis that other individuals present at the platform at the same time as the data subject’s exposure would clearly also have the right to protection. References to the relevant national legislation are made. During this research, this is the only time a data controller addressed the rights of other data subjects. Regarding the disclosure of personal data to third parties and who these might be, the data controller again states that it has strict routines for the processing of the information from the CCTV surveillance. And further, that “I praksis er det kun politiet ved etterforskning av straffbare handlinger eller ulykker som får utlevert opplysninger”, meaning that it is only the police when investigating a crime or an accident, that can obtain information. The relevant section of the legislation is quoted. Further, the data controller states that no one gets to see the footage stored on the hard disk unless there has been an “incident” (“hendelse”), and that as far as the data controller has been able to find, there has not been an “incident” at the site of our request at the time we are requesting information from. Finally, the data controller stated that information regarding the footage at the time and place for which we requested has not been disclosed, neither to business partners nor to subcontractors. The letter is jointly signed by the daily manager of the metro lines operator and a lawyer.

The overall assessment of the practice of the data controller in responding to the data access request can be considered partially positive, both in relation to the process and the content.

---

50 It should be noted that the data controller did not address automated decision making, but, in this specific case, it should be imputed to the fact that the data subject request, by mistake, did not include a specific question.
Concerning the process, the research team had little problems finding the relevant address of the data controller, as this was quite apparent on the website of the company. However, the research team eventually chose to contact the data controller via the general address. This proved to be successful, as no further action was required from the researchers, and no follow-up request had to be sent. The data controller responded well within the 30-day timeframe, and apologized that because of sickness in the relevant department, the request would take some more time to process, and that the data controller would get back to us when the request has been processed. The final response from the data controller was received only four days exceeding the original 30-day timeframe, which must be considered an acceptable delay.

Even though no footage was disclosed, the response addressed all the questions raised in the subject access request, and the body text of the email with the .pdf response attached, stated that if the data subject would like to receive the letter via post, to please submit a more accurate postal address. The email was sent from the work email of the same lawyer who signed the actual response.

The data subject did not receive any personal data, and in terms of disclosure of information the experience could be considered negative. However, the data controller was provided with an explanation as to why the disclosure of the requested data could not be met, which seems satisfactory. The data controller also addressed the privacy of the other individuals who might be caught on the same CCTV footage, as the only one. Several references to the relevant sections of the national data protection legislation are made.

_CCTV in an open street city centre_

As there was no signage next to the visible cameras, it was hard to identify the relevant data controller. An internet search suggested that many cameras had been disabled, but that the ones on the top of a commercial center, pointing in the direction of the public square were still used by the Oslo Politiet (Oslo Police). Therefore, the research team opted to contact them as data controller.

The initial data access request was sent on the 13.01.2014 by email. No response was obtained so a follow up request was sent on the 28.02.2014, also by email to the same address.

The reply from the data controller was received on 03.03.2014. This response was sent by a member of a unit of the Oslo politidistrikt (Oslo Police District) staff. From the name of the unit, it seems that the response was not coming from staff with explicit responsibility for handling data protection related questions. In the response, the police official claimed that they had not received the previous request and that the Oslo Police District had no information about which cameras the data subject was referring to. Therefore, the police official stated that “unfortunately we have nothing to give access to” (“dessverre ingenting å gi innsyn i”). Furthermore, the reply noted that the Oslo Police District had now opened a case file about the request, but that further request of information should be addressed to the generic email address.

---

51 Interestingly, the delayed submission of the first request was not an issue in the exchanges with the data controller.
The overall assessment of the practice of the data controller in responding to the data access request can be considered negative. First of all, no signage at all is available on the public square, despite the visible presence of several CCTV cameras. This square is an important public place in Oslo, and passing by is a quite common activity, especially being in the city center and next to the main train station of Norway’s capital. With no signage, it was very difficult to identify the relevant data controller and – to date – the research team is still not sure that the Oslo Police District is the relevant one.

Assuming that the Oslo Police District is the data controller, the assessment of the practice should be considered a particularly negative one. On the website of the police there is no specific office or department which is formally responsible to handle data access requests. Thus, the only solution is to use the generic email address, which may have caused the delay in the response from the police itself. While the email sent by the police official was formal and polite, it did not provide useful information, and implicitly showed the lack of structural organization in dealing with such kind of requests.

It should be acknowledged that, given the belated reply by the Oslo Police District, the research team was lacking the adequate resources to further follow up on what appeared a particularly complicate case. In particular, the request of the police staff to keep contacting the generic email address created the feeling that no step forward had been really done so far, and that no specific competent office was going to handle the request.

This experience further confirm the observation that signage concerning CCTV is not a practice well established in Oslo, with little or no relevant information, and often completely absent. Moreover, according to Norwegian legislation, even disabled CCTV cameras have to be treated as operating cameras (unless they are removed), including the use of appropriate signage. Finally, the interactions with the Oslo Police District shows, at least, that this important actor has no dedicated office or department to handle data access requests (no address available online, and no reference to specific officers in the response).

**CCTV Private – Large department store**

The department store is one of the largest stores in Oslo. There are several CCTV inside its premises. Even to a non-expert, the CCTV cameras seem to be of different models (different size and forms) and they tend to be very visible. Despite the presence of several CCTV cameras, there is no consistent and proper signage (see Picture 3 below).
The signage only emphasizes the presence of cameras, but does not provide any information about the data controller and the rights of the data subject. Therefore, the research team opted for relying on the website of the store. However, the website does not provide any further specific information about CCTV, but only a general address. As a result, the initial data access request was sent on the 21.10.2013 by post.

The data controller did not reply to the first data access request (21.10.2013). After a follow up request was sent on the 10.01.2014 (to the same address, also via post), the data controller replied on the 14.02.2014. The response from the data controller was sent by a manager of the Technical and Administration Section of the company. The email was also copied to other two colleagues from the same company and one employee of an external security organisation. The response included no footage nor other data requested by the data subject. Apart from an apology for the belated answer, the reply mostly contended that the use of CCTV in the store is registered and approved by the Norwegian DPA, that the cameras are operated according to regulations concerning surveillance (no specific mentioning of relevant legislation). The data controller states that there is signage outside the building stating that the store is a CCTV-surveiled area. No explicit reason is provided for not disclosing the requested data.

Furthermore, the response does not address the question of third party sharing and automated decision making. Finally, the email invited us to contact the Norwegian DPA to obtain further information.

---

52 The affiliations of the individual copied in the response have been deduced from the email addresses.
The overall assessment of the practice of the data controller is negative. First of all, signage of CCTV is of poor quality, lacking the information needed to contact the data controller or to understand the relevant rights of the data subject. The website of the store does not provide much further specific information, and no address of a specific office in charge of handling data access request is provided. The data subject needed to submit a follow up request to obtain a response. The response is largely inadequate in relation to the questions advanced by the data subject. It is vague and does not offer clear reasons for not disclosing the footage. The reference to relevant legislation is not precise enough to permit the data subject to easily locate and access it.

Given the relative size of the department store and the on-going collection of images from a large number of individuals, the lack of a proper procedure to promote data access rights and handle relevant request is surprising.

**CCTV at a bank**

On the front door of the building there is a signage concerning the CCTV, which mentions that they are operated by a private company. This company has no specific website, has no listed contact on the internet (at least at the moment in which the research was done) and it appears to be part of the bank itself. For these reasons, the research team decided to opt for using the bank’s general address.

The initial data access request was sent on the 09.10.2013 by post. The data controller did not reply to both the first data access request (09.10.2013) and the follow up reminder (10.01.2014). The data subject then received a telephone call (on his mobile phone) from an employee of the bank on the 15.10.2013. The employee implicitly acknowledged reception of the request, but was mostly interested in asking the reason behind the request. The employee first spoke in Norwegian, and when asked to shift to English accepted to change language. The employee asked about the change of language and about the motivation of the data access. The data subject replied that he was aware he had a data access right and that a colleague writing in Norwegian helped him. This was the only interaction with the bank. The data subject sent a follow up request on the 10.01.2014 but no response from the bank was received since then.

The overall assessment of the practice of the data controller is particularly negative, as no proper response was received. Furthermore, the phone call received on the 15.10.2013 was not helpful for the data subject but seemed more addressed to assess the worthiness of the request in itself.

The practice of signage can also be considered particularly poor as the sign does not provide sufficient information about the contact of the data controller and the rights of access of the data subject. Moreover, the website of the data controller is not designed to ease the submission of a data access request.

---

53 The bank provides an online query form. However, this online form is of no or little use: access request is not listed among the possible issues, the platform does not allow attaching documents and it has no space to insert the full request.
Concluding remarks

As already stated, this country report concerning the exercise of data access requests in Norway has no pretention to offer an exhaustive assessment of the overall implementation of this data protection right. However, the study of these 15 cases permits to advance a few insights that should be further investigated in more comprehensive research and, eventually, can be discussed in a wider debate at societal and political level.

From the perspective of the expected end result – the disclosure of the requested data to the data subject and further information about third party data sharing and automatic decision making – the picture that emerges is pretty negative. Only few data controllers finally disclosed the requested data: 6 out of 15. Also, only 6 out of 15 data controllers provided information on third party data sharing, and 4 out of 15 on automated decision making. However, in some cases, data controllers did not disclose data but provided further information on third party data sharing or/and automated decision making, and, *vice versa*, some data controllers who disclosed data did not respond on the other requests.

In many cases, the practices of data controllers were far from satisfactory from a data subject’s perspective. Most of the access requests became very time-consuming, and required follow up from the side of the researcher/data subject. Then, when these interactions did not result in adequate responses from the side of data controller, the exercise became quite frustrating. In several cases, it could have seemed reasonable to refer the lack of (adequate) response to the national Data Protection Authority: this was the case in at least 5 cases out of 15.54 The research team decided to abstain from taking this step, because it would have been too demanding in light of the resources available for this study.

The difference in the quality of the responses obtained (even among the positive or partially positive ones) implies that a more complex assessment of the data access practices is needed. For this reason, the first remark that can be formulated is that data access practices should be assessed both in terms of process and content. In general terms, the best practices experienced where those in which both the interactions with data controllers were or became smooth, and the data controller was able to provide clear answers and not only the ‘bulk’ data. In other words, all data access requests were not simple straightforward interaction with the data controllers (even those that failed), but a series of exchanges, often starting with the identification of the data controller itself, and finishing (in the most successful cases) with the ‘interpretation’ of the personal data and of the other information received.

Paying attention to both the process and the content permits to advance further remarks. First, the very possibility that data access request can be lodged is often not foreseen by data controllers in their everyday procedures of management. Only few data controllers seem to have offices specifically trained and responsible for handling smoothly this kind of requests.

54 We determine that it would have been reasonably to make a complaint to the DPA regarding the practices of data controllers of the following sites: (i) CCTV (Public – Public space, open street; (ii) CCTV (Private – Bank); (iii) CCTV (Private - Large Department Store); (iv) Private (Banking records); (v) Private (Advanced Passenger Information); (vi) Private: Google; (vii) Private: Microsoft; (viii) Private: Amazon. It should be noted that, by complaint, we understand the formal request to the DPA to intervene in a specific case. This assumption is not based on the legal analysis of each case, but on the apparent difference between what a data subject may expect by reading the legislation, and what these data controllers provided in terms of responses (in they provided a response at all).

IRISS WP5 – Norway Composite Reports

Final Draft

14/05/14
Even in fewer cases, the data controllers provide up-front information on the possibility of data access, and on how to submit a request. While it is difficult to state if the lack of organization and information are part of a strategy aiming at pre-empting requests, it should be noted that this creates a huge cost on the data subject, who is left proceeding by trial and error.

The non-availability of a recognized template does not facilitate the exercise of the access right. However, the experience with online forms made available by some data controllers underline that templates and forms may also hamper and limit the exercise of the right in the very moment in which the data subject submit a request. While they facilitate contacts with the data controllers, their design may impose limits on the kind of information requested. For example, if the online interfaces and the templates cannot be customized by the data subject, or if no alternative channels of communication exist, it may become very difficult to even request the same amount of information that the research team systematically asked for (e.g. third party data exchange).

Another remark linked to the process concerns the question of the language and of the clarity of the interactions. Responses to data access requests may easily contain a lot of data protection jargon, which is often difficult to understand for not trained people, and even for people that have been trained in a different language. From this perspective, the decision of several data controllers to switch to a foreign language may hamper the experience, or put a too high price on the side of the data subject, even when the data are finally disclosed. A possible solution could consist in ensuring that the interactions are carried on in the language in which the data subject is more comfortable with.

When it comes to attention to the content, this research highlights the need to pay attention to the quality of the information provided by data controllers. First of all, in few cases the data controllers seemed to have cut and pasted sections from their privacy policies, rather than addressing the questions of the data subject with specific information and the disclosure of data. Furthermore, in few cases the messages sent to the data subject were not clear, either because sentences and words were missing or incomplete, or because the internal messages between the staff was not removed. Second, the specific support on which the data disclosed will be stored and transmitted to the data subject was generally chosen by the data controller. Again: not all the supports and formats permit the same possibility of interaction with the received data. This should be made clear upfront by the data controller, and the data subject should be put in the position to decide the format and the means of communication. It should also be noted that the response to a data access request potentially multiplies both the personal data and the sites where these data are stored. A principle of data minimization may be considered, so to avoid all unnecessary redundancies and ensure a high level of data security.

In any case, access to the same service via traditional login seems to be an appropriate solution. Even if all the data were to be available there, little information about their use and the related metadata would be accessible. Indeed, the disclosure of an avalanche of personal data, even if considered a success, may result in little information, if the data subject has no tools to make sense of them and their function, or just properly check their accuracy.

The lack of attention to the quality of the content may explain the poor results in terms of information about third party data sharing and automatic decision making. This information is linked to the role of personal data within the workflow of the data controller(s). Often,
access to this information is the core of data access request, because it permits to cast a light on how data subject’s data are used and what foreseeable consequences can trigger.

Finally, a last remark concerns the poor quality of CCTV signage in all the cases examined. This made the exercise of the data access right extremely complicated, if not practically impossible. While this should be already considered a negative finding, it becomes particularly problematic in the cases where many people are exposed to camera, and have little possibility to avoid exposure. A more consistent implementation of the relevant Norwegian legislation should be considered, lacking it, data access remains a merely speculative exercise.
SIGNIFICANCE OF FINDINGS - NORWAY

Overall evaluation of the research experiences

The research team at PRIO carried three small-scale studies concerning data access (innsyn) rights and practices in Norway. The first study focused on the Norwegian legislation which provides the right of data subjects to access their personal data and receive further information about the data, such as the responsible data controller and the kind of processing at stake. The main purpose of the second study was to assess the level and quality of accessibility to data controller information, adopting a semi-ethnographic approach. The aim of the third was to evaluate the experience of requesting data access from the perspective of a data subject, and data controllers’ practices in responding (or not) to data access requests.

Together, these three studies offer a first overview of data access in Norway, from the double perspective of the legal and the ethnographic analysis. This overview has no claim to be fully exhaustive. Both the challenges encountered during the research exercises and the findings themselves invite others to carry on further research on a topic that is often overlooked in the scientific literatures and often absent from major political debates. Nevertheless, these three studies permit us to advance some insights on the current situation and to formulate some policy considerations which may be taken into account at national and European level.

Significant findings (including best and worst practices)

The analysis of the relevant national legislation providing for the right of data access highlighted three main findings.

1. ‘On the books’, Norwegian legislation provides for a rather comprehensive right of data access. The main provision is Section 18 of the Personal Data Act (PDA), which provides for both a sort of ‘general’ right of access to “any person” and an ‘individual’ right of access to information. Beyond Section 18 PDA, data access rights are also reinforced, inter alia, by Section 22 PDA concerning automated decision making, Section 27 PDA concerning data rectification, Section 28 on data minimization, and Sections 16 and 17 PDA imposing time-limits of the data controllers’ responses and establishing that no payment should be asked from the data subject.

2. There is little case law concerning data access at judicial level. The most relevant cases may be found at an administrative level, in the rare cases brought to, and decided by, the Privacy Appeals Board (Personvernmennsla, a Norwegian sui generis institution). This seems to indicate that data access is not a right and a practice that triggers litigation in Norway.

3. No publicly available codes of conduct have been devised so far. There is also no available common template to submit a data access request, with the notable exception of a template to access data from employers, designed and put at disposal

55 The members of the research team at PRIO are (in alphabetical order): Rocco Bellanova, Stine Bergersen, J. Peter Burgess, Maral Mirshahi, and Marit Moe-Pryce. The research team would like to thank all the Norwegian data protection experts that provided advice and feedback in the preliminary phases of the study.

56 The distinction between “generelt innsyn” (general access) and “individuelt innsyn” (individual access) is drawn from the website Personvern på nettet operated by the University of Oslo (cf. http://personvern.info/verktøy/krev-innsyn/). While the general right of access permits to anybody to obtain generic information about data processing and the data controller, the individual right of access allows the data subjects to acquire further information from the data controller.
The semi-ethnographic research concerning the availability and quality of data controllers’ information underlined the following trends:

1. The average approach of public agencies is one of denial, or at least lacking facilitation. Staff seemed to be uninformed about data protection regulation, and either hesitant or lacking appropriate information about the data controller.

2. The public agencies categorized under the domain of security imply a rather time consuming and bureaucratic procedure for identifying the specific information about the data controller. This is due to the fact that ‘the police’ are mentioned as the general data controller, in which no detailed information is given about the office or entity particular to each respective case.

3. The average approach of private agencies was, with the notable exceptions of CCTV and internet-based site, much more facilitating. The staff seemed more prepared to answer questions concerning data protection and could provide information about the data controller.

4. When it comes to CCTV sites, the claimed need to contact the relevant police office raises some concerns as to the facility to identify the responsible data controller. It should also be noted that CCTV signage – required by law – is extremely poor and very often lacking key information.

5. Online sites, such as social networks, email providers and search engines, have a somehow frustrating approach: while they all provide some sort of interaction with the data subject or concerned person (e.g. via online forms or trouble-shooters), they provide little satisfactory information in terms of contact details.

6. Establishing too high barriers to access one’s own personal data could have a negative effect on the capacity of everyday users to assess whether their sensitive data are collected in sites that are, apparently, not sensitive (shops, public spaces, etc.).

The study concerning the effective exercise of the data access right (from lodging the request to interactions with data controllers and possibly receiving a response) permitted us to advance the following insights:

1. In general, only few data controllers were able to fully and exhaustively address the data access requests (less than half). The difference in the quality of the responses received (including the negative, evasive or vague ones) invites us to assess the practices concerning data access not only in terms of effective data and information disclosed, but also in terms of process and content.

2. From the perspective of process, it is remarkable that it is often challenging to identify the office or department of the data controller that is responsible for handling data access request. Very few data controllers provide upfront information on how to lodge a data access request.

3. Data controllers that have staff who are data protection-aware tend to interact in a smoother way with the data subject, and provide more pertinent information. The ability to deal smoothly with the request is paramount, given that all data access
requests seem to imply several exchanges between the data controller and the data subject.

4. While the lack of a recognized template may not facilitate the exercise of the access right, the use, by data controllers, of their own templates and online forms may partially hamper it, too. In particular, online forms often discipline the type of request that the data subject may lodge, generally limiting, *ex ante*, the scope of the request.

5. From the perspective of content, the forms in which data and information are provided to the data subject deserve specific attention. First, the choice of the support on which data are disclosed has consequences on the effective ability of the data subject to make use and sense of the received data. The disclosure of data via email further multiplies the quantity of data concerning the data subject, and the sites where they are stored. Finally, the ‘bulk’ transmission of data may eventually preempt the ability of the data subject to understand and verify them, if the type of data (e.g. metadata) and their function is not duly explained by the data controller.

6. Language proved to be a main issue to be addressed. On the one side, it is extremely difficult for data subject who do not speak Norwegian to identify the relevant data controllers. On the other side, all multinational companies switched to English as soon as they responded to the requests, despite the fact that original requests had been drafted in Norwegian. While the shift towards English may ensure smoother interactions when the data subject is fluent in English, the technicality of the some responses and information may prove a barrier even to them.

7. The exercise of CCTV data access requests confirmed the poor quality of the signage, and the negative side effect it has on data access.

**Policy considerations at national and European level**

- Given that the main overall finding of the studies is the strong discrepancy between the law in the books and the effective practices concerning data access, Norwegian competent authorities should consider carrying out more extensive studies and assessments.

- The relevant authorities should also consider evaluating the impact and use of the data access template for data access requests to employers that has been put at disposal by the Datatilsynet. When deciding about the development of other templates, the competent authorities should keep the limits of the same, and eventually design one that can be easily modified by data subjects, and still easy to be handled by data controllers.

- CCTV signage should be radically improved, and brought in line with the requirements set in the legislation. The use of a common template may be a solution. Whenever the police is the relevant data controller, this should be duly stated in the signage, with precise information concerning the apposite department in charge of data access requests.

- Competent authorities should consider the best strategies to invite data controllers to set up specific offices or departments in charge of data protection related questions. Data controllers should be invited to provide more clear information about their responsibility and competences, as well as the best ways to be easily contacted.

- More attention should be paid to the question of language, especially given that many online services (social media, email providers, etc.) are provided by multinational...
companies that have no offices in Norway. Similarly, Norwegian data controllers should be invited to provide clear information in English on their website.

- A debate about the use of common templates and online forms should be welcomed at European level. The goal should be to assess their actual use, their potential, their limitations and the design of more customizable versions (data subject-friendly).

- Data controllers operating in diverse countries should be invited to address data access requests in the language of choice of the data subjects. When this is not possible, both the data controller and the DPA should extensively support data subjects, so as to ensure that their full rights of data access can be exercised (i.e. rectification, erasure, blockage).

- More attention should be paid to the way in which data are disclosed, and to the accompanying information about their function and role in the data processing workflow. Data subjects should be put in the situation in which they can make effective use and sense of the data received. A principle of data minimization should be followed at the moment of disclosure.
References

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

Datatilsynet, ‘Regulations on the processing of personal data’ (Personal Data Regulations). Available at: http://www.datatilsynet.no/Global/english/Personal_Data_Regulations_20100215.pdf

Datatilsynet, ‘Virksomheter med ombud’ http://www.datatilsynet.no/Personvernombud/Virksomheter-med-ombud/#Andre%20virksomheter


http://personvern.info

http://www.slettmeg.no/English

Human Etisk Forbund: KRL- seier for humanistene. URL: http://www.human.no/Livssynspolitikk/Religion-og-livssyn-i-skolen/?index=2


Microsoft, ‘Microsoft Support: Contact Us – Privacy Feedback’ https://support.microsoft.com/contactus/emailcontact.aspx?scid=sw;no;1310&ws=1prcbn

IRISS WP5 – Norway Composite Reports
Final Draft
14/05/14

Surveillance/monitoring HR-2013-00234-A (2012/1334)

Universitetet i Oslo: Personvern på nettet: http://personvern.info/verktøy/krev-innsyn/
List of Abbreviations

ANPR - Automatic Number plate Recognition
CCTV - Closed Circuit Television
DPA - Data Protection Authority
EU DPD - European Union Data Protection Directive
GPS - Global Positioning System
IRISS - Increasing Resilience in Surveillance Societies
KRL - Kristendom, religion og livssyn (en: Christianity, religion and philosophy of life)
NGO - Non-Governmental Organization
PDA - Personal Data Act
PDR - Personal Data Regulations