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

AUSTRIA COUNTRY REPORTS

INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN, AUSTRIA

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN AUSTRIA – JARO STERBIK-LAMINA

LOCATING THE DATA CONTROLLER IN AUSTRIA – STEFAN BIRNGRUBER & JARO STERBIK-LAMINA

SUBMITTING ACCESS REQUESTS IN AUSTRIA – JARO STERBIK-LAMINA

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN AUSTRIA

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

In Austrian law, all important data protection principles are written down in the Data Protection Act (current version: Datenschutzgesetz – DSG 2000)[1] since the first act on data protection was introduced in 1978. Alongside this, there are several other regulatory parts and pieces that fill in gaps, define exceptions or regulate certain issues in more detail. Moreover, there is some national implementation regulation in form of national decrees (for example the Datenverarbeitungsregister-Verordnung 2002 and 2012[2], the Datenschutzangemessenheits-Verordnung[3] or the Standard- und Musterverordnung 2004[4]) and Data Protection Acts in the nine different Länder[5] complementing the national Data Protection Act.

The constitutional right of data protection is derived from the European Convention on Human Rights[6] which has constitutional status in Austria[7] and emphasized by the fact that the first three paragraphs in the Data Protection Act 2000 form a constitutional provision. In these first three paragraphs the fundamental right to data protection is recorded (including the rights to data access, correction and deletion), as well as the legislative power and enforcement of this law and the territorial dimension of the jurisdiction.

---

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

[2] Austrian Chancellor (2012): Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2012 – DVRV 2012), Bgbl. II Nr. 257/2012; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007925 (last accessed 23 July 2013).

[3] Austrian Chancellor (1999): Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung DSAV), Bgbl. II Nr. 521/1999, as amended on June 12th, 2013, last Amendment Bgbl. II Nr. 150/2013; http://www.dsk.gv.at/DocView.axd?CobId=30701 (last accessed 23 July 2013).

[4] Austrian Chancellor (2004): Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004), Bgbl. II Nr. 312/2004, as amended on July 23rd, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495 (last accessed 23 July 2013).

[5] Austrian Data Protection Agency (2014): List of laws in the nine different Austrian Länder relevant for the data protection legislation in Austria; https://www.dsb.gv.at/site/6202/default.aspx (last accessed May 8th, 2014).

[6] The Council of Europe (1950): Convention for the Protection of Human Rights and Fundamental Freedoms, as amended on Protocol 14, in force by June 1st, 2010; http://www.echr.coe.int/Documents/Convention_ENG.pdf (last accessed 23 July 2013).

[7] The European Convention on Human Rights has been ratified in 1958 after Austria joined the Council of Europe and completely got constitutional status in 1964: The Austrian Parliament (1964): Bundesverfassungsgesetz vom 4. März 1964, mit dem Bestimmungen des Bundes-Verfassungsgesetzes in der Fassung von 1929 über Staatsverträge abgeändert und ergänzt werden, Bgbl. Nr. 59/1964, as amended on July 23rd, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000391 (last accessed 23 July 2013).

The current Austrian federal data protection law itself derives from the Data Protection Act of 1978[8] and was passed in 1999 (effective from 2000), implementing the provisions from the Directive 95/46/EC.[9] In general the Data Protection Act 2000 forbids the use of personal data, unless there is a lawful exception (and these exceptions are defined mostly in the data protection act itself and partly in other regulations).

The law has undergone several amendments since its inception, the most interesting of which came in 2009[10] and 2013.[11] The amendment of 2009 (in force as of 2010, therefore called "2010 amendment") is notable because until then, data collected by CCTV had to be handled like any other personal data. The recording as a form of processing (potentially sensitive) personal data had to be permitted a priori in an often lengthy process by the Data Protection Commission during which the data controller would be entered into the national register of data controllers. This led to a situation where around 95% of all CCTV systems were installed without this permission and we therefore effectively operating illegally. In 2010 there were about 1.200 registered CCTV-systems (only 18 of them operated by the police) and estimated 1.000.000 cameras.[12] In truth, since the Data Protection Commission in Austria faces significant budget constraints[13], they probably wouldn't have been able to deal with all the requests anyway. With the 2010 amendment, this situation was changed by inserting a section specifically about data processing and storing by CCTV systems.[14] Most CCTV systems can now be operated legally either without information to the DPA if it is not a camera (dummies); if the data are not stored, so called "Echtzeitüberwachung"/real time surveillance; if the recordings are stored on an analogue medium (video cassette) and are deleted within 72 hours; if the recordings are only for personal/familial activities and if they comply with the Standard SA032 "Videoüberwachung".[15] This is the case of cameras installed in banks, jewellers, goldsmiths, antique dealers, tobacconists, petrol stations, private

[8] Austrian Parliament (1978): Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG), Bgbl. 565/1978, http://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf (last accessed 23 July 2013).

[9] European Parliament and the Council of Europe (1995): Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last accessed 23 July 2013).

[10] Austrian Parliament (2009): Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010), Bgbl. I Nr. 133/2009, http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2009_I_133 (last accessed 23 July 2013).

[11] Austrian Parliament (2013): Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2013), Bgbl. I Nr.57/2013, http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2013_I_57 (last accessed 23 July 2013).

[12] Although one CCTV-system could have more than one camera, it is safe to assume that not all CCTV-cameras are part of a CCTV-system known to the DPA. Austrian Broadcasting Company Online Portal (2013): Private Videoüberwachung im Vormarsch; http://wien.orf.at/news/stories/2581260/ (last accessed 23 July 2013).

[13] The Austrian Data Protection Commission (2012): Datenschutzbericht 2010/2011, http://www.dsk.gv.at/DocView.axd?CobId=47839 (last accessed 23 July 2013), p. 24ff.

[14] Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended on July 19th, 2013; Unofficial English translation: http://www.dsk.gv.at/DocView.axd?CobId=41936 (last accessed 23 July 2013), section 9a, §§ 50a-e.

[15] Austrian Chancellor (2010): Verordnung des Bundeskanzlers, mit der die Standard- und Muster-Verordnung 2004 – StMV 2004 geändert wird (Novelle zur StMV 2004), Bgbl. II Nr. 152/2010, http://www.dsk.gv.at/DocView.axd?CobId=39692 (last accessed 23 July 2013).

covered areas, provided that they are operated only for certain reasons (e.g. prevent crime); are not allowed for controlling employees; have a max. 72 hours storage; only certain people are allowed to see the data (only in case of something happening); or as long as the DPA is informed about it in advance (obligational registering – "Meldepflicht" – in the "Datenverarbeitungsregister", see below for further details) and the recorded data is encrypted with a key only the DPA holds. Otherwise, still the DPA has to do a prior check. The 2013 amendment, effective from 2014, is also interesting. Since it deals with repairing an incompatibility with the Directive 95/46/EC it is described in Section 4 of this report.

Besides the rights and obligations the Data Protection Act also defines some principles to follow when processing data (in § 6) such as fair use, prohibition of function-creep, responsible use, proportionality and immediate deletion, as soon as the data isn't needed for the announced purpose anymore. Codes of conduct regarding data handling for the private sector have to be evaluated by the Federal Chancellor.

Some other laws with an implication on data protection for Austrians are: trade, commerce and industry regulation (Gewerbeordnung 1994)[16], especially for direct marketing (§ 151); the E-Government Law[17], the Code of Civil Law (Allgemeines Bürgerliches Gesetzbuch – ABGB[18]); the law for the register of persons living in Austria (Meldegesetz 1991)[19]; the Telecommunications Act (Telekommunikationsgesetz 2003)[20]; the Insurance Contracting Act (Versicherungsvertragsgesetz 1958)[21]; the E-Commerce Act (E-Commerce Gesetz von 2001[22]); the act on controlling shares/bonds (Wertpapieraufsichtsgesetz 2007)[23]; and last but not least the article 8 in the Austrian Federal Constitutional Law[24].

---

[16] Austrian Parliament (1994): Gewerbeordnung 1994 - GewO 1994, Bgbl. Nr. 194/1994, as amended on July 25th, 2013; https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10007517 (last accessed 25 July 25 2013).

[17] Austrian Parliament (2004): Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), Bgbl. I Nr. 10/2004, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230 (last accessed 26 July 2013).

[18] Austrian Emperor Franz I. (Emperor of the Holy Roman Empire Franz II.) (1811), Kaiserliches Patent: Allgemeines bürgerliches Gesetzbuch für die gesammten deutschen Erbländer der Oesterreichischen Monarchie, JGS Nr. 946/1811, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622 (last accessed 26 July 2013).

[19] Austrian Parliament (1992): Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 - MeldeG), Bgbl. Nr. 9/1992, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005799 (last accessed 26 July 2013).

[20] Austrian Parliament (2003): Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003), Bgbl. I Nr. 70/2003, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849 (last accessed 26 July 2013).

[21] Austrian Parliament (1958): Bundesgesetz vom 2. Dezember 1958 über den Versicherungsvertrag (Versicherungsvertragsgesetz - VersVG), Bgbl. 2/1959, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001979 (last accessed 26 July 2013).

[22] Austrian Parliament (2001): Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG), Bgbl. I Nr. 152/2001, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001703 (last accessed 26 July 2013).

Definitions in the Data Protection Act 2000 can be found in § 4[25], amongst others for the following terms:

- Data/personal data: "data" ("personal data") ["Daten" ("personenbezogene Daten")]: Information relating to data subjects (sub-para. 3) who are identified or identifiable. Data are "only indirectly personal" for a controller (sub-para. 4), a processor (sub-para. 5) or recipient of a transmission (sub-para. 12) when the Data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means.
- Sensitive data: "sensitive data" ("Data deserving special protection") ["sensible Daten" ("besonders schutzwürdige Daten")]. Data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life.
- Data subject: "data subject" ["Betroffener"]: any natural or legal person or group of natural persons not identical with the controller, whose data are processed (sub-para. 8);
- Controller: "controller" ["Auftraggeber"]: natural or legal person, group of persons or organ of a territorial corporate body [Gebietskörperschaft] or the offices of these organs, if they decide alone or jointly with others to use data (sub-para.8), without regard whether they use the data themselves (sub-para. 8) or have it done by a service provider (sub-para. 5). They are also deemed to be controllers when the service provider instructed to carry out an order (sub-para. 5) decides to use data for this purpose (sub-para. 8) except if this was expressly prohibited or if the contractor has to decide under his own responsibility, on the basis of rules of law or codes of conduct.
- Processor: "processor" ["Dienstleister"]: natural or legal person, group of persons or organ of a federal, state and local authority [Gebietskörperschaft] or the offices of these organs, if they use data only for a commissioned work (sub-para. 8).
- Filing system: "filing system" ["Datei"]: structured set of personal data which are accessible according to at least one specific criterion.
- Use of data: "use of data" ["Verwenden von Daten"]: all kinds of operations with Data, meaning both processing of data (sub-para. 9) and transmission of Data (sub-para. 12).
- Processing of data: "processing of data" ["Verarbeiten von Daten"]: the collection, recording, storing, sorting, comparing, modification, interlinkeage, reproduction, consultation, output, utilisation, committing (No. 11), blocking, erasure or destruction or any other kind of operation with data except the transmission of Data (sub-para. 12).

---

[23] Austrian Parliament (2007): Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007 – WAG 2007), Bgbl. I Nr. 60/2007, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005401 (last accessed 26 July 2013).

[24] Bundesrat (in terms of the Austrian Constitutional Law from 1920) (1930): Bundes-Verfassungsgesetz (B-VG), Bgbl. Nr. 1/1930, as amended on July 23rd, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000138 (last accessed 23 July 2013).

[25] Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended on July 19th, 2013.

- Consent: "consent" ["Zustimmung"]: the valid declaration of intention of the data subject, given without constraint, that he agrees to the use of data relating to him in a given case, after having been informed about the prevalent circumstances.

Organisational structures according to the Data Protection Act 2000 are:

- Data Protection Agency (Datenschutzbehörde, before: Datenschutzkommission);
- Data Protection Council (Datenschutzrat);
- Data Processing Register (Datenverarbeitungsregister).

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

The right of access to data is regulated in the Data Protection Act 2000 (DSG 2000) in § 26, according to which:

> "§ 26. (1) A controller [Auftraggeber] shall provide any person or group of persons with information about the data being processed about the person or the group of persons who so request in writing and prove his/her identity in an appropriate manner. Subject to the agreement of the controller, the request for information can be made orally. The information shall contain the processed data, the information about their origin, the recipients or categories of recipients [Empfängerkreise] of transmissions [Übermittlungen], the purpose of the use of data [Datenverwendung] as well as its legal basis in intelligible form. Upon request of a data subject, the names and addresses of processors [Dienstleister] shall be disclosed in case they are charged with processing data relating to him. If no data of the person requesting information exist, it is sufficient to disclose this fact (negative information). With the consent of the person requesting information, the information may be provided orally alongside with the possibility to inspect and make duplicates or photocopies instead of being provided in writing".

According to Art. 26 (2), data controllers have the right to refuse information for the following reasons:

> (2) The information shall not be given insofar as this is essential for the protection of the person requesting information for special reasons or insofar as overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an obstacle to furnishing the information. Overriding public interests can arise out of the necessity:
>
> 1. to protect of the constitutional institutions of the Republic of Austria or
> 2. to safeguard of the operational readiness of the federal army or
> 3. to safeguard the interests of comprehensive national defence or
> 4. to protect important foreign policy, economic or financial interests of the Republic of Austria or the European Union or
> 5. to prevent and prosecute crimes.

In these circumstances the refusal is subject to control by the Data Protection Commission [Datenschutzkommission].

The data subject should cooperate with the information procedure upon enquiry, to a reasonable extent to prevent an unwarranted and disproportionate effort on the part of the controller (Art. 26 (3)). So, for example, if the data subject knows his customer identification number, it could be given to the controller; or if the controller operates different databases and the data subject knows in which of them there could be some data stored about him, this information could also be useful for the controller. Of course this doesn't mean the data controller is allowed to send just the information already known to the data subject, but giving this kind of information could make it easier for the data controller to process an access request. When it comes to CCTV the data subject could specify very precisely date and time, the colour of the clothing worn and so on. Art. 26 (4) establishes that within eight weeks of the receipt of the request, information shall be provided or a reason given in writing why the information is not available or not completely disclosed. The information may be refused if the person requesting information has failed to cooperate with the information procedure mentioned above or has not paid the cost of making a request (one per year is free but if a subject access request is submitted a second time, the costs for answering the access request have to be reimbursed by the requester).

In case the data subject wants to have access to his personal data that are in the domain of public authorities and the data controller refuses to disclose it, a specific procedure has to be followed. In cases where no data on the requester is held by the data controller, data controllers should give an indication that no data are being used which are subject to the right to information. Elsewhere, in cases where the data subject seeks access to data which are stored for one of the five exemptions, the reply he would obtain will be the same as if the data controller would not have stored any data about him (i.e.: the requester will be advised that no data is processed over which he has the right of access). The legality of such course of action is subject to review by the Data Protection Commission [Datenschutzkommission].

According to Art. 26 (6), information shall be given free of charge if it concerns the current data files [Datenbestand] in a database and if the person requesting information has not yet made a request for information to the same controller regarding the same application purpose [Aufgabengebiet] in the current year. This implies that the data subject does not have to pay for having access to data as long as the data controller does not have to restore data which are located in databases from some point in the past and he submits an access request for the first time. In all other cases, a flat rate compensation of 18,89 Euro may be charged. Moreover, deviations are permitted to cover incurred higher expenses. A compensation already paid shall be refunded, irrespective of any claims for damages, if data have been used illegally or if the information has otherwise led to a correction.

As of the moment the controller has knowledge of a request for information, the controller shall not erase the data relating to the person requesting information until four months have passed or in case a complaint is lodged with the Data Protection Commission until the final conclusion of the proceedings (Art. 26 (7)). Specific provisions also apply in the case of access to criminal records files, according to the Criminal Records Act 1968 [Strafregistergesetz 1968].

In cases where legal provisions lead to a qualification as controller, though the data are processed for a third party in order to carry out a job (§ 4 para 1 sub-para. 4 last sentence), the person requesting information may also first direct the request for information to the entity

that ordered the job. This provision entails that if an entity is processing data as a third party on behalf of the data controller, this entity would be qualified as data processor. However, if for legal reasons this entity is categorised as a data controller too, then the data subject can decide who to contact first for an access request. This entity has to provide the person requesting information, to the extent that one does not know already, with the name and address of the effective controller within two weeks, free of costs, so that the person requesting information may assert his right of information according to para 1 against him. In case a request for information is directed to a service provider and it is obvious that the person requesting information mistakes him for the controller of the data application operated by him, the service provider shall forward the request for information immediately to the controller and to inform the person requesting information that no data are processed by him as controller. Within eight weeks after the request for information has been received by the service provider the controller has to grant information to the person requesting information or argue in writing, for which reason it is not granted or not completely.

The right of access in case of CCTV recordings however, is regulated in § 50e, which states that:

> "§ 50e. (1) "the person requesting information, after having indicated the timeframe during which he/she might have been captured by the surveillance and after having indicated the location as precisely as possible and after having proven his/her identity in adequate manner, is to be granted information on the data processed on his/her person, by sending a copy on the data processed in a common technical format.[26] Alternately, the person requesting information may request inspection on a reading device of the controller and is also entitled to be handed over a copy of the requested data in such case. The other elements of the information (available data on the origin, recipient or circles of recipients of data transmitted, purpose, legal basis and eventually service providers) are to be given in writing also in case of surveillance, unless the person requesting information agrees to receive oral information.
>
> In case an information cannot be disclosed because of an overriding legitimate interests of third parties or of the controller, the person requesting information is entitled to a written description of his/her behaviour processed by the CCTV device or to have access to a footage, in which other persons have been made unrecognizable. In cases of real time surveillance, no access right is granted".

CCTV and information by signs

Art. § 50d sets legal provisions as to how to mark and identify CCTV systems. "The controller of a video surveillance shall put up appropriate signs. The sign shall specify who the controller is, unless already known to the data subjects based on the circumstances of the case. The information sign has to be fixed in places in a way, that any potential data subject approaching the surveyed object or person has the possibility to bypass the video surveillance" (Art. 50d (1)). In addition, video surveillance within the frame of implementation of official executive tasks, although exempted from the obligation of

[26] The "common technical format" could for example consist in a file in MPEG or Quicktime format stored on a DVD.

notification, needs not be marked with signs (Art. 50d (2)). Official executive tasks, listed in § 17 (3), are: protecting the constitutional institutions of Austria; safeguarding the operational readiness of the federal army; safeguarding the interests of comprehensive national defence; protecting important foreign policy, economic or financial interests of the Republic of Austria or the European Union; preventing and prosecuting of crimes

Decisions of the Austrian Data Protection Commission[27]

An interesting decision from the last DPA report concerns the use of CCTV on public transport in Vienna. This finding was not new as such but rather reinforced a previous finding of 2008. In this case, the right of access to CCTV footage captured by the CCTV system of the public transportation company (Wiener Linien) in Vienna was considered. Specifically, the case concerned the identification of third parties on the footage as part of analysing the footage when responding to individuals' subject access requests – i.e.: would a third party's privacy be compromised by a detailed review of the footage? After two test phases, Wiener Linien successfully obtained a permanent permit to install CCTV cameras in stations, trains, trams and busses to record the images and store them for 120 hours to ensure the security and safety of the staff and the passengers and to reduce vandalism. The company claimed that the data was not analysed/looked at and deleted after 48 hours except when an incident had occurred and the police needed the images. The DPA decided[28] that the process of analysing the material and potentially identifying individuals (which have been recorded but not identified until then) in order to find footage requested via an access request, was an intrusive process since the privacy of third parties would be compromised. As a result, the DPA applied an exemption to the company in this regard and Wiener Linien are thus not required to fulfil any obligation to answer subject access requests when it comes to CCTV footage. This was a controversial decision, since the DPA argued that while searching for the specific data subject, other passengers who also have not been identified until this moment might be identified by chance when looking at the data. Opponents would simply answer that this can happen everywhere in public space and is not very likely.

Following the implementation of the 2010 amendment to the Data Protection Act with new provisions regarding video surveillance, another request/complaint was made with a view to accessing footage captured by the Wiener Linien via an access request. Once again, the DPA reinforced its previous decision and upheld the company's blanket exemption to having to respond to access requests for CCTV footage.

In 2013 this decision was annulled by the Austrian Higher Administrative Court after the European Court of Justice ruled against the Republic of Austria, finding that the independence according to the data protection directive of the Austrian Data Protection Commission was not safeguarded. The Higher Administrative Court decided that the DPA was not competent to decide in this matter as a result of this lack of independence. This was also done with a lot of other previous findings of the DPA. After Austria repaired its data protection law to give the DPA the necessary organisational independence, the DPA reissued some of its opinions when complaints had brought up the matter again. Although this has not happened at the time of writing, it can be assumed that the DPA will also reissue its opinion

[27] The sum of all dictates of justice (Rechtssätze) and decisions of the Austrian Data Protection Commission can be found here: http://www.ris.bka.gv.at/Dsk/.
[28] Data Protection Commission (2008): Bescheid (verdict), Geschäftszahl K121.385/0007-DSK/2008.

on answering subject access requests in regard to non-analysed CCTV material and indeed this has been informally discussed by the DPA.

Another decision of the DPA dealt with the question as to whether information about data stored only for documentary purposes also has to be part of an answer following a subject access request. In this case the police undertook preliminary proceedings against a citizen which were later closed without charging him. The information about the proceedings was stored in an electronic file within one of the police information systems. Since the file was archived and police units were not able to access the information, the internal operators were of the opinion that this data does not have to be part of an answer to a subject access request. In contrary the DPA decided, that all data, in all systems, even if it is only kept for documentary purposes has to be included. In this specific case the police had to inform the citizen not only about the kind of data that is stored about him, but also about the content – which is regulated in a different act, so § 26 DSG 2000 was not applicable.

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

In Austria, both living natural persons (the law does not apply to deceased persons)[29] and legal persons[30] can be data subjects and therefore in principle exercise their data subjects' rights. As a result, this can cause difficulties, as Korff (2002) explains:

> "More problematic is the fact that the laws in Austria, Italy and Luxembourg extend the concept of data subject to **legal persons**. This means that, in these countries, the restrictions on the collecting, storing, disclosing etc. of data on natural persons (in principle) also apply to legal persons, and that legal persons can (again, in principle) exercise the rights of data subjects. Here, the definitional differences lead to clear **divergencies** in the application of the law…"[31]

Besides this, the Austrian law applies to any processing of personal data, although the right of access to data only applies to data which is automatically processed or held in "structured" manual files.[32] Further exceptions are regulated in § 26 (2) DSG 2000:

Exceptions to the right to access are described in Section 2 of this document and in general are granted if the requesting person has to be protected or if there are legitimate interests of others. If these legitimate interests are public interests, like "protecting the constitutional

[29] All fundamental rights cease to exist with the death of a person.
[30] A legal person is a consortium of persons or a collection of assets which is capable of holding rights because of public (sovereign?) approval, and which – in contradiction to non-incorporated firms (business partnerships?) – is financially independent, viz. with only limited liability.
[31] Korff, Douwe (2002): EC Study on Implementation of Data Protection Directive 95/46/EC – Report on the Findings of the Study, http://ssrn.com/abstract=1287667, p. 20.
[32] Korff, Douwe (2002): EC Study on Implementation of Data Protection Directive 95/46/EC – Report on the Findings of the Study, http://ssrn.com/abstract=1287667, p. 38; "structured" refers to the definitions in DSG 2000 § 4 where "filing system" ("Datei") is defined as a *"structured set of personal data which are accessible according to at least one specific criterion"*; according to a ruling by the Data Protection Commission this does for example not include data stored during corresponding with a data subject by written letters.

institutions", the organisation responsible for this has the right to refuse by telling requesters that "no data are being used which are subject to the right to information".[33]

Compatibility of national legislation with Directive 95/46/EC

The most prominent case of incompatibility concerned the problem the Austrian Data Protection Commission's lack of autonomy/independence. This was in the case C-614/10[34] and was decided by the European Court of Justice in favour of the EC's point of view and repaired by the Austrian Parliament in the 2013 amendment to the Data Protection Act 2000.

Prior to this amendment, the DPA was established by the Data Protection Act 2000 as an office within the organisation of the Federal Chancellery of the Republic of Austria (as it was before implementing the Directive 95/46/EC by the Data Protection Act (from 1978)). In addition, their members were functionally, as members of the DPA, not bound to directives, but the Data Protection Act 2000 regulated that the head of the DPA must always be a federal employee of the Chancellery. Therefore he/she would have to obey orders given to him/her in the context of the supervision. The EC stated in a letter of formal notice that this combination was not sufficient when it came to the DPA's independence as defined by the Directive 95/46/EC. After two reminders, the EC sued the Republic of Austria. In response, the Republic insisted that the DPA was independent because it was established as a collegiate authority with judicial functions ("Kollegialbehörde mit richterlichem Einschlag") within the meaning of the Austrian Federal Constitutional Law (Bundes-Verfassungsgesetz – B-VG)[35] which would guarantee independence comparable to that of an independent court of justice.
In the end, the European Court of Justice ruled:

> "that, by failing to take all of the measures necessary to ensure that the legislation in force in Austria meets the requirement of independence with regard to the Datenschutzkommission (Data Protection Commission), more specifically by laying down a regulatory framework under which the managing member of the Datenschutzkommission is a federal official subject to supervision, the office of the Datenschutzkommission is integrated with the departments of the Federal Chancellery, and the Federal Chancellor has an unconditional right to information covering all aspects of the work of the Datenschutzkommission, the Republic of Austria has failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data …"[36]

[33] Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended on July 19th, 2013; Unofficial English translation: http://www.dsk.gv.at/DocView.axd?CobId=41936 (last accessed: July 23rd, 2013), § 26 (2).
[34] Grand Chamber of the European Court of Justice (2012): Judgement of the Court in Case C-614/10; http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=359958 (last accessed 24 July 2013).
[35] Bundesrat (in terms of the Austrian Constitutional Law from 1920) (1930): Bundes-Verfassungsgesetz (B-VG), Bgbl. Nr. 1/1930, as amended on July 23rd, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000138 (last accessed 23 July 2013).
[36] Grand Chamber of the European Court of Justice (2012): Judgement of the Court in Case C-614/10; http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=359958 (last accessed 24 July 2013).

As a result, Austria repaired the law with the 2013 amendment. In the course of this amendment, the Data Protection Commission (Datenschutzkommission) was renamed, and is now the Austrian Data Protection Agency (Datenschutzbehörde).

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

As described above, whilst the use of CCTV is governed by explicit rules in the law, some of these rules are still not followed by many of the operators of such systems. For example, some operators are not even registered with the DPA where it would be obligatory. Moreover, the regulation in § 50d regarding the use of signs is clearly not followed by most of the operators. This makes it hard for data subjects to exercise their rights of access since it would be sufficient to name the operator. Contact details have to be researched by the data subject, ideally they can be looked up in the "Datenverarbeitungsregister", where all data controllers are registered. But since the enforcement of the 2010 amendment made an exception for many of the privately operated surveillance systems, only some need to be registered. In addition, employees of CCTV-operators are often unaware of the right of access in the first place. This situation is more or less accepted by the public, since most citizens aren't aware of their rights, too. So the provisions of the 2010 amendments have not led to a better situation for data subjects regarding video surveillance, since there are many exceptions to the obligation to register. If a citizen cannot find a data controller in the register, this may not necessarily mean that the operator has done something wrong; instead, it is possible that the CCTV system in question falls under one of the exception categories. Nevertheless the number of complaints appealed to the DPA is increasing.[37]

An interesting detail when it comes to restricting the ways in which CCTV data can be managed and processed can be located in § 50a (7) which states:

> "Data collected of data subjects concerned by video surveillance may not be analyzed by comparison with other picture data and not be searched using sensitive data as selection criteria."

So, for example, CCTV operators not allowed to match the recordings with an image database using face recognition technology, if the CCTV system falls under this section of the Data Protection Act

With regards to credit scoring, in Austria there are certain companies servicing other companies with information about credit scores of consumers – besides the sector- or business-internal lists and data. The most prominent is Kreditschutzverband 1870 – KSV. Although people in general do not know much, customer profiling and credit scoring, they know that the information such companies hold influence the conditions they have to face at their bank. So such companies are used to receiving subject access requests and thus have forms[38] on their websites and tend to handle requests in a speedy, pragmatic way.

[37] Data in this respect can be found in the Annual Report of the Austrian Data Protection Commission. The most recent is as follows: The Austrian Data Protection Commission (2012): Datenschutzbericht 2010/2011, http://www.dsk.gv.at/DocView.axd?CobId=47839 (last accessed 23 July 2013).

[38] KSV, Selbstauskunft bestellen (order a subject access request), http://www.ksv.at/KSV/1870/de/4privatpersonen/1selbstauskunft/index.html (last accessed 24 July 2013).

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

The Austrian Data Protection Commission undertakes very few pro-active compliance screenings ("Amtswegige Prüfverfahren nach § 30 Abs. 2 DSG 2000"), although it has the right to review every data processing in cases of reasonable suspicion. This is due to the constraints in HR resources, which are mentioned repeatedly by the Data Protection Commission itself in its biannual report[39] (in comparison with other European DPAs the Austrian Data Protection Commission can only employ less than 50% of the average number of employees and has no single employee with a technical background). However, anyone who thinks his or her rights have been violated in context of the data protection legislation can either file a formal complaint to the DPA or appeal to the DPA in an informal way ("Ombudsmann-Verfahren"). The first will lead to a process under administrative law and end with a decision of the DPA which could, if necessary, be enforced by a court of justice. The latter will start a process where the DPA is acting as mediator. This will lead to a statement by the DPA, but the data subject has no means to enforce these findings. Nevertheless, often the intervention by the DPA leads to a satisfactory result for the appellant. People are only entitled to start one of these processes if they are affected by the potentially unlawful data processing.

Besides this, the commission operates the "Stammzahlenregister" and the "Datenverarbeitungsregister". The first was implemented by the E-Government Act[40] and stores a secret number for each natural person in Austria derived from the number in the Central Population Register ("Zentrales Melderegister", ZMR-Zahl). From this secret number ("Stammzahl") which in addition could be stored on the eID-card ("Bürgerkarte") another number is generated, in a cryptographic one-way-process, too, for each administrative area citizens' data are processed ("bereichsspezifisches Personenkennzeichen") so different authorities use different numbers for the same person to protect citizens' privacy by limiting the amount of information which is stored about a person in one of the administrative areas and the possibility of automatically combining these informations.

The second register, the "Datenverarbeitungsregister" was introduced by § 16 of the Data Protection Act 2000. It contains a list of all data controllers with a data application that had to be reported and/or approved to/by the DPA in order for data controllers to be compliant with the Data Protection Act. Every data controller in this register has a seven digit number which has to be used when communicating with data subjects, so citizens are able to see where their address on a certain letter is processed. This is intended to add to the accountability and transparency of data controllers.

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

[39] The Austrian Data Protection Commission (2012): Datenschutzbericht 2010/2011, http://www.dsk.gv.at/DocView.axd?CobId=47839 (last accessed 23 July 2013), p. 21.

[40] Austrian Parliament (2004): Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), Bgbl. I Nr. 10/2004, as amended on July 24th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230 (last accessed 24 July 2013), § 6 and § 7.

Generally speaking the Austrian DPA is not involved in the process of exercising citizens' rights unless the citizen has the feeling that a data controller is not acting lawfully in this respect. Then there are the two options to involve the DPA, as described above.

The website of the DPA is not very helpful when it comes to exercising rights if one is not at least somehow familiar with the topic – although there is one page with an explanation about subject access requests for data subjects[41] citing all the paragraphs from the Data Protection Act 2000, including a link to a very brief template for a subject access request; and one for data controllers explaining how to answer a subject access request.[42]

As a result of the DPA's inability to fully help citizens with regards to privacy-related matter, a number of NGOs fulfil this function, such as ARGE Daten.[43] Among other activities, these bodies help citizens to exercise their rights by providing more detailed templates, explaining what their rights are and what specifically companies are allowed to do. They also monitor suspicious behaviour by companies, offering training for the industry and operate as a certificate authority.

[41] The Austrian Data Protection Commission (2009-2010): Das Recht auf Auskunft, http://www.dsk.gv.at/site/7434/default.aspx (last accessed 24 July 2013).
[42] The Austrian Data Protection Commission (2009-2010): Wie gebe ich Auskunft?, http://www.dsk.gv.at/site/7435/default.aspx (last accessed 24 July 2013).
[43] Arge Daten (2000-2013), Website: http://www.argedaten.at (last accessed 24 July 2013).

LOCATING THE DATA CONTROLLER IN AUSTRIA

Introduction

This country report profile summary reflects the findings and the experiences that were gathered to find data controller contact details while researching 32 Austria-based sites. The chosen examples do not claim to reflect the practices of all data controllers in Austria but represent the individual researcher's experiences. Nonetheless, we describe some examples of good and bad practices dealing with the Data Privacy Act.

Methodological thoughts

The following nine domains were analysed in course of this study: health, work, communications, civic engagement, consumerism, education, finances, leisure and transport. For each domain we studied several homepages of Austrian institutions.

Note that three work areas were not being considered in our study because they do not exist in Austria. These sites are "ANPR" (Automatic Number Plate Recognition, there are only pilot tests in Austria to explore the usefulness of such a measure in detecting stolen vehicles before passing the border), the "entry/exit system at your place of work" and the "nationally-held patient health records". The last one is called ELGA (Elektronische Gesundheitsakte – electronic health record) but it is still in research and development phase.

Furthermore, due to school holidays it was initially not possible to get information about "locally-held primary school records" and "locally-held secondary school records". We tried to contact these institutions directly by telephone, but no responsible person for these questions was available in July. In September and October we made a second and successful attempt to collect relevant information.

Our sampling strategy was the following: for the public authorities and governmental organisations (e.g. boarder control, passport service and Interpol) we used the official online homepages. For examining CCTV signage we visited places and shops that are located geographically closest to our place of work (i.e., Karlsplatz, Vienna). In order to analyse the handling of school records we directed our enquiries to the schools we attended in the past. For specific sites (e.g., online games, email data) we tried to examine national or local companies. In some cases we were unsuccessful, therefore had to contact international companies.

The most successful method was via websites. In most cases, links to online privacy policies were located at the bottom of web pages. There, we often found information about the responsible authority or what type of data was collected and used.

In contrast, we were unsuccessful when speaking to people in person. We were confronted with a general nescience and non-awareness about data protection and the right of access of personal data. Often, we were only referred to the company's homepage to make an online enquiry, which seems to be the standard response to customers when the employee's organisational knowledge is not sufficient to answer the customer's request. Unfortunately, when it comes to data protection there is a general lack of knowledge about its mere existence, not to mention its implementation within the organisation. This often creates an unpleasant situation for the employee to whom an enquiry is made and this employee will try to end it by being unfriendly, sometimes rude; or by referring the "importunate" customer to

the contact form on the website. The failure to educate employees about the topic might either be an act of complete ignorance towards the legislation, or at least an unwitting strategy of denial.

Overall impressions

Data controller contact details successfully identified in first round of visits	22 of 32 cases (69%)
Data controller contact details unable to identify in first round of visits	10 of 32 cases (31%)
Total number of data controller contact details successfully identified after second round of visits	24 of 32 cases (75%)
Total number of data controller contact details unable to identify after second round of visits	8 of 32 cases (25%)
Contact details identified via online privacy policy	18 of 23 (successful) cases
Contact details identified after speaking to member of staff on phone/via email	5 of 23 (successful) cases
Contact details identified after speaking to member of staff in person	1 of 23 (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	2 – Adequate

Average rating given to quality of information given by staff on the telephone	3 – Good
Average rating given to quality of information given by staff in person	1 – Poor

After the first and second round of visits we had 24 successful sites from 32 attempts. In some of these cases it was easy to find data controllers' contact details, like in the case of credit reference checks/rating. A high quality of data controller information was given in the sites "membership to leisure time/sport clubs", the "loyalty card scheme for a food and drinks retailer"[44] and at Europol. At the sport clubs' online privacy policy, a detailed list of stakeholders and the collected data can be found, including contact details for the responsible persons. Starbucks explicitly names the Data Protection Act and explains what data are processed and the customer's respective rights. Europol provides a two-page PDF-file[45] which can be found on the DPA's website that contains a lot of information, like what they do, general rights of citizens and the right of access to personal data is explicitly mentioned.

In the case of insurance records it took two e-mail requests to receive a satisfactory answer. There, we first had to reference the data privacy act. The customer service of the metro company refused the right of access to personal data on the basis of a decision of the Austrian Data Protection Commission (for a detailed case analysis, see the report for 5.1). We were surprised by the inefficiency of personal contacts in this round of research. We never got satisfactory information when enquiring in person and the responsible authorities told us to make an online query.

In summary, after a first and a second attempt we were only successful in 24 of 32 samplings. Therefore, we were unable to identify data controller in more than a quarter of all cases.

Online content

Of the 23 successful samplings, data controller details were found with the help of websites in 17 cases. The homepages had privacy policies in different degrees in depth of information. The visibility of online privacy policies reached from poor to good, while most were classified as reasonable. Most policies were found under the category "legal notice" (Imprint/Impressum). These links were located almost always at the bottom of the web pages in a small font. This is also the place where one expects them to be located. It is worth mentioning that often one click is enough to get to the privacy policies, rarely two or more clicks. Furthermore, no great difference between the public and the private sector was observable regarding quality of the privacy information. One observed drawback was the fact that only two websites provided a template for requests: one was the "Kreditschutzverband 1870" (credit scoring information broker) with a form specifically for subject access requests;

[44] http://www.starbucks.at/about-us/company-information/online-policies/privacy-statement
[45] Merkblatt zu den Rechten der Betroffenen bezüglich Europol (Information sheet on concerned persons' rights regarding Europol): http://www.dsk.gv.at/DocView.axd?CobId=30587

the other one was "Zielpunkt" (supermarket chain) with a form for all kinds of service requests. In all other cases the interested person had to write an e-mail to get information.

In summary, the only common feature of the 17 websites was providing some form of privacy policy but more often focused on data collected from visitors of the website and not concerning all data handled by the respective company. Nevertheless the data controller's contact details could be found.

In the following section, some strategies dealing with data privacy act and the right of access to personal data are presented.

Public

Strategies of facilitation

Concerning government/public agencies the enquiry for Europol showed the best practice dealing with data privacy. This can be called a strategy of facilitation. The national authority responsible for Europol enquiries in Austria is the Ministry of the Interior. Together with the DPA they provide a two-page PDF-file which can be found on the DPA's website that contains a lot of information. It explains what Europol is, what they do, general rights of citizens and the right of access to personal data is *explicitly* mentioned. They also note that within three months any request has to be completed (according to the Europol Convention). For the right of correction and deletion and for complaints, some contact data were listed: a postal address, phone and fax numbers, and an e-mail address. Only a template is missing but based on the other contact possibilities this is negligible. It would be even better practice to see this information on the website of Europol or the Austrian Ministry of the Interior also, but once the information is found, it delivers great benefit to the citizens and can be an example of transparency and accountability.

Furthermore, the Ministry of the Interior has a dedicated service for citizens (Bürgerservice) and an information service for general questions. These two services are not explicitly responsible for data protection issues but can probably refer to other institutions.

Strategies of (Unwitting) Denial

It does not seem that government/public agencies pursue deliberately a strategy of denial. However, it also happened occasionally that the enquiry office only responded to general questions and that they were not adequately qualified for answering questions about specific data protection issues.

One example is the "driving licence record", held by an Austrian public sector agency. On the homepage of this agency, one can find contact data for general enquiries but not for data protection details.

The same applies to site "passport services": here one is referred to a district office that only provides contact data for general information.

Regarding the domestic police records, it was easy to get information that is stored about yourself in the so called "Strafregister" (criminal records). There exists a standard procedure known by probably all citizens that allows you to obtain your criminal records at the local police station. This is well known perhaps because in the past decades, potential employers

often asked for a criminal records summary, especially when assigning new employees to jobs dealing with sensitive information.

But there may be more information, especially when it comes to surveillance by the "BVT – Bundesamt für Verfassungsschutz und Terrorismusbekämpfung" (Federal Office for the Protection of the Constitution and for Fighting Terrorism, formerly known as "Staatspolizei" (a special section of the federal police), the Austrian domestic intelligence agency of the Ministry of the Interior) or the ".BK – Bundeskriminalamt" (Federal Criminal Police Office).With respect to this we found a little bit of information on how to exercise citizens' rights on the website of the Ministry of the Interior. It was not as easy to understand but gave some hints on the process of sending a subject access request, covering the different police databases. The problem here is that according to the DP law, a citizen has to "help" in a reasonable extent in finding his/her data, which is interpreted by the ministry as telling them in what databases to search. One may argue that this is an easy task when remembering your last traffic ticket but almost impossible when someone has been watched by the BVT, since you probably wouldn't have noticed that you have been under surveillance in the first place, and even if you knew, how can an ordinary citizen tell the police where *they* have stored his/her data?

In addition, the subject access requests to certain police information systems are regulated in sector specific laws like the "Sicherheitspolizeigesetz" (Law on Public Security). These laws sometimes constrain the rights given in the Data Protection Law by, for example, charging fees for looking up the citizen's data (which is in general free once a year).

In summary, it does not seem that there is a strategy of active denial; maybe it is more the wish to discourage interested citizens and thereby reduce the possible amount of work for the authority.

Private

Strategies of Facilitation

Concerning private agencies, we found two sites during the research phase where it can be said that strategies of facilitation were used. The first one is an internet service provider. The online content of the homepage was very detailed. They mention that the contact person has the legal right to know which information is collected, shared with thirds and they even provide a direct link to an e-mail address. Furthermore, they offer a postal address and a fax number.

The second example of good practice is our chosen example for "email data". This site demonstrated some very good practice insofar as their online privacy statement included a lot of information about what type of data is collected and what it is used for. The webpage also had a clearly defined section entitled "right of access of personal data" which included a link for e-mail enquiries. Especially compared to other, big/multinational email providers like Google or Microsoft/Hotmail with their quite ambiguous privacy policies this can be seen as a near-perfect example of transparency.

Strategies of Denial

We also encountered several examples of poor/bad practice, particularly in cases involving large, multi-national online corporations. As we researched the content of the Facebook

homepage we found a lot of information about data privacy. This included explanations of what data is collected, what it is used for and with whom it is shared. Concerning the right of access to personal data, Facebook offers two options: firstly, they provide a postal address in Ireland and secondly, they have an online contact form. However, it is unclear whether one actually gets in contact with the data controller or data protection section. So there is no clear information for citizens which correlates with Facebook's somewhat juxtaposed attitude towards privacy: on one hand they have to give their users the feeling of secure communications, of a somehow "private" setting, while on the other hand they are not willing to take actions in this respect, because they also want their users to reveal as much information as possible since this is the currency Facebook is trading in for real money. This shifting of responsibilities, the idea that users are responsible for their privacy while they are not provided with the necessary settings, while concurrently trying not to give any privacy to them, can be seen as a very bad practice in helping exercising one's rights.

Another example is the site "membership to a national children's charity organisation". Searching on their webpage we could not find any information about data protection or what types of data are collected and used. They only offered a general phone number if one wishes to contact them.

CCTV and signage

The following five CCTV sites were analysed:

- a transport setting (subway)
- a public space (Karlsplatz)
- a large supermarket
- a small store, and
- a bank

CCTV signage was present at four sites (bank, public space, subway, large supermarket). One site (small jewelry shop) had no sign. The visibility of the signs was rated from poor to reasonable because they were rather small in size. In large sites, like the public space or the subway, more than one sign was visible. In all cases, it took less than five minutes to find the signage, except for the public space where we spent approximately 15 minutes to find some signs. At the supermarket we found the signs when leaving the shop because the only signage was at the sliding entrance doors.

Each sign has to fulfill two basic requirements according to Austrian law: first it should inform people about the presence of CCTV cameras and second the initiator should be named if it's not completely obvious who is operating the CCTV equipment[46].

Remarkable was the fact that in our sample the signs contained hardly any information about the reason for CCTV or contact details of the data controller. Furthermore the designs of the signs are completely different. They do not have a template or a uniform format. Therefore,

[46] § 50d Data Protection Law 2000: *"The controller of a video surveillance shall put up appropriate signs. The sign shall specify who the controller is, unless already known to the data subjects based on the circumstances of the case. The information sign has to be fixed in places in a way, that any potential data subject approaching the surveyed object or person has the possibility to bypass the video surveillance."*

even in cases where they are available, it is difficult to quickly perceive data controller details.

In order to give a deeper insight into the current situation, we include some pictures of CCTV signs in the remainder of the report.

As a public space we chose the Karlsplatz, where ten CCTV cameras were established in 2005 to reduce crime. It took us about 15 minutes to find the first sign. This is due to the small size of the signs, which makes it difficult to spot them in a public area. Furthermore the signs are installed on street lights approximately one meter above eye level, which additionally complicates their detection.

After locating the first sign it was much easier to find further plates. As a matter of fact the signage does exist on every third or fourth street light. There is no phone number on the sign one can call for details on the data controller. Only a hint is given on the police department that is responsible for CCTV. Back in the office we found out the phone number of the "Polizeidirektion Wien" and tried to get some information about the CCTV cameras. After talking with three different persons we got some data controller details. The first contact at the hotline probably would have been able to answer more general (or more often asked) questions but not this one, and therefore, after explaining our request, transferred the call to another department. In this department the person who took the call was not able to answer the question after we again explained what we are looking for and offered to switch the call to his boss. His boss, the third person we were speaking to, was quite astonished about the nature of our request but was able to answer and give us the contact details.

Picture 1: Signage located in public space[47]

[47] The signage reads: Polizeiliche Videoüberwachung: An dieser Örtlichkeit werden von der Sicherheitsbehörde gemäß § 54 Abs. 6 Sicherheitspolizeigesetz personenbezogene Daten Anwesender mit Bildaufzeichnungsgeräten ermittelt und zur Abwehr und Aufklärung gefährlicher Angriffe sowie für Zwecke der Fahndung verwendet. (Translation: Video surveillance by the police: In accordance with §54 section 6 of the law on public security in this place the police is recording personal data about present persons with the help of image recording equipment. The Data are used to prevent and solve dangerous attacks and for manhunt.)

Picture 2: Signage located in public space with height perspective

Picture 3: Signage located in supermarket

For CCTV in a large supermarket we visited a chain supermarket. We did not see any signage the first time we entered the shop but when we left the supermarket we saw the signage on the sliding door (picture above). Due to the fact that no further information was given we talked with an employee. The first person that we talked to seemed to be absolutely astonished about the fact that we have the right to get information about CCTV. Therefore she sent us the manager who was unaware as well. We only got the information that we should send an online contact form to the company headquarters.

Picture 4: Signage located at an Airport

This picture shows CCTV signage on a sliding door at an airport in Austria. The signs fulfil the two requirements: it gives information about the reason for CCTV and who is responsible. However, from our point of view plates on a sliding door are not the best solution. It is abundantly clear that every person has to pass the door and the position at eye-level is good but nevertheless the door is constantly moving which makes it very difficult to read the text.

Visiting a bank branch we found CCTV signage on the sliding door at the entry. We asked an employee of the bank where we can get contact data and information about CCTV. We were questioned why we want to know this. We explained to the bank employee that we have a legal right to access our personal data. He was astonished and told us to wait briefly. After some minutes he returned with another employee of the bank who told us that he has no information and he is not able to give us any information. In particular he emphasised the words "not able". Nevertheless he gave us the advice to read the homepage of the bank and to contact head office. The CCTV signage of the bank indicated that there is CCTV but without any further information.

Looking for CCTV in a small local store we visited a jewellery store. When we asked the storeowner whether he has video cameras in his shop and what happens with the data he was astonished and asked us why we wanted this information. After explaining to him the reason that we have the right to access our personal data he stated that he hired a security company and that they take care of everything. Furthermore he looked for a business card and gave us the homepage address. By looking at the homepage we found out that this security company only sells equipment and monitoring systems for CCTV but each customer itself is responsible for protection of data privacy. So we got incorrect information from the shop owner which might be caused by the fact that he had no idea about data protection and wanted to get out of this unpleasant situation, or because he never cared about it (despite the

fact that he operates CCTV equipment) and might even think that it's not his business. One way or the other it shows again the endemic lack of knowledge when it comes to the legal provisions on data protection.

At the Vienna subway we found two different types of signs. The first picture shows the label directly in the subway, while the second picture shows the CCTV information in a subway station. It is curious that both types of signs only mention that there is CCTV but do not give any further information.

An enquiry to the customer service of the subway company revealed that they reject the right of access to personal data on the basis of a decision of the Austrian Data Protection Commission.

Picture 5: Signage located in a subway train

Picture 6: Signage located at underground station

Since the signage never had a phone number and often not even the responsible authority was named, it was difficult or even impossible to get information about data controller details.

Whether this is against the regulation in the Data Protection Act is unclear. There it is stated that the data controller has to be named on the signs if it is not obvious who operates the CCTV equipment. Since there is only one company in Vienna operating subway lines one could argue that it's clear where to look for information on the data controller. Nevertheless it's not helpful for data subjects.

Furthermore, the evident lack of expertise of the respondents (especially in the small local store) oftentimes resulted in receiving incorrect or incomplete information about how to request our personal data.

Concluding thoughts

For citizens it is important to know who is responsible for the collection of personal data and how this data is used. Therefore data controller details have to be available on homepages and contact details should be mentioned on signs. Otherwise, it is not possible for citizens to exercise their right of access to personal data.

In some cases, it was not possible to get information in the first attempt. Therefore, we started a second round in these cases. Unfortunately, even then we were often unable to get a decisive answer because people were unaware of the responsible authority. This was especially the case when we talked with employees in person. From our point of view, employees did not avoid providing information about data controller details deliberately, but there is a general lack of knowledge with respect to rights and handling of personal data. This unwitting strategy of denial may have its reason in a kind of ignorance towards the respective legislation. Since the fines for not complying are low and the Austrian DPA is not able to fulfil an active role in controlling data controllers most of them supposedly consider efforts towards complying with the data protection law as unnecessary costs. Nevertheless we assume that even easy to implement measures like better staff training and standard procedures within an organisation could help a lot in bridging this gap of knowledge.

During our investigations, we found some homepages with very detailed information about data controller details, and approximately an equal number that give inadequate information. An example of good information policy is the homepage of an Internet service provider. They refer to the data protection law and they mention that the contact person has the legal right to know which information is collected, shared with third parties and they even have a direct link to an E-mail address to contact. Furthermore, they offer a postal address and a fax number. For site "email data" we found a website which mentions the right of access to personal data. Moreover, they have implemented a link for e-mail enquiries. These two examples are in contrast to the privacy policies of global players like Google or Microsoft. But it has to be noted that our examined examples are small, local companies.

Concerning the CCTV signage, in most cases it was unclear who the responsible authority was. A phone number was missing in all analysed cases. This makes it more difficult or even impossible to get information about data controllers. Nevertheless the data protection law does not demand contact details on the signs.

In summary, the reflections of privacy practices lead to the following conclusion: the idea of the right of access of personal data has not been asserted. Due to the fact that hardly anyone knows about this law, maybe it can be described as a "dead law". Therefore, it needs to be asked whether regulatory control is lost.

SUBMITTING ACCESS REQUESTS IN AUSTRIA

Introduction

This country report reflects the experiences of submitting 17 subject access requests to different organisations within both the public and private sector and across a range of domains. While the results outlined below do not claim to reflect all practices and approaches of organisations in response to subject access requests, the chosen sample is nevertheless reflective of domains with and in which citizens interact on a systematic and consistent basis. Thus, the overall trends observed as part of this research may be indicative of the experiences a citizen may encounter when submitting a subject access request in Austria.

Methodological issues

For the Austrian cases I decided to send an e-mail in the first instance when submitting requests since I assumed that this would be the way I would go if I held little knowledge of data protection or data protection legislation since this is a low-threshold entry-point: faster than writing a formal letter, printing it, buying a stamp and so on. Additionally, a lot of companies answer with a generic confirmation or note that they received the e-mail, which might be handy evidence and creates an electronic paper trail if needed at a later time.

With regards to public CCTV systems or CCTV systems of public authorities, I switched to a registered letter as medium for the first contact (details can be found in the respective case descriptions). This was because I have found that public authorities often carry out their identification procedures by comparing the signature in the letter with the signature on the copy of my ID (in this case my driving license[48]). The letters were sent via registered mail because with this measure I could prove that the letter had been sent and when I had sent it, if this became necessary.

The legal time limit for data controllers to respond to subject access requests in Austria is eight weeks. As part of the access request procedure, the requester has to prove his/her identity, which in theory can be done by giving the data controller some details about the stored data or one's birth date, which would not be known to any person, and ask for an answer via a registered letter. Then the staff of the post service would check the identity before delivering the letter.[49] Additionally, the data subject has to "help" the data controller to

[48] In Austria every citizen can have different types of IDs, for example: "Identitätsausweis" – a national identification document (in form of a card), "Personalausweis" – the national identity card (similar to the first one, but valid for travelling in most European countries), the passport, an official service card or a driving license. These are called "Amtlicher Lichtbildausweis" (meaning ID with a picture issued by a public authority; it contains at least the first name, last name, date of birth and location of birth) and are an accepted way of identifying one self.

[49] On March 7th, 2014, the Austrian Data Protection Agency published a new version of their information about the right to information on their website, informing interested citizens that it is good practice to send a written letter and not an e-mail since all data controllers have to identify the requesting person by comparing the signature on the letter with the one on the ID, and that it is not sufficient to request an answer via a registered letter with reply advice. It gives no special reasoning for this new specification (this was not a formal decision but rather an informal information in the news section on the agency's website), but it is mentioned that these registered mails cost more postage and therefore, since the requester has to prove his/her identity, the data controller should not have to bear the costs for this kind of delivery.
Since this was published after all the initial requests were sent this is only relevant for this study because it shows that the procedures of the public authorities have (already?) been in line with the later information of the DPA.

find his/her data if necessary, so the burden of time and effort on side of the data controller is acceptable and is not disproportionate.[50] Access to the data subject's information can be restricted if the data controller proves that there exists an overriding legitimate interest on its side or a third party's interests.[51]

Overall, 17 subject access requests have been sent. To make no mistakes in the legal phrases and in trying to keep the communication with data controllers efficient, in some cases I made use of templates and suggestions for subject access requests published by an Austrian NGO which tries to help people in their struggle for informational self-determination. Nevertheless only six requests were answered in a satisfactory way, some of them with room for improvements. Five have been completely ignored.

	Public/Private	**Site**
1	Public	CCTV in an open street
2	Public/Private	CCTV in a transport setting (Subway)
3	Public	CCTV in a government building
4	Private	CCTV in a large department store
5	Private	CCTV in a bank
6	Public	Criminal Intelligence Records
7	Public	Border Control
8	Public	Europol
9	Private	Loyalty card (air miles)
10	Private	Loyalty card (air miles)
11	Private	Mobile phone carrier

[50] See the legal analysis above for details on subject access request regulation.

[51] Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended by March 17th, 2014, unofficial English translation, §26/2: *"The information shall not be given insofar as this is essential for the protection of the person requesting information for special reasons or insofar as overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an obstacle to furnishing the information."*

	Public/Private	**Site**
12	Private	Banking records
13	Private	Credit card records
14	Private:	Mobile phone carrier
15	Private	Amazon
16	Private	Microsoft
17	Private	Facebook

Finally two formal complaints have been sent to the DPA: Hutchison (mobile phone carrier) and Nokia (mobile phone manufacturer). Possible future answers are not part of this report since the time limit has been reached within this project. Hutchison has been selected because I'm interested in the DPA's response regarding data collected under the data retention directive, and Nokia to see whether this big company can improve its handling of subject access request when confronted with a DPA (see details to these cases below). Maybe there will be more complaints in the future if this is a satisfactory step in completing the research outside the project and the personal experiences made in the context of this project.

Case by Case Analysis

<u>Public – Facilitative Practice</u>

Europol

The DPA refers data subjects to an e-mail address if someone wants to contact Europol in Austria. This contact point is in a special section of the Federal Ministry of Interior. So I sent my request to this address. Asking for all the data they have about me, even if they are in a joint information system. The time for answering such requests is 3 months (not 8 weeks as it is for all the other data controllers in Austria).

Four days later I got a letter from the DPO's office telling me that the Europol information system is not a joint information system. I never claimed that, but maybe they had a problem with my German. The letter stated that if I still wished to make a subject access request, I should do so via a letter and send a copy of my passport or "Personalausweis (identity card)", because the driving license is not sufficient.

I sent it a week later and another two weeks later I got another letter from Europol telling me that Europol is not processing any data about me, together with an image folder about Europol making Europe safer. So while the response received was somewhat short, it can nevertheless be considered a complete and satisfactory answer.

Polizei/Innenministerium

I sent an e-mail to the Federal Ministry of Interior which is responsible for the police in Austria. The email was sent to a generic address for citizens' inquiries. For the text of the mail, I used a template from a NGO called "Arge Daten". Since I heard that the police are not very helpful in sending requests like this, I thought the template might be a good idea. The author of the template researched all registered data processes so one could choose the ones that sound like there could be data about one self and ask for that. It is said that the police only address data questions made specifically and expressly in access requests rather than answering general requests for all data held about an individual.

A few days later I got a letter telling me that they are not able to answer my request because an electronic or personal signature is missing. In this letter they also refer to and quote from all relevant regulations, including the ones that define their duties.

As such, I sent them a formal letter I had signed together with a copy of my driving license. Three weeks later, I got a very long letter from them listing all the relevant databases and data processing procedures (including ones I hadn't asked for) and informing me item by item, obviously collected from different departments, about the data they have stored about me: none. Incidentally, according to Austria law, the language used in the letter to explain that no information was held about me was the same as would be used if the data controller was not permitted to confirm/deny if any data was held about me.[52]

In addition they informed me about the fact that when processing data on IDs and ID data they are processing the data on behalf of the Vienna city police department and a department of the city administration. I would therefore have to turn to them if I want more information about these data.

They seemed to be competent and quite fast in handling requests like this. Moreover, they tried to handle the information securely: I had to send them a signed letter and got back a letter which must not be delivered to anyone else than me. This is in general a good practice although the formal requirements might be seen as burdensome for data subjects if they can't ask for "their" data via e-mail.

Border Control

I was informed by the police/Federal Ministry of Interior, that in the three databases I mentioned my request (National Schengen Information System (N.SIS), Supplementary Information Request at the National Entry (SIRENE) and Schengen Information System II (SIS II)) there is no information about me. They are obliged to disclose this to me under the right of information regulated in the data protection law so the data controller was legally compliant in this case.

<u>Public – Restrictive Practice</u>

[52] Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended by March 17th, 2014, unofficial English translation, §26/5: *"In all cases where no information is given even when in fact no data on the person requesting information is used instead of giving a reason in substance, an indication shall be given that no data are being used which are subject to the right to information."*

No significantly restrictive practices were observed during this research in requesting (non-CCTV related) personal data from public sector institutions. However, this is not to say that public institutions displayed universally outstanding or exemplary behaviours. Rather, this merely indicates that the extent of restrictive practices experienced in the private sector (completely ignoring the request; seemingly deliberate attempts to dissuade the requester from following up his/her access request) were absent in the public sector during this research.

Private – Facilitative Practice

Credit Card Records

I sent my subject access request by e-mail to a generic customer service address I found on the company's website. Attached to the mail was a scan of my driving license. I also informed them of my credit card number.

An immediate generic response was sent to inform me about the reception of my mail. Two weeks later I got a letter from the company, in which the company informed me about the following:

- the data they have stored on me and where they got it from (my application);
- that they additionally store transaction data which would be listed in my monthly account statements (they did not list all the transaction data they have currently stored on me therefore it's not possible to see how long the history is);
- under which number the processing is registered;
- why they need it;
- a list of third parties which fulfil services for the company and therefore also have my data (but have to keep it securely, use it only for the intended purpose and delete it afterwards);
- on the basis of which DPA decision they are allowed to transfer data to other countries,
- that they are not transferring data to credit scoring companies.

Although there was again no information about automated decision making, this was in general a timely and quite complete answer, which was easy to understand.

An interesting detail is that they are willing to answer a subject access request sent by e-mail but, in an unrelated matter, they were not willing to change my address without me sending them a signed form via postal service (I have to download the form from their website, insert the necessary information – old and new address – and print it). As such, a notable juxtaposition emerges here in which high levels of privacy security practices are employed when I seek to change a fairly basic detail of my account settings but significantly lower levels of security are demonstrated when a large amount of personal data is in transit. This perhaps illustrates the (low) regard given to the importance and value of customers' personal data by this organisation.

Bank Records

I have my salary account, a savings account and a small loan at the bank to which I submitted my access request. They also issued my Visa card. Basically most of my financial business is known to this bank. A branch office of this bank is located next to the place where I live. So I

visited this branch office, drew some money from the indoor cash machine, took a picture of the CCTV cameras in the foyer and left. After this visit I wrote an e-mail requesting the data from the CCTV system, the data from the credit card account and all the other data they have on me.

A week later I had an appointment together with my girlfriend with our account manager, who is, as it happens, a friend of my girlfriend. When we arrived she showed me the mail I had written a week before and asked me whether this was from me because in her eyes it was unusual for me to send a formal mail like this, which I had addressed to a generic customer service address. I affirmed that this mail was from me and asked her why she has been forwarded it, and what she was going to do with it. She answered that she got it because I'm a customer of the bank and all customer requests are forwarded to the respective account manager. She had never seen something like this before, but planned to send it to the legal department. In a very professional way she did not ask me why I sent this but seemed to accept the fact that I wanted to know this.

Exactly six weeks after my initial e-mail I got a letter from the bank. The letter listed the information they have about me, like name, address, date of birth, but also location of birth (with wrong information), civil status, the name of my father, my mother and the name of my girlfriend (so they store that I have a girlfriend and her name) and some others. Additionally a list of their products I use and a list of cards issued to me. What I didn't get was a list of all the account transactions.

They also informed me on:

- where they got the information from,
- why they are storing it (purpose and legal basis),
- that my data are not transferred to another country,
- all the other data which are stored about me do not contain personal information but only account- and product-specific details which are needed to process my transactions,
- that no automated decision are made which would be subject to the regulation in §49 in the Austrian data protection law.

They also sent together with the letter 10 prints of still frames from all the CCTV cameras in the foyer on which other people's faces have been broadly covered with white circles. Since I had been in the branch office only for about 3 minutes, ten images out of this timeframe seem to be an acceptable amount of information. Although §50e in the Austrian Data Protection Law states that the data has to be sent to the data subject in a usual technical format (or if the data subject wishes to do so it can view the video at the data controller's office; if the identity of other people cannot be masked it would also be sufficient to send a description of what can be seen on the video footage), which raises the question whether a print is a usual technical format for video images.

In general it was not the fastest answer but a quite complete one. The prints of the CCTV footage are ok for me as a data subject because I can see what has been recorded so my request is essentially fulfilled.

I was a little bit disappointed that they did not reveal at least a little bit of the calculations going on in the background, based on the knowledge of my financial transactions. For example, I know that this bank calculates credit scores because they told me when I was

taking out the loan. But these calculations are not necessarily a case of automated decision making as it is defined in the data protection law. As a customer however, one has the theoretical opportunity to disagree with the score one is given and to change it, and of course calculating a score is not the decision itself whether someone gets a loan or not. Therefore I don't think they answered incorrectly but maybe something's missing. Ultimately, in cases such as these, citizens cannot be sure of whether they have received the entirety of the personal data held about them and this is one of the major problems with subject access requests.

Loyalty card (air miles)

I have a loyalty card issued by a major air carrier. Therefore I navigated to the company's website and searched for an e-mail address. Since I couldn't find one, I used a form on the website. When entering my request, I realised that the text field is only made for short messages. So I reduced the extent of my request and just told them that I wanted to send a subject access request to them and asked for a suitable e-mail address to send it to.

I did not received an answer directly to this query but after around three weeks, I got a letter from the air carrier company giving me a detailed list of all the data they have stored about me and informing me about the legal basis on which the data is stored, also referring to the correct section in the Bundesdatenschutzgesetz (the German Federal Data Protection Law).

This can be seen as one of the best examples in this research. They answered in time, in a friendly manner, without trying to make you feel bad, and in a way that I think the answer is complete and correct. They even sent me the answer to a subject access request *before* I had actually sent it. While other data controllers demand that I have to send a letter, for the company the fact that I expressed my intention to send a request was sufficient to answer it. This pro-activity and willingness to process my data request was unique in the research and therefore represents an example of one of the most facilitative practices encountered. A minor point may be made however that my personal data was disclosed to me without undergoing any identification checks and had this been a fraudulent request by someone with access to my letter box, the data controller would have provided my personal data with no consideration for the security of my privacy. As such, the commendable willingness to pro-actively answer access requests must be balanced against ensuring proper security procedures are followed.

<u>Private – Restrictive Practice</u>

Amazon

I sent my subject access request to Amazon via a form on amazon.at (which is identical to amazon.de). On the same day I received an answer by e-mail from customer support. In a very friendly tone I was informed that Amazon is only storing the data that I can see when I log into my account. Additionally I was referred to the data protection policy on the website with the note that I can contact them if the policy would not answer my questions and they would send me the requested data.

So I wrote back an e-mail (sending a reply to their mail) telling them that I would like to have a complete compilation of all the data Amazon is storing about me, and that the questions regarding automated decision making and sharing data with third parties had not been answered in their previous correspondence.

After I had sent the reply I got a generic error message from Amazon (from an address used for information about the status of an order) informing me that customer support had not received my mail and that I should use one of the contact options on the website or call them. I decided to use the e-mail address used in the privacy policy (impressum@amazon.de). Since all companies in Germany (as well as in Austria) doing business via a website have to give their customers an e-mail address in the imprint, I thought the company might read the mail and react. However I never got another response from Amazon regarding this matter.

In this case, the first answer came fast and was friendly, and if it would have been satisfactory it could have been a best practice example. But unfortunately their answer was in my view not what I am entitled to under the Austrian data protection law. They have to give me this information and not answer in a way that sounds like I can do the job on my own by searching their databases. In addition, I assume that the history of orders I placed on their website within the last few years is not the only data they have on me. A proof for this could be seen in their practice of advertisements: When I navigate to their website and search for something, I will get an offer within the following weeks for the category of the goods I searched for. To send me this personalised offer/advertisement they have to store the information about my surfing habits and searches on their website. At the very least, this kind of information (and I would bet much more) is not accessible via my customer account.

It looks like answering the easy way is part of their business strategy which probably satisfies most requesters. It further seems that in the absence of complaints from dissatisfied data subjects, DPAs across Europe accept Amazon's working practices. In any case, should such complaints be submitted and Amazon fails to win a legal battle, the potential fines placed upon data controllers which in Austria in this case range from € 500,- to € 10.000, make such non-compliance sound like a bearable risk for a company the size of Amazon.

Mobile Phone Carrier

The company to whom I submitted my request have been operating as a mobile phone provider network for some years and only recently took over one of their bigger competitors. So it was interesting to see how much data (going back in usage history) was stored about me.

I used the contact form on their website to send them my request. In addition to the subject access request regarding the stored data and the questions about automated decision making and sharing data, I specifically asked for the data stored under the data retention regulation.

Five weeks later I got a long letter from the company in which they informed me:

- that they only process data on a legal basis (naming the relevant Austrian laws),
- that I gave them data about myself when accepting the terms of my current contract, and that this data was sent to the Austrian office of CRIF[53] for a solvency check,
- that traffic data is stored as long as it is necessary for billing, after that it is deleted or anonymised (no word about data retention at this point),
- that they don't store content data
- that they have attached a compilation with all the data stored about me.

[53] See also the WP3 case study on credit scoring.

Furthermore they wrote that they are legally obliged to store traffic data under the regulations regarding data retention (referring to the respective section of the Austrian Telecommunication Law), but that disclosing this data is legally (they refer to overriding legitimate interests without specifying them) and factually impossible because:

- they are not the data controller and are therefore not obliged to disclose this data to me,
- data stored for the purpose of data retention is always historic traffic data for which there are certain regulations regarding disclosure,
- disclosing this traffic data would therefore be unlawful,
- the data protection agency has decided that the answer to a subject access request must never include traffic data (here they quote from the DPA's decision),
- retention data are encrypted and separated from the other data and therefore it's technically not possible for the company to access the data except from the situations described in the Datensicherheitsverordnung (data security decree)[54] which does not foresee the disclosure to private persons but only to law enforcement,
- the company is not the data controller when it comes to data retention (again).

Attached to this letter were print outs of four different sources (data bases/tables). One listed all my standing data (including that my first contract started in 2001), another was a list of all account changes from 2004 to the present date, one titled "changes subscriber" listed the changes I can trigger via my phone or website regarding additional services or packages (only the ones for the current contract), and the last one – "contacts" – listed all the communication between the company and me (probably from their customer relations management system) since the acquisition from their competitor, including the full text of my subject access request.

The question regarding automated decision making was not directly answered. In good faith, one could deduce from their claim that the company is processing data in compliance with the law (they explicitly mentioned the data protection law, which regulates that automated decision making is only allowed under certain conditions and if it does not affect the data subject in a negative way or has judicial consequences) that Hutchison is not using the data or the data they receive from CRIF for automated decision making.

In general this was a complex answer which was difficult to comprehend without being a lawyer. I tried to analyse the different arguments and concluded that the answer is not complete. (Additionally it's strange to be informed that they are not storing content data which they would never be allowed to anyway.) For example, the list about changes in my account has a number in the comment field titled "Telco: Bonität" (telco credit rating) which changes between once and four times a month. Sometimes it goes up, more often it decreases. When answering a subject access request, the data controller is obliged to deliver the data in an understandable form. In this case, I can see that they are rating my creditworthiness, but I don't understand how it is calculated. Moreover, this looks like an automated calculation and therefore raises the question whether any automated decisions are made on the basis of this data.

[54] The Austrian Minister for Traffic Infrastructure, Innovation and Technology (2011), Datensicherheitsverordnung, BGBl. II Nr. 402/2011, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007596 (last accessed Feb. 21st, 2014.

Moreover, the decision of the data protection agency quoted in the letter refers to something different than retention data. It is about traffic data in itemised bills. Since it is (in the opinion of the DPA) not clear that only one person is using a certain telephone/number, the called numbers on an itemised bill have to be truncated to protect the privacy of a potential third party. The Austrian telecommunication law does not mention the right of access to one's data in the same way as it is regulated in the data protection law. But in the telecommunication law, the provisions for the data retention are codified. And there it is only listed under what circumstances the data might be passed to law enforcement. From this fact, Hutchison deduces that it is prohibited (since not explicitly mentioned) to pass this information also to data subjects exercising their informational rights via a subject access request, because the telecommunication law is – in their point of view – the so called lex specialis compared to the data protection law, which is seen as the lex generalis in this case. In my opinion this argument is weak especially since in my understanding, the exegesis of the principle "lex specialis derogat legi generali" says that this is only true if the lex specialis is more demanding or more accurate than the lex generalis, and must not be applied if the two norms are contradicting.

The data security decree only regulates the how and when of data disclosure to law enforcement agencies and has no word about private persons or subject access requests. Again, in my opinion this does not allow the company to deny a data subject's right to information. Additionally it's interesting to read that they are *technically* not able to access the data unless (in their opinion) the law permits it.

However, the worst part of their argument is the claim that they are not the data controller for the data stored under the data retention regulation. Everyone can look up the company (Hutchison) in the Austrian Datenverarbeitungsregister (Data Processing Register) and look at the registered data processings, where, under number 0908177/008, a data processing is registered for "*Verarbeitung und Speicherung von Vorratsdaten gemäß §§ 102a ff iVm 94 TKG iVm DSVO sowie Übermittlung in verschlüsselten und gesicherten Dateiformaten an die Strafverfolgungs- und Sicherheitsbehörden über die Durchlaufschnittstelle gemäß DSVO*" (Processing and storing of retention data in accordance with §§102a and the following together with §94 Telecommunication Law together with the Data security decree as well as transferring in encrypted and secure file formats to law enforcement- and security agencies via the clearing house defined in the data security decree). They argue that they are not the data controller since they are storing this data under the national implementation of the data retention directive for law enforcement. However, the data processing register shows that they are responsible for this processing.

In this case a formal complaint has been filed with the DPA. In this process my complaint is forwarded by the DPA to the respective data controller with the invitation to comment on this complaint. Four weeks after I sent my complaint to the DPA, I got an e-mail and a letter by registered mail from the company with the same content, the answer from Hutchison's legal department to my complaint. In their answer they explain some of the abbreviations and that the expression "Telco: Bonitaet" would be a leftover from an older version of their software, which is not in use anymore. It would reflect my payment history (no further explanation) but have no consequences and therefore is not relevant regarding §49, automated decision making, from the Austrian Data Protection Law. Regarding the questions on the retention data they refer to the case C-46/13-2 at the European Court of Justice because the Austrian Data Protection Agency sent these questions to the court for a preliminary ruling. There has been no decision on this by the court yet. My criticism regarding their denial of the fact that

Hutchison is the data controller for the data collected under the data retention regulation remains unanswered at the time of writing.

Facebook

Since I don't have a Facebook account this communication was done by my colleague as per the third party protocol of the research methodology. I prepared the request with references to the respective regulations in the Austrian data protection law. The request was sent through a form[55] on Facebook's website which should be used for all customer requests regarding the use of data. She entered the text, added her personal details for identification, offered additional information or help if needed and sent the request.

No answer has been received within eight weeks or later.

Microsoft

The Microsoft website does not offer an e-mail address for contacting the company. Therefore I entered my subject access request into a contact form on the website. When trying to send the form, it became apparent that I had entered too much text into the box. So I reduced my request in order to simply ask where I should send my access request to. After sending the form, a notification was displayed informing me that the company will try to answer my request within 24 hours. I never got an answer on this request.

After 2 months I decided to have another try and sent an e-mail to three generic mail-addresses that have been used in the past for correspondence between Microsoft and me. I got an undeliverable-error message for one of the three but not for the other two.

In my mail I gave them a lot of information about where they could have stored data about me (registered Microsoft partner, Action Pack subscription, Windows Phone user; for all this a Microsoft Live account is needed) to fulfil my legal duty of contributing to finding the data about me.

I also didn't receive an answer on this mail within the obligatory 8 weeks or indeed later. Meanwhile I'm still getting marketing information from this company.

Loyalty card (air miles)

I got a loyalty card issued by a major airline because at the time, I had a flight from Munich to Vienna and the lady during the check in at the airport told me that I would be entitled to take part in the reward program, and I thought that the airlines would store the data anyway therefore I could as well collect the miles.

Fortunately, I didn't have to determine to which airline I have to send my request because the loyalty card scheme has its own website with a contact form I used more than once in the past to recover a forgotten PIN/password.

This time I also used the contact form on their website and entered my request there. Immediately afterwards I got the confirmation that they have received my request and will answer as soon as possible.

[55] Form for sending question regarding the use of data:
https://www.facebook.com/help/contact/173545232710000 (last accessed Feb. 21st, 2014).

Unfortunately I didn't receive any answer within the obligatory 8 weeks or afterwards.

Mobile Phone Carrier

I use a smart phone manufactured by the company with a lot of preinstalled or subsequently uploaded apps provided by them that collect data about the usage of the telephone. Additionally years ago, one of my first mobile phones was also manufactured by the company. Back then I registered for their mailing list and received newsletters and so on. Therefore the company could have stored a lot of data about me and my old and current mobile phones.

Since I couldn't find an e-mail address on the company's websites I decided to call the company and ask where to send my request to. Calling them costs € 1.09/minute. The first person on the other end of the line had no clue what I was talking about, had never heard the expressions "Datenschutz (data protection)" or "Auskunftsbegehren (subject access request)". He seemed to be overstrained by my request and had to ask another person. While he was asking, I was placed on hold. When he was back with me he asked for my name to pass me on to the next level, then he stopped speaking, nothing was happening and I was still waiting. After a minute I was switched to the waiting loop. Then another person was on the line. He said he had heard my request would be about data protection. He told me that he could not help me with this request but was not offering to pass me on to someone who might know something about access requests. So I was asking to be transferred to someone knowledgeable. He refused and told me to use a form on the company's website for my request. I was asking for an e-mail- or post address. He refused to give me any address. In the background it sounded like the whole call centre was listening to this conversation. He repeatedly advised me to use a form on the German website which is used for complaints. I tried to explain that I live in Austria and that I didn't want to complain, I just wanted to be informed about the data that is stored about me and that I have a right to get this information. He told me that the form for complaints is probably also available on the Austrian website and that I should use this one for my request. The call ended after 6 minutes.

A little bit disappointed, I searched for the form on the website. After I had found it, I entered my request although the categories I had to fill are not useful for a subject access request and the text on this site explicitly stated that this form is only for complaints and questions regarding the operating system can be directly sent to Microsoft. Since the person on the phone recommended especially this form I decided to use it anyway. Maybe a friendly employee would forward it to the right department. After sending the request I got an immediate generic reply confirming that customer support will deal with my complaint. If I don't have a complaint I should use the contact options listed in the support section of the website.

Navigating to this section starts a wizard where I had to choose the model for which I want support. Choosing the phone I use led to another website where all the different functionalities of the phone are listed but nothing else. Clicking on one of them opened a Q&A section on this topic. There simply is no chance to contact the data controller.

Since I never got an answer to my request, a formal complaint has been filed with the Austrian DPA.

Once in a while one is forced to contact a company via its call centre. Sometimes these are unpleasant experiences, because the underpaid employees in a call centre don't get the

information and training they would need to fulfil their tasks. Sometimes they are very professional, listen carefully and act accordingly in a – at least from a customer's perspective – very satisfying way. And sometimes they act like they have to deal with an imbecile who is not able to read and understand, not listening to what is said. In this case I was really curious how a company of this size would handle my request. Additionally, I wanted to know what data they are storing about my smart phone usage. After other experiences in this work package I took it as kind of a sporty challenge to find out what I'm entitled to know. Metaphorically speaking I hit a brick wall. This is often disappointing but especially in this case, when there is no explanation why it has to be like this, why they are not able, willing or – in their view – responsible for answering. They are just fending off interested persons.

It seems to me that the company is not able to handle requests like this. Moreover, maybe they are simply not willing to do so. A company of this size could easily establish an internal process to handle subject access requests and organize an entry point to this business process for customers on its website especially since this is a corporation based in an EU country. Another thing that is well illustrated in this case is the fact that a lot of companies have a cultural problem with subject access requests. The organisational culture of most companies seems to have learned to deal with product-specific requests, with public relation communications, with complaints and brand marketing. There is some kind of binary thinking going on, when it comes to customer communication. If a customer has something positive to say, everything is fine. If it is something negative, it's a complaint and the company has to act. Since a subject access request urges the company to act, it has to be a complaint. Insinuating that some of the companies do not have the business processes necessary for answering such requests, it could also be an unconscious act of defence, assuming that the customer wants to complain about impossibility of exercising their rights under data protection law.

Most companies are able to comply with all kinds of laws and regulations. Multinational ones even have to obey rules from different countries. Often compliance departments are formed next to the legal department to better focus on how the company can efficiently comply with all the regulations. And nevertheless, it seems quite hard to comply with data protection law, probably because of the fact that so far no severe fines have been imposed for violations of the data protection law.

CCTV

CCTV in a public space

From the Viennese opera to the Karlsplatz is an underground passage with shops. It was one of the first in Vienna. Connected to this passage are stations of three different subway lines, 2 bus lines and 5 tram lines. Karlsplatz/Opera is also one of the two hubs for the Vienna Nightlines (buses in service during night hours when no other public transportation is available).

For some years a small park at Karlsplatz was the meeting point for drug trafficking. Therefore the whole area was extensively watched by police controlled CCTV cameras. I went through the whole district from the opera to Karlsplatz, entered the park, visited the so called "Schubertlinde" (a lime/linden tree in memorial of the composer Franz Schubert), took some pictures and went back to the opera.

The cameras in the park have signage stating that the police department of Vienna is responsible for these cameras. So I decided to write them a registered letter (when entering the passage there is the signage the public transport company in Vienna, with no additional information, but living in Vienna, one knows the pictogram used by this company; seeing a different signage in the district gave me the impression that the company would surveille the area as part of their station monitoring).

Ten days later I got a reply from the police department of Vienna, dated a week after I had written my letter. It informed me about the fact that my letter was received by the police department four days after I had sent it. The police monitors the square and the passage (not the public transport company). They informed me about all the relevant details as to why they monitor the area, the legal basis for doing so and the storage time. After 48 hours the footage is overwritten automatically, therefore, when they received my request, there were no images stored about my person, since there had been no incident during this period which would have stopped the automatic overwriting.

Although this was disappointing since I did not receive any video footage, this response in fact represented one of the best answers received in the research insofar as it was correct, complete and fast.

CCTV in a transport setting

The company organising and conducting public transport in Vienna is well known to the public interested in data protection. This company is also interesting because it was founded as part of the city administration. Some services in Vienna have been administered by the city for a very long time, like the fire brigade. Other services were added later especially after World War I when all citizens in Vienna were allowed to vote and the majoritarian socialist city was separated from the surrounding country (Lower Austria). At the end of the nineteenth century, the city administration started to municipalise more and more services like energy, funerals and tram services. Later administrations in the 1920s and 1930s tried to regulate an increasing number of services because of the social and welfare problems after the war and in taking a socialistic view about what the authorities should handle, and what can be done by the individual, a family or private organisation; following in its own way the ideas of a paternalistic state. Vienna became a socialist model city in this time before a lot of these accomplishments were reversed during the totalitarian regimes in the 1930s and 1940s.

The effect of this development caused a big bureaucratic administration of all these services but in the late twentieth century in Vienna when neo-liberal economic policies led, amongst other outcomes, to the outsourcing of these parts of the administration into a company under private law. This holding company has different corporations. As a result, the company for public transport is a private company, but still under a very strong influence of the city administration, because the City of Vienna holds 100% of the holding company. This case therefore presents something of an example of a data controller straddling both private and public spheres.

In recent years, there have also been some controversies around data protection and proportionality around the company, particularly when they started using CCTV systems that were able to record and store the images filmed.

Abusive use of data has been reported on some occasions since the beginning of the CCTV test phase and later. For example, a politician received images of drivers to identify one he wanted to complain about. Elsewhere, unauthorised personnel accessed the data of an incident which had taken place two months previously (they are allowed to store the data for 120 hours and claim that it can only be accessed by selected, specially trained authorised personnel). Finally, it was discovered that the data from the CCTV systems had not been encrypted before storing it.

The Austrian data protection agency took the controversial decision that the right of access to data from video surveillance systems does not come into effect until the material has been analysed. However, this decision was deregulated/subsequently overruled[56] by the Austrian Higher Administrative Court last year. In 2013, the European Court of Justice ruled against the Austrian state, finding that the necessary independence of its data protection agency envisaged by the Data Protection Directive was not guaranteed in Austria. Given this alleged lack of independence, the Austrian Higher Court decided[57] that this (the non-independent data protection agency) agency was not competent to issue decisions in cases involving data protection and privacy matter, including in the case of CCTV and access rights. In other cases where this has happened in recent months, the data protection agency, which after the 2013 amendment is now considered to be independent and therefore competent to decide, revisited previous cases and reissued its opinions. It can be assumed that this will happen with the decision on access rights as well.

I sent my subject access request to the company by e-mail on a Monday evening, immediately after travelling in one of its trams with installed CCTV system. Attached was a copy of my driving license and the email included a description of what I was wearing and when and where I might have been filmed by the cameras in the tram. I got back an error message because the attached scan of the driving license was too big. So I reduced its size and resent the mail the next morning.

The next day I got an e-mail back from their customer service. Attached was their answer to my request. In this answer someone from the compliance department informed me that they are not able to fulfil my request because I have to write them a letter and sign this letter, so they can compare the signature on my driving license with the one on the letter.

So a few days later I sent them a letter, including a copy of my driving license, referring to the previous correspondence. A month later, I got an answer from the same person in the compliance department. In her letter she cited the respective paragraphs of the data protection law, referred to the previous correspondence and noted that her answer was sent in due time.

The cut-off date for their internal collection of data about me was two weeks after my letter and 4 weeks after I sent my initial e-mail. As such, if they held more data about me beyond these timelines, they would not disclose it to me in their response. They reported that they had stored my name, gender and e-mail address when I corresponded with the company in the summer of 2013 as well as the reason for storing and the legal basis for doing so. All the

[56] The Austria Higher Administrative Court effectively found that the DPA never had the competence to make this ruling at the time. Therefore, the court's decision equated to the DPA's ruling never having happened in the first place.

[57] Austrian Higher Administrative Court (2013), Zl.2010/17/0186-6, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20100730_K121605_0014_DSK_2010_00 (last accessed Feb. 20th, 2014).

questions on automated decision making and the potential sharing of data were answered (by stating that the company didn't do any of these).

Regarding the data from the CCTV systems, they informed me about the reason why they are allowed to store the data and for what purpose, who has access to the data, that it is encrypted to prevent unauthorised access, and is only analysed in case of an incident. The correspondence then included a page of explanations as to why it makes sense to deny the right of access in cases where the data has not been analysed. They cited the now obsolete decision and the corresponding opinion of the data protection agency and came to the conclusion that in my case, there was no analysis of the data and therefore they are not allowed to inform me about the stored data, which in the meantime had been overwritten anyway.

In an additional paragraph they informed me about the high effort which is necessary to access data in the decentralized network of the company and therefore asked me to limit my subject access requests to the situations for which the CCTV system has been installed (vandalism and protection of their personnel and passengers).

Generally speaking, it looks like they are ignoring (perhaps deliberately or negligently) the fact that the decision they are quoting has been deregulated/overruled because it is a convenient argument to deny the right of access. However, it should not be discounted that the legal proceedings following a formal complaint would cause the Data Protection Agency to reissue its former opinion and prove the company's legal point of view to be correct after all. So a fundamental lack of clarity exists here.

Furthermore they used a reporting date which was long after my initial request, when the relevant data had already been deleted. This is against the law, where it is stated in § 26 section 7 that in case of a subject access request the data has to be stored for at least four months starting from the date when the data controller is informed about the subject access request[58]. In addition they tried to persuade the data subject to abandon his/her right to access for economic reasons (from the company's point of view). This is an argument often heard in discussions about video surveillance but completely out of place in this context because the company argues that the data from CCTV systems in trains and stations is stored in the respective location and not centrally. Therefore access to this data requires a lot of effort and lots of money. Interestingly, they told me that all the data about me was already deleted – so there shouldn't be any costs, unless they have accessed and searched the material. But in this case they would have analysed the material and their believed exemption from answering my subject access request would not be valid anymore.

When communicating with a company of this size, which maintains its own compliance department, it can be expected that they know about the legal situation regarding their rights and duties. Therefore it looks like this company tries to fend off citizens exercising their rights. In addition, the answer from the data controller implies that the request I sent may have abused the right of access by sending a subject access request without being the victim of a crime. Trying to give the data subject a guilty conscience because he/she tried to exercise

[58] Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended by Feb. 20th, 2014.

a right that only exists because the company is using video surveillance is in a subtle way one of the meanest things to do in this context.[59]

CCTV in a government building

The building I visited uses a CCTV system inside and around the building on the outside. I decided to add this building within the category government building because it gives easy access to people not working there since you can visit the building any day in the week and take a touristic tour through the historically interesting parts of the building.

So one afternoon I joined one of the tours together with my girlfriend, took some pictures before, and after the tour, inside the building and on the outside, and back in the office sent a registered letter to the building's administration.

Similar to the letter described above from the police department of Vienna, a little bit more than a month later I got a letter that informed me that my letter took seven days to reach the parliamentary administration. Since the footage is only stored for 48 hours (unless there is an incident that makes it necessary to analyse the data), there was no data about my person stored when they received my letter.

Additionally I was informed about who the data controller is, why the CCTV system is operated and under which number the processing is registered.

Strangely enough, the parliamentary administration also informed me about the opinion of the DPA regarding non analysed data from CCTV systems. So I would expect, even if they got my request earlier, they wouldn't have sent me the footage.

Interestingly, the administration was the only authority that sent an ordinary letter when answering my request. All the other authorities sent a letter with personal service to the addressee.

CCTV in a bank

See description above.

CCTV in a department store/shopping area

In the first district, next to my office, is a mall with different shops, which uses a CCTV system. I entered at one of the main entrances, looked around a little bit, took a picture of one of the CCTV cameras and left the same way I had entered the building. Back in the office, I sent them a registered letter and asked for the data from the surveillance cameras.

Four days later I received a letter from the company which organises and administers the mall stating that they are not the data controller for the CCTV system. The letter also explained that the owner of the building has installed the system and is responsible for it. The building is owned by a big insurance company and the administration forwarded my request to this insurance company, so the data controller can answer it. Unfortunately I never received an answer from them.

[59] Quote from their answer: "D*er Vollständigkeit halber möchten wir darauf hinweisen, dass aufgrund der dezentralen Datenträger in Fahrzeugen und Stationen die Beschaffung der Daten und die Auswertung mit hohem Aufwand und hohen Kosten verbunden ist. Wir dürfen Sie daher ersuchen, die Auskunft über Videodaten auf diejenigen Fälle zu beschränken, deren Zweck die Videoüberwachung dient."*

Conclusions

As described below (Public vs Private) and briefly in the methodology section at the beginning of the report, I sent out e-mails as the first correspondence with the data controller. Back then, the subsequently published guidance of the Austrian DPA didn't state what medium to use when sending subject access requests. For a lot of people interested in data protection, e-mail is their standard way of professional communication. If formal requirements prevent organisations from answering such requests by handing out the requested data, it would be nice if they would at least not overwrite the requested data while they wait for the formal letter. These requirements might have their benefits when it comes to identification and the security of the requested data, but they also prohibit disclosure (e.g. the disclosure of CCTV data in most cases), therefore rendering the right of information in these cases non-exercisable or effectively useless.

As mentioned before one of the problems in this process is that it's not possible for the data subject to verify whether the given information is complete or not. Therefore this would be the job of the national DPA which in Austria unfortunately is not able to fulfil this role for various reasons (see the legal analysis above for further details).

So the cases are most interesting where I presume certain data to be processed. In these cases it's rather disappointing if the expected data is not revealed (for example bank, credit card companies or CCTV data). The expectations are simple: to get all the information stored about my person; not only the data collected from me or other sources but also the data that has been calculated or otherwise produced from the original data. The experiences in this research show that these expectations might be too high. Data protection is still not a topic often discussed in society, and subject access requests are sent seldom. Therefore if a person has come this far and is sending a subject access request, the frustration might even be higher if simple and clear expectations are not met – be it because of formal/legal reasons or because the respective data controller is not able or not willing to answer the request correctly. This might also account for a certain disinterest in data protection or the feeling of helplessness, which again might get in the way of a loud and disgusted outcry in society after the Snowden revelations.

Further questions

In a first comparison of the different experiences in the involved countries, it looks like the obligatory "Datenschutzbeauftragter (person responsible for data protection matters in an organisation)" in Germany significantly helped in improving the responsiveness when it comes to subject access requests. If an organisation has to name a person responsible for these issues, the topic gets more awareness with this organisation, and respective processes are handled more seriously.

A question for further research would be to compare the resources of different DPAs across Europe and see whether an interdisciplinary composed staff, more financial resources and/or different implementations of the Directive improve the overall strict observation of data protection regulations within the EU.

Public vs Private

Generally speaking, more public authorities provided correct and complete answers within legal time limits than private companies. They seem to know what their duties are and have

an internal process set up for answering the requests. Interestingly, only public authorities insisted on a letter sent by postal service, signed by me, before answering my request. Not all of them had the chance to accept an e-mail because two of them received a letter from me as the first contact. But it can be observed that public authorities are maybe sticking a little bit more to the letter of the law, or maybe are less flexible in their responses compared to private companies.

Private companies are more straightforward in their handling of the requests – if they handle them in the first place. While no public authority completely ignored my requests, this happened quite often in the private sector. Indeed, even if the representatives of public authorities might not be particularly friendly in all cases, they are usually correct and they don't try to avoid sending the answer by treating the customer in an unfriendly way.

Interestingly it seems most of the respondents, public or private, don't deal with requests like this in the way they would handle any other customer requests: in the way that satisfies the customer and is in compliance with the law. The variety of answers is bigger in the private sector insofar as this sector presents one of the best and the worst answers at both extremes of the continuum.

It seems that all public CCTV systems store the data for only 48 hours. On one hand it's good to know that they are not keeping the footage forever, but on the other hand as long as they insist on a letter sent by postal service as the only way of submitting an access request, a citizen never has a chance to see the video footage depicting him/her because the postal service (or the internal delivery to the legal department) is not fast enough. This also means that there is de facto no control about the usage of the CCTV systems because the only other control mechanism would be the work of the DPA, and they admit themselves that they don't have the resources to actively control other companies or authorities. (See the legal analysis for details.)

General remarks on access rights

In my opinion the right to information is one of the better weapons against mass surveillance. Especially now, after the Snowden revelations and all the publicity the topic gets, it is evident that many companies don't care about potential infringements upon citizens' privacy. Transparency would help in the struggle to maintain, or better regain, one's informational self-determination. But this transparency is often denied, be it by denying the right itself, or by sending incomplete answers, often in a tone that seems to intend fending off querulous persons.

A prominent problem, which is also the reason for a slight bias towards the surveyor, is the fact that one can never know who is storing what about her/him. This means that the data subject is not able to verify whether the information disclosed is complete or not.

But without a functioning right to information, the balance of power between surveyors and surveilled is even more shifted to the surveyor. Unfortunately democratic societies need this balance, the control, and they need privacy for their citizens, otherwise a democracy is not working. That's why these rights are protected. In practice it can be observed that these fundamental rights are easily denied and ignored – without any consequences for the offenders.

SIGNIFICANCE OF FINDINGS - AUSTRIA

When dealing with the topics of privacy and data protection, one often gets the feeling that this is somewhat abstract and hard to understand for a lot of people. But it is nevertheless important for the functioning of our democratic political system, therefore all the regulations and protected fundamental rights.

One also often has the feeling that a lot of companies don't care about data protection, not even about compliance with the law in this respect. This research shows, unfortunately, that the impressions have been right. A lot of companies don't care and when you talk to people, employees, about your right to access information they often don't have a clue.

It might be no coincidence that one of the best practice examples in the research has been a company based in Germany where obligatory data protection officials may have helped to raise awareness for data protection.

One of the worst performances in answering a subject access request is a big company: Nokia. The strategy of complete ignorance and fending off their own customers can only work for them, if almost no one is interested in sending such requests and the data protection legislation or at least its enforcement is a completely toothless paper tiger.

Another finding of the work in this research is that Austrian public authorities are much better in answering subject access requests than public opinion might guess. All of them answered, in time, in a complete manner and mostly correctly. In some cases there is still room for improvement, but their responses were generally satisfying – from a compliance point of view. Nevertheless, some responses, especially those regarding CCTV footage, have been quite disappointing. It seems that it is not possible to get CCTV footage in Austria. And although this is on the one hand good news because the reason is that the images are not stored for very long, on the other hand it constitutes a problem when it comes to "watching the watchmen" and identifying a surveilled area. This emphasizes the already big gap in power between the surveiller and the surveilled.

Another problem is that the ordinary citizen is not able to guess who has data stored about him and to control whether a given answer on a subject access request is complete or not. To help him in this struggle the data protection authorities should be able to play a much more active role. In Austria this is a problem. The permanent underfunding of the Austrian DPA gives the impression that the government wants to dry out the agency since it might become nasty if they could start to work like they should.

On a European level it would definitely be necessary to coordinate the efforts for better data protection in a more efficient way and to put this topic on the agenda of the European Commission. In the current setting, the Commission is the one that has the power to deal with large, multinational companies. When it comes to forcing Google, Facebook and others to obey the data protection regulation in Europe, national DPAs are overburdened because of missing resources and their limited jurisdiction within the national borders. If Europe is not taking a more aggressive stance in defending its citizens' data, the bargain sale might go on, which would in the end destroy the trust citizens have in the functioning of democracy and the rule of law.

References

Arge Daten (2000-2013), Website: http://www.argedaten.at (last accessed 24 July 2013).

Austrian Broadcasting Company Online Portal (2013): Private Videoüberwachung im Vormarsch; http://wien.orf.at/news/stories/2581260/ (last accessed 25 July2013).

Austrian Chancellor (1999): Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung DSAV), Bgbl. II Nr. 521/1999, as amended on June 12th, 2013, last Amendment Bgbl. II Nr. 150/2013; http://www.dsk.gv.at/DocView.axd?CobId=30701 (last accessed 23 July 2013).

Austrian Chancellor (2004): Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004), Bgbl. II Nr. 312/2004, as amended on July 23rd, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495 (last accessed 23 July 2013).

Austrian Chancellor (2010): Verordnung des Bundeskanzlers, mit der die Standard- und Muster-Verordnung 2004 – StMV 2004 geändert wird (Novelle zur StMV 2004), Bgbl. II Nr. 152/2010, http://www.dsk.gv.at/DocView.axd?CobId=39692 (last accessed 25 July 2013).

Austrian Chancellor (2012): Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2012 – DVRV 2012), Bgbl. II Nr. 257/2012; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007925 (last accessed 23 July 2013).

Austrian Data Protection Commission (2008): Bescheid (verdict), Geschäftszahl K121.385/0007-DSK/2008.

Austrian Data Protection Commission (2009-2010): Das Recht auf Auskunft, http://www.dsk.gv.at/site/7434/default.aspx (last accessed 24 July 2013).

Austrian Data Protection Commission (2012): Datenschutzbericht 2010/2011, http://www.dsk.gv.at/DocView.axd?CobId=47839 (last accessed 23 July 2013).

Austrian Higher Administrative Court (2013), Zl.2010/17/0186-6, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20100730_K121605_0014_DSK_2010_00 (last accessed Feb. 20th, 2014)

Austrian Parliament (1964): Bundesverfassungsgesetz vom 4. März 1964, mit dem Bestimmungen des Bundes-Verfassungsgesetzes in der Fassung von 1929 über Staatsverträge abgeändert und ergänzt werden, Bgbl. Nr. 59/1964, as amended on July 23rd, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000391 (last accessed 23 July 2013).

Austrian Parliament (1978): Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG), Bgbl. 565/1978,

http://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf (last accessed 23 July 2013).

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

Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended on November 6th, 2013; Unofficial English translation: http://www.dsk.gv.at/DocView.axd?CobId=41936 (last accessed on November 6th, 2013)

Austrian Parliament (1999): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Bgbl. I Nr. 165/1999, as amended by Feb. 20th, 2014

Austrian Parliament (2001): Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG), Bgbl. I Nr. 152/2001, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001703 (last accessed 26 July 2013).

Austrian Parliament (2004): Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), Bgbl. I Nr. 10/2004, as amended on July 24th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230 (last accessed 24 July 2013).

Austrian Parliament (2007): Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007 – WAG 2007), Bgbl. I Nr. 60/2007, as amended on July 26th, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005401 (last accessed 26 July 2013).

Austrian Parliament (2009): Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010), Bgbl. I Nr. 133/2009, http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2009_I_133 (last accessed 23 July 2013).

Austrian Parliament (2013): Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2013), Bgbl. I Nr.57/2013, http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2013_I_57 (last accessed 23 July 2013).

Bundesministerium für Inneres/Österreichische Datenschutzkommission: Merkblatt zu den Rechten der Betroffenen bezüglich Europol (Information sheet on concerned persons‘ rights regarding Europol): http://www.dsk.gv.at/DocView.axd?CobId=30587 (last accessed on November 6th, 2013)

Bundesrat (in terms of the Austrian Constitutional Law from 1920) (1930): Bundes-Verfassungsgesetz (B-VG), Bgbl. Nr. 1/1930, as amended on July 23rd, 2013; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000138 (last accessed 23 July 2013).

European Commission (2011): Press Release: Mortgages: better protection for European consumers; http://europa.eu/rapid/press-release_IP-11-383_en.htm?locale=en (last accessed: July 24th, 2013), giving information on: European Commission (2011): Commission adoption of a proposal for a Directive of the European Parliament and of the Council on credit agreements relating to residential property, COM(2011)142, http://ec.europa.eu/internal_market/finservices-retail/credit/mortgage/index_en.htm (last accessed 24 July 2013).

European Parliament and the Council of Europe (1995): Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last accessed 23 July 2013).

Grand Chamber of the European Court of Justice (2012): Judgement of the Court in Case C-614/10; http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=359958 (last accessed 24 July 2013).

Korff, Douwe (2002): EC Study on Implementation of Data Protection Directive 95/46/EC – Report on the Findings of the Study, http://ssrn.com/abstract=1287667.

KSV, Selbstauskunft bestellen (order a subject access request), http://www.ksv.at/KSV/1870/de/4privatpersonen/1selbstauskunft/index.html (last accessed 24 July 2013).

The Austrian Minister for Traffic Infrastructure, Innovation and Technology (2011), Datensicherheitsverordnung, BGBl. II Nr. 402/2011, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007596 (last accessed Feb. 21st, 2014)

The Council of Europe (1950): Convention for the Protection of Human Rights and Fundamental Freedoms, as amended on Protocol 14, in force by June 1st, 2010; http://www.echr.coe.int/Documents/Convention_ENG.pdf (last accessed 23 July 2013).

List of Abbreviations

ABGB - Allgemeines Bürgerliches Gesetzbuch

AG - Aktiengesellschaft

ANPR - Automatic numberplate recognition

Arge - Arbeitsgemeinschaft

Art. - Article

Bgbl. - Bundesgesetzblatt

BK - Bundeskriminalamt

bPk - berechsspezifisches Personenkennzeichen

B-VG - Bundesverfassungsgesetz

BVT - Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

CCTV - Closed circuit television

CRM - Customer relationship management

DP - Data protection

DPA - Data protection agency

DPO - Data protection officer

DSAV - Datenschutzangemessenheitsverordnung

DSB - Datenschutzbehörde

DSG - Datenschutzgesetz

DSK - Datenschutzkommission

DSVO - Datensicherheitsverordnung

DVD - Digital Versatile Disc

DVR - Datenverarbeitungsregister

DVRV - Datenverarbeitungsregisterverordnung

EC - European Commission

ECG - E-Commerce-Gesetz

e.g. - exempli gratia

E-GovG - E-Government-Gesetz

eID - electronic identification

ELGA - Elektronische Gesundheitsakte

EU - European Union/Europäische Union

Ff - folgende

GmbH - Gesellschaft mit beschränkter Haftung

HR - Human resources

ID - Identification

iVm - in Verbindung mit

JGS - Justizgesetzsammlung

KSV - Kreditschutzverband 1870

MeldeG - Meldegesetz

MPEG - Moving Pictures Expert Group

NGO - Non-governmental organisation

N.SIS - National Schengen Information System

PIN - Persönliche Identifikationsnummer/Personal identification number

PDF - Portable document format

SA - Standardanwendung

SIRENE - Supplementary Information Request at the National Entry

SIS II - Schengen Information System II

StMV - Standard- und Muster-Verordnung

sub-para - sub-paragraph

Telco - Telecommunication company

TKG - Telekommunikationsgesetz

VersVG - Versicherungsvertragsgesetz

WAG - Wertpapieraufsichtsgesetz

Zl. - Zahl

ZMR - Zentrales Melderegister