Chapter 7
Exercising Access Rights in Hungary

Ivan Szekely and Beatrix Vissy

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

7.1 Mapping the Legal and Administrative Frameworks of Access Rights in Hungary

7.1.1 Introduction

A legal analysis of access rights in Hungary cannot start without considering the general data protection framework in which access rights are inscribed. Similarly, one cannot underestimate the importance of informational rights in Hungary, following the repeal of the Soviet type regime (Szekely 2008). The main characteristics of the Hungarian data protection system (Szabo and Szekely 2005) are: the following of the German model of informational self-determination; the interconnected concept of data protection and freedom of information which is reflected both in the legislation (the same act regulates the protection of personal data and access to data of public interest) and the institutional protection (the data protection authority is in charge of protecting both rights); the fundamental logic of constitutional law; the general law/sectoral law model; and the high penetration of sectoral

I. Szekely (✉)
OSA Archivum, Budapest, Hungary
e-mail: Szekelyi@ceu.edu

B. Vissy
ELTE University, Budapest, Hungary
e-mail: vissyb@alkotmanyjog.hu

C. Norris et al. (eds.), *The Unaccountable State of Surveillance*, Law, Governance and Technology Series 34, DOI 10.1007/978-3-319-47573-8_7

and area-specific legal regulation into various branches of the legal system. One of the most important elements of the data protection regime was the institution of the Parliamentary Commissioner for Data Protection and Freedom of Information, which had been working successfully during most of the period after the political transition, until its closure in 2011.

It should be noted that the present political regime, which has been in power since 2010, introduced significant changes to this legal and administrative system (Halmai and Scheppele 2012). Among others, it replaced the Constitution and the combined data protection and freedom of information law of 1992 with new laws; restricted the mandate of the Constitutional Court; closed down the institution of the Parliamentary Commissioner for Data Protection and Freedom of Information and replaced it with a lower legitimation government authority (this was one of the reasons why the European Commission launched an accelerated infringement proceedings against Hungary in January 2012, inter alia, due to the violation of independence of its data protection authority, and the premature termination of the term of the Commissioner in office. See European Commission (2012)); and limited the rights of data subjects in the interest of the data controllers in several detailed legal provisions. Nevertheless, the fundamental framework of the system remained unchanged.

The Hungarian law on data protection follows the model of combining general and sector-specific regulation. The key principles and guarantees of data protection, including the conditions of legitimate limitation to the right to informational self-determination are laid down in a general act, the Act No. CXII of 2011 on the right to informational self-determination and freedom of information (hereinafter: "Data Protection Act"). This Act contains general provisions on the request, collection, handling and transfer of personal data, and sets out legal remedies available to individuals to address violations of their right to protection of personal data. Explicit authorizations for, and specific provisions (additional guarantees or specific limitations) on, data processing of various types of data can be found in sector-specific acts.

The right to the protection of one's personal data enjoys extensive protection in Hungary since the application and interpretation of data protection rules are determined by the concept of informational self-determination – a right that was originally developed by the German Constitutional Court in the famous census decision of 1983 (see the German chapter in this collection). This principle was outlined in a landmark decision of the Constitutional Court in 1991, in which the court declared that the unlimited use of the universal personal identification number was in conflict with the individuals' right to self-determination and implied a direct and significant restriction on the fundamental right protecting personal data. In this decision the court established the constitutional framework for drafting of the legislation on data protection that was already in progress at the time of adopting the decision. The principle of informational self-determination forms the basis of the provisions for making the data processing legitimate under Hungarian law. According to this concept, everyone has the right to decide about the disclosure and use of his/her per-

sonal data.[1] In exceptional cases, personal data may also be processed if required by law (an Act of Parliament or a Decree of a local government).[2] However, since mandatory processing of personal data results in limitations of the right to informational self-determination, it is constitutional only if it is in accordance with the general conditions of the restriction of fundamental rights, i.e. if it stands the test of necessity and proportionality specified in the Fundamental Law.[3]

7.1.2 Legislation and Case Law on Access Rights

Legislation

It is easy to comprehend that without granting the right to data subjects of access to their data, the constitutional idea of informational self-determination would become a mockery. This was confirmed by the decision of the Hungarian Constitutional Court on the unconstitutionality of the universal personal identification number quoted above, when the court held that the right of access to personal data is the precondition of, and thus, the most essential guarantee for exercising the right to informational self-determination.[4] In the given case, when reviewing the constitutionality of the regulation concerning the population register, the court deemed unconstitutional that the law did not provide for data subjects the possibility to know and follow the route and circumstances of the use of their personal data stored in the population register. It was because the law lacked the obligation to officially document the process of personal data of data subjects, i.e. to record whose data were supplied to whom, when and for what purpose. In contrast to this, the court pointed out that the right to informational self-determination relies on the active participation of the data subjects. That is the point that distinguishes this right from other fundamental freedoms: "The Constitutional Court does not interpret the right to the protection of personal data as a traditional protective right, but as an informational self-determination right, with regard to the active aspect of this right."[5] This is what led the court to conclude that the data subjects have to be ensured the opportunity to monitor the route of their data during the processing and to enforce their rights.

In compliance with the constitutional requirements articulated by the Constitutional Court, under the Data Protection Act, individuals are granted by law

[1] Section 5 a) of Data Protection Act.

[2] Section 5 b) of Data Protection Act.

[3] Cf. Decision No. 15/1991 (IV. 13.) AB. Art. I (3) of the Fundamental Law stipulates: "A fundamental right may be restricted to allow the exercise of another fundamental right or to defend any constitutional value to the extent absolutely necessary, in proportion to the desired goal and in respect of the essential content of such fundamental right".

[4] Decision No. 15/1991 (IV. 13.) AB.

[5] Decision No. 15/1991 (IV. 13.) AB.

the right to access their personal data and, where necessary, to request its correction or even deletion. More precisely, the data subject may request from the data controller (a) information on his/her personal data being processed, (b) the correction of his/her personal data, and, except in the case of compulsory data processing, (c) the erasure or blocking the use of his/her personal data.[6] The data subject also has the right to object to the processing of data relating to him/her.[7] The legal right to inspect the Data Protection Register can also be qualified as a data subject right.[8] Besides the Data Protection Act, the vast majority of sector-specific acts contain rules on subject access rights. These acts often repeat the relevant provisions of the Data Protection Act but several of them contain specific provisions establishing special limitations on data subject rights and/or provide further guarantees for their enforcement. Such provisions can be found, for instance, in the separate sector-specific acts on processing of personal data: the Population Register Act,[9] the Personal Identifiers Act,[10] the Medical Data Act,[11] the Direct Marketing Act,[12] and in the specific provisions relating to data processing, of other acts: the Police Act,[13] the Health Act,[14] the Security Services Act,[15] the Electronic Communication Act[16] etc.

Under the general Data Protection Act, the data controller shall provide information upon the data subject's request about the sources from where personal data were obtained, the purpose, legal grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and – if the personal data of the data subject is made available to others – the legal basis and the recipients.[17] With a view to verifying legitimacy of data transfer and for the information of the data subject, the data controller shall maintain a transmission log, showing the date of time of transmission, the legal basis of transmission and the recipient, description of the personal data transmitted, and other information prescribed by the relevant legislation on data processing.[18] Data controllers must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within no

[6] Section 14 of Data Protection Act.

[7] Section 21 of Data Protection Act.

[8] Section 65 (4) of Data Protection Act.

[9] Act No. LXVI of 1992 on the Register of Personal Data and Addresses of Citizens.

[10] Act No. XX of 1996 on the Identification Codes and Methods Superseding the Personal Identification Number.

[11] Act No. XLVII of 1997 on the Handling and Protection of Medical and Related Data.

[12] Act No. CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing.

[13] Section 91/B of the Act No. XXXIV of 1994 on the Police.

[14] Section 24 of the Act. No. CLIV of 1997 on Health.

[15] Sections 29-32 of the Act No. CXXXIII. of 2005 on Security Services and Private Investigators.

[16] Sections 154-156 of the Act No. C of 2003 on Electronic Communications.

[17] Section 15 (1) of Data Protection Act of 2011.

[18] Section 15 (2) of Data Protection Act.

more than 30 days.[19] The information shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. The amount of such charge may be fixed in an agreement between the parties. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.[20] Where personal data is deemed inaccurate, and the correct personal data is at the controller's disposal, the data controller shall rectify the personal data in question if so requested by the data subject.[21]

Personal data shall be blocked instead of erasing if so requested by the data subject, or if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose which prevented their erasure.[22] Upon the request of the data subject, personal data should be erased, save where processing is rendered mandatory. Erasure is also needed where personal data are incomplete or inaccurate and it cannot be lawfully rectified.[23] When a piece of personal data is rectified, blocked, or erased, the data subject and all recipients to whom it was transmitted for processing shall be notified. Notification is not required if it does not violate the rightful interest of the data subject in light of the purpose of processing.[24] If the data controller refuses to comply with the data subject's request for rectification, blocking or erasure, the factual or legal reasons on which the decision for refusing the request is based shall be communicated in writing within 30 days of receipt of the request.[25]

In case of violation of subject's rights, namely when information, rectification, blocking or erasure is refused, the data subject may take the data controller to court or to the National Data Protection Authority (NDPA).[26] The data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the NDPA.[27] The judicial proceeding is endorsed by special guarantees aimed at supporting the legal position of the data subject. The burden of proof to show compliance with the law is reversed in such a suit: the data controller has to prove that data processing was lawful.[28] Moreover, the NDPA may intervene in the action on the data subject's behalf.[29] A data controller has to pay damages to compensate for the damage caused by unlawful data processing. That obligation is only cancelled in case of force majeure.[30]

[19] Section 14 (4) of Data Protection Act.
[20] Section 14 (5) of Data Protection Act.
[21] Section 17 (1) of Data Protection Act.
[22] Section 17 (4) of Data Protection Act.
[23] Section 17 (2) of Data Protection Act.
[24] Section 18 (1) of Data Protection Act.
[25] Section 18 (2) of Data Protection Act.
[26] Section 22 (1) of Data Protection Act.
[27] Section 18 (2) of Data Protection Act.
[28] Section 22 (2) of Data Protection Act.
[29] Section 22 (4) of Data Protection Act.
[30] Section 23 of Data Protection Act.

In its landmark decision in 1991 the Constitutional Court made clear from the outset that the data subjects' rights can be subject to legislative restrictions. Hence, where limitations on the right to informational self-determination are justifiable, personal data may be processed and transmitted even without the knowledge of the data subject. However, since such a restriction seriously jeopardises the controllability of data processing, it is constitutional only if the legislator provides adequate guarantees for keeping the data processing within objective (controllable) limits.[31] The lack of such guarantees led the Constitutional Court to abolish those provisions of the Police Act that allowed the police as data controller to withhold information from the data subjects on personal data relating to investigation in certain types of crimes listed in the Police Act. The Constitutional Court stated on the one hand, that the protection of state security, crime prevention or the rights of private persons could make it necessary to prohibit providing information to data subjects on certain data processed by the police. In the given case, however, the court concluded that because of the vagueness of the legislation, it could not be defined or delimited precisely on the basis of the challenged provision, in which cases data cannot be accessible on the data subject's request. According to the decision, when restricting fundamental rights, here the right to informational self-determination, such legal uncertainty is not permissible.[32] Following the guidance of the Constitutional Court the Parliament amended the relevant rules of the Police Act, and provided more explicit description of the cases in which access requests to personal data may be refused.

Under the Data Protection Act, anyone is entitled to inspect the Data Protection Register maintained by the NDPA which includes also the right to take notes on the official records on data processing details.[33] For the purpose of providing satisfactory assistance to data subjects, the register contains a wide range of information: the name and address of the data controllers and data processors, the place where records are kept and/or where processing is carried out, the legal basis and the purpose of the data processing, the scope of data subjects, a description of the data pertaining to data subjects, the duration of the processing, the categories of data transferred, the recipients and the grounds for transfer (including transfers made to third countries), the nature of the data processing technology used, and, where applicable, the name of and contact details of the internal data protection officer.[34] The Act sets out that apart from mandatory processing, data processing may not commence prior to registration.[35] It should be noted that the initial text of the new Data Protection Act promulgated on 15 July 2011 would have ensured wider access to the register to the general public by obliging the authority to publish the register

[31] Decisions No. 24/1998 (VI. 9.) AB and No. 44/2004 (XI. 23.) AB.

[32] Decision No. 44/2004. (XI. 23.) AB. The English summary of the decision is available here: http://www.codices.coe.int/NXT/gateway.dll/CODICES/precis/eng/eur/hun/hun-2004-3-008?fn=document-frameset.htm$f=templates$3.0 (last accessed 17 September 2014).

[33] Section 65 (4) of Data Protection Act.

[34] Section 65 (1) of Data Protection Act.

[35] Section 66 (1) of Data Protection Act.

on its website.[36] For unknown reasons, however, the Parliament amended the relevant provisions of the Act and eliminated the NDPA's legal obligation to publish the register on the Internet.[37]

Case Law

Insofar as can be established from open sources,[38] individual cases aimed explicitly at enforcing subject access rights occur only sporadically in Hungary. In a recent lawsuit concerning subject access rights, the complainant lodged a complaint with the NDPA against an insurance company alleging that the company (data processor) refused his request to access the medical expert opinion regarding his claim for compensation following his injury in a traffic accident (NDPA 2012a). The complainant had submitted his request three times before initiating the authority's procedure. The insurance company held that the medical expert opinion was an in-house document. Since the company was reluctant to provide access to the documentation, the NDPA imposed a fine of 500.000 HUF (approx. 1.600 euro) to the data controller because of the breach of the Data Protection Act. When determining the amount of the fine, the NDPA paid special attention to the facts that the insurance company violated a subject access right, i.e. the right to be informed of personal data, and that the data concerned are special data which enjoys special protection. The authority's decision also emphasized that an insurance company, which processes a wide range of personal data, is expected to take special care to respect subject access rights (NDPA 2012a). The insurance company lodged an appeal against the decision of the NDPA with the Metropolitan Court against the decision but the court upheld the authority's decision.[39]

In a case of 2002, a citizen was shocked to find, while shopping at a telecommunication store in the town of Godollo, that someone had already purchased a mobile phone set in his name. The customer was curious to know who had used his

[36] Section 65 (4) of the Act. No. CXII of 2011 on the Right to Informational Self-determination and on the Freedom of Expression as published in the Official Gazette 88 (2011) on 26.07.2011 stipulated: „The Data Protection Register is open to the general public, it shall be made accessible to anyone on the webpage of the NDPA."

[37] Section 411 (6) of the Act No CCI of 2011.

[38] In Hungary court decisions are themselves non-transparent, with judgments remaining virtually inaccessible. The most important available authentic source of court rulings is the Compendium of Court Decisions – an online database operated by the National Judicial Office. This database contains a significant amount and range of anonymized judgments that have reached the courts of appeal and/or the Curia (Supreme Court) and were released after January 2007. The database is available at http://www.birosag.hu/ugyfelkapcsolati-portal/anonim-hatarozatok-tara. For more details see Section 163–166 of the Act No. CLXI of 2011 on the Organisation and Administration of Courts. Available in English at: http://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2012)007-e (last accessed 17 September 2014) Summaries of potentially relevant court rulings can be found in the Annual Report of the Hungarian NDPA too, since the authority regularly publish a brief summary of the court cases adjudicating the lawfulness of the NDPA.

[39] Metropolitan Court 26.K.32.704/2012/5.

identity, and sought to find out his "previous phone number," but the service provider refused to give out the information citing reasons of data protection. Then, the customer submitted a complaint to the Parliamentary Commissioner for Data Protection and Freedom of Information. In his reply, the Commissioner informed the petitioner as follows: "Telecommunications data qualify as personal data. (…) The data controller is liable to provide information upon request about the individual's personal data in its control. In your case, this means that the provider must tell you which of your personal information it keeps in its records. You are entitled to a copy of the contract and to know the associated call number, because according to the provider's records you are the party to the contract. It will take a criminal investigation to try to identify the person who signed the contract in your name."[40] Further information on the case is not available however, the general conclusion of the case was that the Commissioner emphasized the absurd nature of the situation when a data controller denied the exercising of a data protection right on grounds of data protection, with respect to the same person.

As regards the restriction on subject access rights in the telecommunication sector, following several complaints over the years, the Commissioner had repeatedly stressed the prohibition of providers to deliver caller lists to their clients in order to abide data protection and confidentiality. His opinion has been codified into legal norms: a sectoral rule prohibits the sending of caller lists to clients.[41] Telecommunication service providers are liable for handling the data acquired in connection with operating the network confidentially, and may not give them out unless explicitly required by law to do so, only if the unwanted calls involve threats to life or bodily integrity, or blackmail. It is only in such cases that the investigative agency may act on the user's written request and access the content of calls received at the user's set, and to discover the identity of the caller – both within the time frame specified in the user's request. In the said cases, the law also provides for the option of intercepting, tapping and taping calls.[42] It should be noted however, that the detailed lists of calls *initiated* from the user's set can be obtained by the written request of the user, provided that the user undertakes all responsibility regarding the personal data of others whose data may be included in, or concluded from, the detailed list (typically: who might have used the user's set, and whom this person called from the user's set).

Research conducted in the Compendium of Court Decisions resulted in a finding that no precedent of cases in which a court forced data processors to pay compensation to the data subject as a consequence of committing violation of access rights. In

[40] Annual report of 2002 by the Parliamentary Commissioner for Data Protection and Freedom of Information.

[41] Section 157 (1) of Act C of 2003 on Electronic Communications.

[42] 1470/A/2006. Published on 25 October 2006. Available in Hungarian at http://abi.atlatszo.hu/index201.php?menu=allasfogl2006&dok=1470_A_2006 (last accessed 17 September 2014).

a lawsuit of 2010,[43] the plaintiff sued a hospital for compensation alleging that the hospital denied his request to gain access to the medical record prepared on him and to receive copies thereof. His legal action was based on the Health Act declaring that any patient shall have the right to become acquainted with the data contained in the medical record prepared on him or her, and shall have the right to request information on his or her health care data.[44] Although the court established the violation of access rights and also declared that without having knowledge of health care data, individuals cannot make responsible decisions regarding the way of their lives, it did not order compensation.[45]

Elsewhere, the operation of Google Street View in Hungary is a notable issue. One of the reasons why Google Street View started to operate in Hungary only in November 2012 was the lack of adequate guarantees for ensuring the rights of the data subject affected by the service. In May 2009, when Street View cars appeared on Budapest streets, the Parliamentary Commissioner for Data Protection and Freedom of Information launched an *ex officio* investigation in connection with the Street View service of Google in Hungary. The Commissioner expressed his concerns regarding the fact that Google failed to clarify, among other things, how the data subjects can exercise their rights. As a result, Google temporarily suspended recording images in Hungary. Two years later, the Commissioner published its final position on the operation of the Street View determining the conditions which should be adhered to by Google.[46] On 28 November 2012, the Budapest Metropolitan General Assembly passed a resolution in support of allowing Google to launch the service in Budapest,[47] with the proviso that Budapest may only be featured on Google Street View in compliance with the guidelines of the NDPA (2013a). Now anyone is able to report his/her concern to Google if he/she notices that Google does not provide enough protection for his/her or a third person's personal data (by, for instance, not blurring an image or a license plate).[48]

---

[43] 1470/A/2006. Published on 25 October 2006. Available in Hungarian at http://abi.atlatszo.hu/index201.php?menu=allasfogl2006&dok=1470_A_2006 (last accessed 17 September 2014).

[44] Section 24 (3) of Act No. CLIV of 1997 on Health.

[45] Fovarosi Torvenyszek P.25905/2010/26. It should also be noted that, according to the decision of the court, the period of limitation for claims had already expired at the time of starting the court procedure.

[46] ABI-2136-3/2010/K. Published on 16 May 2011. Available in Hungarian at http://abi.atlatszo.hu/index.php?menu=aktualis/allasfoglalasok/2011&dok=ABI-2136-3_2010_K (last accessed 17 September 2014).

[47] Resolution No. 2643/2012 (11.28.) of the Metropolitan Assembly.

[48] It can be ascertained that the reporting function of Google Street View is operating satisfactorily. To test the reporting system of Google we submitted a report on 25 July 2013 at 10:17 a.m., complaining that a license plate in the 11th district of Budapest (Hungary) had not been blurred. Our complaint was answered by Google on the same day at 10:23 a.m. In its response Google informed us that it had already taken the necessary measures to handle our privacy concern, and indeed, it had.

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

The Hungarian Data Protection Act implements the provisions of the European Data Protection Directive 95/46/EC at national level. However, a few remarks in this regard need to be made. According to the Directive, the rights of data subjects may be restricted by law in order to safeguard the external and internal security of the State, such as defence, national security, the prevention and prosecution of criminal offences, the safety of penal institutions, to protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in regulated professions, prevent and detect breaches of obligation related to labour law and occupational safety – including in all cases control and supervision – and to protect data subjects or the rights and freedoms of others.[49] Consequently, the data controller may refuse to provide information for the data subject or to comply a data subject's request to correct, erasure or delete his/her personal data being processed in these cases if covered by a provision of national legislation.

Exceptions to the general provisions of the Directive, and to the general provisions of the Hungarian data protection act, can be found in the Data Protection Act itself and, on grounds of authorization by the Data Protection Act, in several sector-specific legal provisions containing detailed rules of processing of personal data. For example, in the data protection register – the obligatory content of which and the range of data controllers who are obliged to register their data processing operations in the register, are enlisted in the Data Protection Act – national security agencies indicate only the name and address of the given national security agency, and the purpose of and legal basis for data processing.[50] Should a request for information be denied, the data controller shall inform the data subject in writing on the legal grounds for refusal. According to the National Security Services Act, the Head of the Services may refuse the data subject's request for access to his or her personal data processed by the Services, on grounds of national security or in order to protect the rights of others.[51] The Money Laundering Act provides that the reporting persons and the authority operating as the financial intelligence unit shall not provide information to the customer concerned or to other third persons on the fact that information about the customer has been transmitted, on the contents of such information, or on whether a money laundering or terrorist financing investigation is being or may be carried out on the customer.[52] In addition, once a year, data

[49] Section 19 (4) of Data Protection Act.

[50] Section 65 (2) of Data Protection Act.

[51] Section 48 (1) of Act No. CXXV of 1995 on the National Security Services.

[52] Section 27 (1) of Act No. CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing.

controllers shall notify the NDPA on the annual information regarding refused requests, by 31 January of the following year.[53]

The NDPA, in connection with the new draft Data Protection Regulation of the EU has put forward a suggestion for harmonizing the right of access to one's own personal data at EU level. The authority suggested that instead of the present system whereby the data protection Directive and the national laws define general exemption categories, the new system should prescribe an obligation for data controllers to conduct case-by-case consideration, thus necessitating the performing of the necessity and proportionality test in each case of denial of access (NPDA 2012a: 35).

7.1.4 Surveillance and Access Rights: Codes of Practice and Access to CCTV Footage

In Hungary, there are no codes of practice at national level concerning a sector or a specific technology of surveillance, nor codes concerning the guarantees of subject access rights (such as the Draft subject access code of practice of the Information Commissioner's Office, UK). In the Codes of Conduct or Codes of Ethics of some professional associations representing organizations of the private sector provisions can be found on the processing of personal data, including general provisions on subject access. A few examples of the use of these codes are illustrated as follows.

Among public sector organizations, the most relevant authority in the area of processing of personal data is the data protection supervisory authority. As noted elsewhere, the term of the Parliamentary Commissioner for Data Protection and Freedom of Information in office was prematurely terminated and the institution closed down, and replaced by a government authority, the *Hungarian National Authority for Data Protection and Freedom of Information*. The commissioners had built up a corpus of quasi case law during the 17 years of operation of the institution which included recommendations, positions and publications. Indeed, the first Commissioner published extensively his recommendations and other relevant documents relating to the institution in English.[54] Among these instruments several documents contain recommendations or positions involving issues of subject access, including cases of security camera recordings. In August 2012 the new supervisory authority issued a recommendation on the basic criteria of operating electronic

[53] Section 16 (3) of Data Protection Act.

[54] See the series "Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information" published in printed format; the annual reports were also accessible on the Commissioner's website. After the closure of the office and its website, an activist organization fighting for public transparency, "Atlatszo.hu" managed to make the whole website of the Commissioner available on its own website, and later the new government authority also made the content of the Commissioner's website available online again.

monitoring systems at the workplace (NPDA 2013b). However, the rules of subject access are not discussed in the recommendation.

In theory, another autonomous authority, the *Hungarian Financial Supervisory Authority* (PSZAF), which has recently merged into the Central Bank of Hungary, may also react with enforcement actions to violations of subject access rights since banks, insurance companies and other financial organizations, which have individual clients, are obliged by detailed legal regulations concerning the processing of their clients' data.

According to the provisions of the data protection act, authorities of nation-wide jurisdiction, and data controllers and processors engaged in processing data files of employment and criminal records, as well as financial institutions and providers of electronic communications and public utility services, are obliged to appoint an internal data protection officer and draw up an internal data protection regulation. These regulations are internal and therefore not accessible to the public. However they regulate the internal system of responsibilities and procedures regarding the processing of personal data, including the ways of enforcing data subjects' rights – among others, their right to access their own personal data.

In Hungary there is no national code of practice on the use of CCTV cameras, nor a separate act regulating the operation of such devices. However, important legal provisions can be found in the Security Services Act[55] and the Condominium Act.[56] The Security Services Act applies to private security services, the design and installation of security systems, and private investigation services – in other words, to outsourced security activities.[57] Security guards are authorized to make and process sound and/or video recordings (that is, CCTV recordings) through an electronic surveillance system, "in due observation of the provisions of the Data Protection Act", however, only on private property, including the sections of a private property that is open to the general public. The legal ground of data processing is the express consent of the data subjects. Legally speaking, consent can also be given through conduct that implies acceptance, that is, if the person, despite the warning, enters the premises.[58] Such surveillance systems may not be used in a place where surveillance is likely to violate human dignity (dressing rooms, toilets, hospital wards etc.).[59] As a general rule, the recordings, if unused for court proceeding or some other official proceedings, shall be deleted within three working days from the day when recorded, within 30 days if the recording was made at public events, and within 60 days if the recording was made for the purposes of providers of financial and related services.[60] The provisions of the act do not specify how data subjects (the identifiable persons on the recordings) may exercise their access rights.

[55] Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators.

[56] Act CXXXIII of 2003 on Condominiums.

[57] Section 1 (1) of Security Services Act.

[58] Section 30 (2) of Security Services Act.

[59] Section 30 (2) of Security Services Act.

[60] Section 31 (2)-(4) of Security Services Act.

In the absence of national codes of practice, it was the Parliamentary Commissioner for Data Protection and Freedom of Information who regularly issued recommendations and positions on the use of CCTV cameras. In the annual reports of the Commissioner, among the important sectoral data processing areas CCTV had been a recurring section, indicated as "Video Surveillance" (2002, 2003), "Surveillance Cameras" (2005) etc. (available via Atlatszo 2014a). In 2000 the Commissioner issued a recommendation on image recording devices in which he analyzed the most important criteria of operating such systems (this recommendation was issued before the enactment of the two acts mentioned above). Nevertheless, the Commissioner's recommendation did not specify the criteria of exercising subject access rights either.

In 2010 the last commissioner in office (in the last year before his dismissal and the closure of his institution) organized a conference on the International Data Protection Day (January 28) titled "Camera Surveillance in Hungary". Among the participants there were police officers, civil activists, representatives of private security services and the security industry (Dajko 2012). The new government authority, the NDPA recently issued two positions in surveillance-related cases: one on surveillance in a production company, and one on surveillance in condominiums (NDPA 2012b, c).

7.1.5 The Promotion of Access Rights by DPAs and National Authorities

The NDPA plays an important role in facilitating individuals to exercise their access rights. As pointed out above, the Data Protection Act assigns multiple tasks to the authority in this regard. Besides investigating individual complaints, the NDPA is responsible for maintaining the Data Protection Register which is essential to the localization of data controllers. Alongside this, the NDPA maintains another register, i.e. the register of refused access requests. As mentioned above, every data controller shall annually submit a report to the authority concerning the access requests it has refused. The annual reports of the NDPA regarding the last 2 years have failed to consider the operation of the register of refused requests. The annual reports of the former supervisory institution, the Parliamentary Commissioner for Data Protection and Freedom of Information, regularly published data about the register of refused access requests.[61]

The activity of the present NDPA cannot be characterized as pro-active and engaged in promoting awareness of subject access rights. The authority has not shown so far any noteworthy awareness-raising moves to improve the level of enforceability of these rights. Such movements have not been typical of the predecessor of the NDPA either. However, the Commissioner had been involved in some

[61] These documents were previously available online via an archive of publications by the Parliamentary Commissioner for Data Protection and Freedom of Information.

awareness-raising activities in this area. In 2002, for example, the Commissioner's Office held a series of open meetings across fourteen counties and published a so called "privacy column" in several county newspapers in order to call the attention of the private sector to the obligation of registering of companies in the Data Protection Register.[62] To help data subjects to localise and supervise the controllers of their personal data, the Commissioner used to publish a guide to support the understanding of the register's structure and content and data subjects were also able to search in the register. Moreover, the Commissioners had been making virtually every year a formal announcement in the Official Gazette to remind data controllers about the obligation to provide data on the refused subject access requests.

The Commissioner's Office regularly published leaflets on the rights of data subjects, and edited a book under the title *"Stories from Tukory Street"* (in Hungarian) in 1999 – that is, the street where the first building of the Commissioner's Office was located (Javorniczky and Majtenyi 1999). The book contained various short stories about how data protection rights can be enforced.

It is important to recall that in January 2012 the European Commission launched accelerated infringement proceedings against Hungary before the European Court of Justice, among others, over the independence of its data protection authorities.[63] This was a result of the abolishing of the institutions of the Parliamentary Commissioner for Data Protection and Freedom of Information and the dismissing of the Commissioner in office prematurely. The institution of the Parliamentary Commissioner has been replaced with a government authority, the complete independence of which – despite the wording of the act establishing the authority – raised serious doubts. The Commission declared that Hungary has failed to fulfil its obligations under the Directive 95/46/EC by removing the data protection supervisor from office before time. Hungary was called by the Commission to amend its law on data protection in order to ensure that the new Authority's legal status corresponds with the European standards. As a result of the infringement proceedings, minor changes were made in the provisions defining the mandate of the new authority. However, the independence of the new authority, which is embedded in the structure of a strongly centralized government, has remained questionable (Szigeti and Vissy 2012). Both the European Data Protection Supervisor, who was allowed to intervene in the court case in order to support the application of the European Commission, and the Advocate-General of the European Court of Justice have argued that Hungary had violated EU law by terminating the Commissioner's mandate before it was fulfilled, and in doing so, exerted indirect external influence on the Hungarian supervisory authority.[64] This was reflected in the Court's judgement delivered on 8 April 2014. In its decision the Court declared that Hungary had

[62] As above.

[63] *Commission v Hungary*, Case C-288/12.

[64] Court of Justice of the European Union (15 October 2013) EDPS pleading Commission v. Hungary, (C-288/12) available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2013/13-10-15_Pleading_EC-Hungary_EN.pdf, and European Commission, Opinion of the Advocate-General, C-288/12, Commission v. Hungary (last

broken the requirements for complete independence of national data protection authorities by prematurely bringing to an end the term served by the Commissioner elected by the Parliament. According to the Court's legal reasoning, complete independence, as set out by Directive 95/46/EC, implies that the decision-taking process of data protection supervisors must be free from political influence of any kind. Even the risk of such influence must be dispelled. Forcing a supervisory authority to vacate office before serving its full term might prompt the authority to enter into a form of prior compliance with political powers. That is why Hungary had not complied with the obligations under EU law.[65] The outcome of the procedure, however, has not resulted in any institutional change in Hungary. The only reaction of the government to the court decision was a short statement issued by the Minister of Justice, László Trócsányi, to express an apology on behalf of the government to András Jóri for the improper removal and to wish him good luck to his further professional work in the field of data protection (Ministry of Justice 2014).[66]

---

accessed 7 May 2014). See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62012CC0288:EN:NOT.

[65] Judgment of the Court (Grand Chamber) in Case 288/2012, 8 April 2014. Available in English at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30db5c525c037f084360b639f83f01c7e5b8.e34KaxiLc3qMb40Rch0SaxuNb3b0?text=&docid=150641&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=405374 (last accessed 17 September 2014).

[66] Following a roundtable discussion organized at the annual Computers, Privacy and Data Protection (CPDP) conference in Brussels in 2015, where researchers presented the empirical results of the international study in subject access rights upon which this edited collection is based to six national DPAs, the Hungarian DPA sent a written comment to the organizers. In his comments, the DPA criticized the observation in the Hungarian findings, according to which the independence of the Hungarian DPA is "questionable". Paradoxically, the DPA referred to the same decision of the ECJ which ruled that Hungary had failed to fulfil its obligations under EU law by prematurely bringing to an end the term served by the former supervisory authority, and which also established that the new authority "in essence, is entrusted with identical tasks" in comparison with the former institution (point 61 of the decision). Although this quotation and the other references enlisted in the DPA's comment (general references to the observations of the Venice Committee, the Schengen Evaluation Committee and the Commissioner for Human Rights of the Council of Europe), including the wording of the national data protection law, are correct, they fail to give a full picture of the position and margins of the new authority. A supervisory authority, which lost its parliamentary status and became embedded in the government, in particular in a country where the weakening of democratic checks and balances triggered repeated criticism and actions at various European institutions, cannot be regarded completely independent in terms of its relative independence from those organizations it supervises, according to the provisions of the data protection directive and the reasoning of the ECJ decision mentioned above.

Recent empirical studies supported this assumption: an investigation of the DPA's financial penalty policy in the period 2012–2014, conducted on the basis of the information published on the authority's homepage, revealed that the authority's official procedures ending with a decision concerned private data controllers much more often than data controllers associated with public authorities. Also, the DPA imposed significantly heavier penalties on private data controllers than on public authorities, in terms of individual fines, the sum total of the fines and the average figure alike (Szabo 2014); (Szabo and Hidvegi 2014). For more about the issue of independence of the Hungarian DPA see Szekely (2016).

7.1.6 Role of NGOs in Ensuring Access Rights

In newly democratic countries where there is a well-working official custodian of informational rights, the activity of civilian organizations is weak in these areas. Conversely, where official supervision is inefficient or nonexistent, NGOs will undertake the missing function of enforcement on their own (Szekely 2008: 195). This was certainly the case in Hungary where the wide recognition of the Parliamentary Commissioner for Data Protection and Freedom of Information (also called as the data protection ombudsman) allowed civilian organizations to shift their activism to other areas, such as environmental issues or gender discrimination. NGOs which included privacy issues in the range of their activities had developed an informal alliance with the Commissioner in cases where the Commissioner and the NGOs had to protect the rights of the citizens against excessive informational power.

In recent years, after the change of government in 2010, the strong legitimacy and independence of the supervisory agency dissolved, and civilian organizations have become much less willing to regard a government authority as their ally, especially in cases where the data controller is a government agency. Consequently, the role of civilian organizations has become more important, and their responsibility increased in cases relating to the enforcement of informational rights. The interest of these organizations towards informational rights have also increased, and although there is no NGO in Hungary specialized in helping citizens to enforce their right of access to their own personal data, and there is no NGO specialized in data protection alone, the impact of the few organizations dealing with data protection cases is not insignificant.

Two NGOs have to be mentioned here, one with a long history and one recently established. The older organization, which had existed even before the foundation of the institution of the Parliamentary Commissioner, is the *Hungarian Civil Liberties Union* (HCLU; its Hungarian acronym: TASZ). HCLU defines itself as a non-profit human rights watchdog and a law reform and legal defence public interest NGO, which is working independently of political parties, the state or any of its institutions. Its mission is to educate citizens about their basic human rights and freedoms, and to take stand against undue interference and misuse of power by those in positions of authority (Hungarian Civil Liberties Union 2014). The focus areas of HCLU's activities are: patient rights (including access to medical records), right to self-determination (abortion, euthanasia), right to information privacy, freedom of expression, right to political representation, drug policy, AIDS policy. HCLU runs a legal aid service in the above areas, which includes a telephone hotline 8 h a day, online counseling, and impact litigation.[67]

[67] Among these litigation cases, HCLU were involved in one concerning the public accessibility of CCTV cameras operated by the police in Budapest. This ended with success in 2007 when after two and a half years of litigations, the Supreme Court ordered the Budapest Police Headquarters to issue data on the CCTV systems operated by the police in Budapest. Locations, and all information regarding the operational, financial, technical, legal and personnel aspects, as well as informing of the public and monitoring of the data are now considered data of public interest and freely accessible on the internet.

The other organization, which was established in 2011 by a group of pro-transparency and anti-corruption journalists, lawyers, IT-specialists, academics and other independent experts, is called *Atlatszo.hu* (atlatszo means transparent in Hungarian), and operating in the form of an online portal. Atlatszo.hu focuses on sister areas of informational rights. It produces investigative reports, accepts information from whistleblowers, files freedom of information requests, and commences freedom of information lawsuits in cases where its requests are refused (Atlatszo.eu 2014b). Atlatszo.hu has won more than 60 % of the FOI lawsuits it initiated, and in some cases the fact of the court application was enough to obtain the public information in question and the case was dropped. The portal includes an online tool designed for average citizens to obtain information from government departments, agencies, and state owned companies. This service (KiMitTud) is modelled after the British WhatDoTheyKnow and is built on the same software application. It is a freedom of information request generator by the help of which compliance of the agency with legal provisions concerning the deadline and the content of the response can be publicly monitored. Historic requests, along with any resulting correspondence, are archived publicly online.

7.2 Section Two – Exercising Access Rights in Practice

7.2.1 Introduction

This part describes, analyses and summarises the experience gathered during our attempts to locate data controllers and, having done so, submit access requests to organisations. As part of this process, we attempted to locate data controllers in 31 organisations and subsequently submitted 19 subject access requests to a wide range of data controllers both in the public and private sector in Hungary and, in case of certain multinational companies, beyond its borders. Below a summary assessment of the findings is presented, followed by the detailed analysis of experiences with public sector organizations, private sector organizations – including multinational companies – and, as a specific category, CCTV operators. In the concluding section of this report the authors not only summarize their findings but also identify some possible outcomes of their research.

7.2.2 Locating Data Controllers

Before citizens can submit an access request, they must of course locate the organisation to whom a request should be sent. Within these organisations, citizens must identify the person or office nominated as the data controller whose responsibility it is to receive and response to subject access requests. We attempted to locate data controllers within 31 different organisations in total. All in all, we were able to locate data controllers at 29 sites by using three different methods: 16 of them were located online, 12 by phone, and 1 could be located by asking for details in person.

The three methods for localization were applied sequentially: first we tried to locate the data controller on the official websites of the concerned domains. We only asked for data controller details by phone if the online scrutiny was not successful. However, in those cases when we were advised by phone to go to the organization website (and there we found the necessary information) we concluded that the data controller was identified online. Visits in person proved to be necessary only for locating data controller details of CCTV operators and checking the CCTV signage. Emails were also sent to enquire about the identity of the data controller in cases when neither the online findings, nor the information provided by phone call or in person were satisfactory and when we were explicitly asked to do so.

The difficulties that we ran into when trying to access to data controller details basically emerged on two dimensions that can be distinguished: (1) *identifying the data controller* in charge of handling subject access requests, (2) *locating the data controller* online or by using other methods, in other words, finding information about the contact details and the privacy policy of the data controller in charge of responding subject access requests. In more detail:

(1) Identifying the data controllers at the sites of the private sector was relatively easy. The same cannot be said for the sites relating to the governmental sector. In the case of companies and organisations in the private sector (banks, insurance companies, ISPs, supermarkets, Google, Facebook etc.) it is basically self-evident or at least easy to identify who the data controller is and on which website to go on for more details about subject access rights. However, in the case of personal data held by governmental organisations (police records, driving licence records, border crossing records etc.) we assume that data subjects are likely get into difficulties while trying to identify the data controller *in charge* of handling individuals' subject access requests. This is because a single piece of personal data may be processed by more than one data controller, and without the knowledge of the relevant legal regulation individuals cannot be completely aware of the identity of all data controllers involved in the processing of their personal data. It is also not simple to find out how the different duties prescribed for data controllers are shared between the data controllers concerned (not to mention the complicated nexus between data controllers and data processors). In other words, compulsory data processing carried out in the public sphere is much less transparent as regards the identity of data controllers and their duties. To give an example, in Hungary, police and driving records are

controlled both by the Police and by the Central Office for Public Administrative and Electronic Public Services. It is not self-evident to citizens who one should submit subject access requests to. In the light if the above, one may argue that, data controllers should have a duty to make their organisational relationships transparent, for example by forwarding citizens' requests to the responsible data controller. Considering that lay citizens cannot be expected to oversee the complicated system of relationships among those participating in the processing of their personal data – cannot be overestimated either.

(2) The question of whether the data subject, after having located the data controller, can obtain adequate information on how she can exercise her rights in connection with the data processing, can be separated from the previous set of problems. Due to different reasons, some of the research sites had to be inspected more than once in order to access data controller details. In some cases we were thwarted in our first attempt to locate the data controller when the persons we got in touch with were not or not completely aware about data subjects' rights. Some of our first attempts failed because of the resistant attitude of the interlocutors. In these cases a "second round" of visits was conducted. It should be mentioned that a number of our attempts to find data controller details by accessing online content were actually unsuccessful at the first time. This was due to the fact that first we had to learn the respective data controllers' logic regarding where they post the information about data subjects' rights on their websites, and later we needed to return to those websites where previously we were unable to identify the data controller. For example, at the beginning of the research, we did not suppose that certain data controllers include (or rather hide) their privacy policy inside their general contractual provisions, thus we regarded these attempts as unsuccessful. Later, when we analyzed the general contractual provisions themselves, we found the missing information there. Nevertheless, we did not regard these trials as repeated attempts, since the analysis of the websites was much more of a continuous or parallel procedure than separate procedures (Table 7.1).

On the basis of our experience accumulated during the course of attempting to locate data controllers, we hypothesize that the ability to identify data controllers (similarly to the possibilities of subject access to the personal data processed by them) highly depends on the organizational culture of the data controller organizations. This can be experienced for example in the financial sector, where multinational commercial banks inherited different traditions from their mother institutions.

The localizability of data controllers also highly depends on the personal attitudes and knowledge of the contact person who receives telephone calls or personal visits from the data subjects. Although we had some positive experiences, too, the lack of information posted on the websites or at the sites operating CCTV cameras, on the identity of the data controller and on the possibilities of exercising data protection rights, makes inquirers subject to arbitrary administering of their requests,

Table 7.1 Summary of findings when attempting to locate data controller contact details

Data controller contact details successfully identified in first round of visits	24 of 31 cases (75 %)
Data controller contact details unable to identify in first round of visits	8 of 31 cases (25 %)
Total number of data controller contact details successfully identified after second round of visits	29 of 31 cases (93.75 %)
Total number of data controller contact details unable to identify after second round of visits	2 of 31 cases (6.25 %)
Contact details identified via online privacy policy	16 of 29 (successful) cases (55 %)
Contact details identified after speaking to member of staff on phone/via email	12 of 29 (successful) cases (41 %)
Contact details identified after speaking to member of staff in person	1 of 29 (successful) cases (3 %)
Average rating given to visibility of privacy content online	1/2 – Poor/Adequate
Average rating given to the quality of information given by online content	2 – Adequate
Average rating given to visibility and content of CCTV signage	1 – Poor
Average rating given to quality of information given by staff on the telephone	1/2 – Poor/Adequate
Average rating given to quality of information given by staff in person	1 – Poor

and the success of their inquiries dependent of the education and attitudes of the personnel at the data controller organization.

We found that lay data subjects experience a significant disadvantage over inquirers in possession of legal knowledge in the course of communicating with the data controller organization.

We did not find, however, any sign of proactive support of the new data protection supervisory authority[68] for helping citizens in their attempts to locate data controllers. On the contrary: the data protection registry maintained by the authority has lost its public accessibility through the internet since the establishment of the authority in January 2012 – hopefully only temporarily.[69]

[68] Hungarian National Authority for Data Protection and Freedom of Information (NAIH), the authority replacing the highly successful institution of the Parliamentary Commissioner for Data Protection and Freedom of Information in 2012, terminating the mandate of the Commissioner in office prematurely.

[69] We filed a freedom of information request to the NAIH to learn when the registry would be again accessible through the internet. In his response the deputy head of the authority informed us that the registry, according to the provisions of the data protection act, is public, however "at present the registry cannot be accessed through the website of the authority" (NAIH-1419-2/2013/H).

Table 7.2 List of addressees of subject access requests

	Site	Data controller
1	Public	CCTV in open street
2	Public	CCTV in a transport setting
3	Public	CCTV in a government building
4	Public	CCTV in a government building
5	Private	CCTV in a department store
6	Private	CCTV in a bank
7	Public	Local authority
8	Public	Police criminal records
9	Public	ANPR
10	Public	Europol
11	Public	Border Control
12	Private	Loyalty card (transport)
13	Private	Mobile phone carrier
14	Private	Banking records
15	Private	Credit card records
16	Private	Advanced passenger information
17	Private	Facebook Ireland Ltd.
18	Private	Microsoft Hungary
19	Private	Google Budapest

7.2.3 Submitting Access Requests

As per the table below, 19 subject access requests were sent via email and/or ordinary mail to data controllers of various sites; 9 of them were actors of the public sector (including 4 CCTV operators), while 10 addressees belonged to the private sector (including 2 CCTV operators) (Table 7.2).

In Table 7.3, the number of substantial responses can be seen divided into two main categories (CCTV and non-CCTV sites), and within each main category the number of those data controllers who provided the requested data completely, or partly, or denied the provision of data. From these quantitative data only the number of substantial responses can be regarded as objective, all other numbers reflect the subjective evaluation of the researchers, and can be interpreted together with the narrative description of the cases. These data do not reflect the specific circumstances of the fulfilment of access request, such as timeliness, facilitation etc. which may influence the overall picture on the situation of the enforceability of the right of access to one's own personal data in Hungary.

The success of the requests heavily depended on the existence of an internal data protection officer (although in one case it was exactly the DPO of a mobile telecommunication service provider who denied access to the requested mobile phone location data by relying on a sophisticated – and false – legal argumentation), the existence of a routine procedure for handling citizens' requests, and the knowledge of law, including data protection law.

Table 7.3 Main qualitative findings

Substantive responses to access requests		Public	9/9	Total: 17/19
		Private	8/10	
Fulfilment rate of access requests (w/o CCTV)	Satisfactorily fulfilled	Public	5/5	Total: 6/11
		Private	1/6	
	Partly fulfilled	Private	3/6	Total: 3/11
	Denied	Private	2/6	Total: 2/11
Fulfilment rate of access requests to CCTV footages	Copy of footage provided	0/6		
	Footage could be seen	1/6		
	Information given on the content of the footage	3/6		
	Obsolete because of deleting the footage	1/6		
	Denied	1/6		

Data controllers generally did not ask the requesters about the purpose of the access request. In one case the data controller argued that the requested data (cellphone location data) were useless for the requester and this was one of the reasons why the data controller did not want to provide the requested data. Access to CCTV recordings constituted a special category in this regard, since certain sector-specific laws stipulate that the requester needs to prove her legal interest – this has raised a general legal question about the content of subject access as defined in the general data protection law and the sector-specific laws. Some of the addressees turned to the NDPA themselves (large department store and the local authority) in order to clarify their obligations.

When experiencing spoiling or diversionary tactics, we referred to concrete legal provisions and found that such action generally helped: in such cases the requests were forwarded to the competent person or organization. There was one case in which the data controller when responding to the second, repeated request, accepted our position and changed its earlier decision. The attitudes and procedures of the multinational companies again constitute a special category: here we primarily tested whether the data are accessible in one's mother tongue.

A general experience was that the data controller organizations did not regard the requested data as "personal data" in terms of data protection law, rather data relating to their own business processes or data necessary for providing a service. In one case, the employee of the data controller argued that the requested data (cellphone location data) are personal "only secondarily": primarily these are data serving the purpose of providing a telecommunication service.

In what follows, the above overall picture about the degree of realization of subject access rights will be detailed in a case by case structure. Experiences of attempts to access personal data held by public and private sector organizations will be discussed in separate sections. The most instructive cases will be analyzed in a very

detailed manner, covering the description and evaluation of every step of the case, while others will be summarized briefly focusing only on the cardinal points of the case.

7.2.4 Public Sector

It was a general experience that public sector organizations have an established organizational structure for handling citizens' requests, including subject access requests, as well as an established procedure for administering such cases.

The request-handling routine of the public sector organisations also resulted in offering facilitative means to us, such as downloadable forms for requesting information, and in most cases this was accompanied by a higher level of preparedness and legal knowledge – not only in data protection law but also in the laws regulating their specific data processing activities. Consequently, the procedure of handling access requests was generally conducted in writing, in a neutral, official way, regulated by established internal rules, no special courtesy or disrespectful communication have been experienced.

The responses of the data controller organizations in the public sector always included the legal reasoning for the decisions taken, whether correct or not, in line with the requirements of the law on the general rules of administrative proceedings and services.

Vehicle Records – Central Office for Public Administrative and Electronic Public Services (COAES)

In the first – and perhaps the most informative – case, we requested our personal data related to the ownership of motor vehicles from the district office of the government authority of the capital city. The office responded in writing (in 10 days, well within the deadline of 30 days defined in the data protection law), informing us that the request had been transferred to the department of traffic registry of the Central Office for Public Administrative and Electronic Public Services (COAES), the office which has authority and competence in the case.

Two weeks later, the COAES department sent us a notice asking us to pay a sum of HUF 1.650 (cca. EUR 6) as an administrative service fee, in order to process this request. In response, we sent another letter to the department, repeating the original subject access request, and explaining our position, according to which demanding an administrative service fee was unlawful and against the provisions of the data protection law. We argued that it is not the law and ordinance on traffic registry the provisions of which are applicable in such cases but those of the Data Protection Act which provide the guarantees of a fundamental right of citizens, and which stipulate that such subject access requests are free of charge the first time within one calendar

year. This second, repeated request was forwarded to the superior organizational unit of the original department.

The head of the superior department, within the legal deadline, responded to the repeated request, and sent an official document to us in which she confirmed that in cases where citizens make subject access requests, the provisions of the data protection law do indeed apply, and demanding a fee was unlawful. In sum, the office accepted our position and changed its decision. Presumably the request had been sent back to the original department, which then sent a detailed letter to the requester a few days later with all the requested data and information.

Police Records

In the case of requesting our criminal personal data from the national headquarters of the police, submitting the request and receiving the response was a seamless procedure. The request was sent to the office of the national police headquarters. The head of the office responded to the request, informing us that he had forwarded the request to the Criminal Director-General of the police, who in turn forwarded it to the head of the criminal analytic department, from where the head of the office received the information that no criminal personal data in connection with us had been processed.

A similar request had been sent to the criminal records authority of COAES, where criminal personal data on prior convictions are stored. This case, however, became more complex than the former. The request sought disclosure of all our personal data processed in the criminal registration system, the date of recording the data, the purpose and legal grounds of storing the data, the expected date of deleting the data, as well as detailed information on which personal data have been forwarded from this registry to which third parties, for which purpose. The head of the competent department of the authority responded to the request in 3 weeks and called us to obtain additional personal identification data (mother's maiden name, date and place of birth) which we provided by return of mail. A few days later, a short reply arrived from the same department head, according to which no data about us were processed in the criminal registration system; however, information about forwarding our data to third parties would be sent in a subsequent letter, since investigation in this matter was under way.

More than a month later, we sent a letter asking when could we expect the promised additional reply about forwarding our data to third parties, and if no data about us had been processed at all in the criminal registration system, what kind of data could have been forwarded in this case. A short reply arrived from the same department, informing us that our request had been transferred to the personal data registration department – that is, to the population register. A few days later an *earlier dated*, long and detailed letter from the head of the personal data registration department arrived, in which the head of department "acknowledged" that we wanted to know what sort of data forwarding about us took place in the 5-year period from 25 September 2008 to 25 September 2013. However, it is worth noting that the original

request was about data processed in the criminal registration system only, and no time period was indicated in the request. Evidently, it was a misunderstanding (or over-zealousness) of the criminal records authority to transfer the request on data forwarding to the population register. Nevertheless, the letter from the population register contained a long list of our personal data which had been forwarded to third parties in 19 cases during the 5-year period, indicating the exact types of data, the dates and the legal grounds of forwarding.

ANPR

A request about our personal data processed in the automatic number plate recognition (ANPR) system operating on motorways was submitted to the state-owned company in charge of controlling motorway administration. At the time of submitting the request, the company was responsible for operating the whole motorway administration under the name State Motorway Company, while at the time of closing the case the company was renamed as National Road Toll Collecting Company with a reduced competence. The request was however processed by the company with the original competence. In the detailed and politely written answer by the competent leaders of the company, we were informed that no data about us were processed in the ANPR system, nor about the car we indicated in our request. The letter also included easily understandable information about the operation of the system, which automatically records number plate data, then cross-checks the ANPR data with the road toll payments, and if the recorded car has a valid road toll payment for the given area and time period, the ANPR data are automatically deleted; only non-payers' data are further processed and stored for 2 years after the termination of the case. Since we were involved in no such incidents, our data were not stored in the system. The letter also indicated the legal provisions relevant to the case.

Border Control – Schengen Information System

The subject access requests concerning border control data was submitted to the international criminal cooperation unit of the national police, and to the national office of the Schengen Information System. These requests resulted in fast and efficient replies. In the first case the director of the international criminal cooperation unit of the national police informed us just 1 day after receiving the request that in the previous year the International Criminal Cooperation Center did not process personal data about us. Moreover, the response explained that requesting information on exchange of personal data in the framework of the Schengen Information System should be submitted on a downloadable form. We submitted such a form to the competent authority, the government authority of the capital city. The authority of the capital city forwarded the request to the same organization as above, the International Criminal Cooperation Center of the national police headquarters. The

director of the Center informed us in a letter that following their searches, no data or warning about us was processed in the Schengen Information System.

7.2.5 Private Sector

In the course of the research, we sent eight access requests to a range of individual private sector entities: a telecommunication service provider (mobile carrier), two private banks (banking and credit card records), an airline company (advanced passenger records), an oil company (loyalty card), and three multinational companies, namely Google, Facebook, and Microsoft.

All in all, the private sector presented a much more heterogeneous picture than the public sector, which made it difficult to draw general conclusions. While certain sites demonstrated high degree of facilitation in handling our access requests, others showed strongly or relatively restrictive practices.

Loyalty Card (Transport)

We made a request to access our personal data relating to our loyalty card to the company via e-mail by writing to the data controller's general contact address. This mail was followed by an acknowledgement mail from the company right after the submission advising that the request was being processed and would be answered within 48 h. This turned out to be a promise that they did not keep. However, the company dealt with the request relatively quickly, and sent its reply around 2 weeks later, many days before the legal deadline.

The response was formulated in a highly professional manner addressing all the questions that the request had contained. The reply was easy to read since the information provided was perfectly itemized and structured according to the questions posed in the request. As for its content, besides the detailed information provided on the legal basis, purpose, and amount of time of data processing as well as the types of data collected and generated, the company also informed us about the questions on third party data sharing and automatic decision making process. In doing so, the respondent specified exactly to whom and for what purpose our personal data had been disclosed. As explained in the letter, personal data relating to our loyalty card had been subject to automatic decision making process in certain parts of the data processing (e.g. information about the amount of loyalty points, sending of a newsletter), however, the company applies high level data security methods in these parts of the data processing procedure in order to prevent unauthorized persons from accessing these data.

In our subjective standard of evaluation, the data controller showed a particularly high degree of facilitation of subject access rights. This company has definitely acknowledged access rights by fulfilling the request in a way as if it had been the most natural thing in the world. The only thing missing from the procedure was that

the company had failed to examine our identity before it started to process our request (even though we submitted the request from a newly created e-mail address that has not been known by the company) which, to some extent, appeared to contradict the respondent's statement on how much effort they invest in the protection of data security. Apart from this, the company performed an accurate, efficient, but also simple processing of access requests.

Mobile Phone Carrier

The request for mobile carrier data was sent both via email and ordinary mail to the internal data protection officer of the company whose contact data was found in the privacy policy published on the company's website. In the request, we asked the company to provide all our personal data generated in connection with our mobile phone use (including locational information) during a certain time period.

The first reply, which was received almost 2 months later, was not sent to our mailing address at the time of making the request (as was indicated in the request), but to an earlier mailing address registered at the service provider's mailing list, which was apparently not up to date. The willingness of the internal data protection officer (DPO) to respond to the request was shown by the fact that following unsuccessful attempts to deliver the reply by ordinary mail, he contacted us by telephone.

The envelope included a list of calls made on our cell phone within the period specified in the access request and a response letter. The letter stated that we could find attached our call itemization, however, the company was not in the position to provide the requested locational (cell) information. It also declared that none of our personal data has been shared with third parties, and stated that the company does not use automatic decision making process. The explanation of the grounds for denial of the requests to access locational information was two-page long starting with the respondent's (i.e. the DPO's) apology: "*I am sorry for making you feel bored with dry legal reasoning but providing accurate information on the relevant laws on locational data is necessary to dispel your doubts that might have arisen in your mind about our policy on handling subject access requests.*" The legal reasoning of the data protection officer can be summarised as follows:

The data protection officer indicated the provision of Decree no. 6/2011 (X.6.) NMHH of the National Media and Infocommunications Authority on the detailed rules of electronic communications subscriber agreements according to which "call itemization may be requested on a case by case basis, for a definite term or until withdrawal; and it shall be made available to the individual subscribers requesting so once a month free of charge. In the respondent's interpretation: "*This provision lays down the framework for the application of the statutory provision on the right to information in the telecommunications sector; i.e. by stating that the service provider shall provide the subscriber with one call itemization per month free of charge*, *it is also indirectly stated that in any such case when the request of personal data has no data management purpose related to the verification of the correctness of fee*

calculation, the right to information shall be restricted." [emphasis added by the authors] According to the DPO therefore, the purpose of such restriction is so the right to information does not become some sort of unlimited right giving room for abuse, since in the course of contracting, the client has the accurate knowledge anyway as to what kind of personal data is managed by the service provider. According to the letter, subscribers have no valid legal title to obtain their own personal data, because they exercise "real time control" over data management by the service providers every time they initiate a call, since they generate the data created during the calls themselves. In this context, it was implicitly considered as an abuse of right that the researcher made an inquiry about cell information: "*When calling, the subscriber should know where he stays, so the need to know cell information may also easily qualify as an abuse of right.*" Elsewhere, also implicitly, it made us appear as though we were seeking to exercise our right of access in bad faith: *"A bona fide client can be expected to be aware of the fact where he has been with his telephone (with the exception of the case of the injured climber, when an appropriate legal title to disclose the data is available to the authorities being competent to do so)."* According to the vision outlined by the DPO, "*should the right to information of the person concerned be unlimited, every subscriber could request every day the provision on an electronic medium of all its cell information generated in connection with the use of the service that day. Such a broad interpretation of the right to information […] would jeopardise the safety of the supply of such service."* The respondent also tried to convince us about the uselessness of cell information with the argument that these technical data do not allow the exact localization of cell phones.

We subsequently replied to the letter in a long response demanding access to all the undisclosed information (cell information, internet traffic data, list of incoming calls). We explained that in our opinion, the decree referred to as the legal basis for the denial of the claim is not a rule restricting the right to access to personal information, but a guarantee for the protection of the consumers, which vests the subscribers with the opportunity of control over the service provider's invoicing practice. The fact that such control is realised by the sharing of personal data with the data subject, not only does not restrict the application of the right to one's own data, but actually promotes it. From the decree it does not and may not even follow that in the electronic telecommunication sector data subjects' right to access to their personal data are limited to a specific purpose, namely to the verification of the correctness of fee calculation, and thus the service provider's obligation is confined to making accessible the call itemization serving such purpose, since no decree may be given a meaning that is contrary to the statutory rule. We also pointed out that the right to access to personal data undoubtedly does not result in an unlimited right; the content and extent of such right may only be established with respect to its legitimate limits. However, data controllers have no leeway to establish the limits of the exercise of rights; such restrictions may only result from legal provisions (like third parties' rights).

Shortly thereafter, we received a response letter explaining that despite all the arguments outlined in our previous letter, the data protection officer did not share the view that the company was obliged to provide locational information. The officer argued that "*cell information are primarily technical details necessary to provide telecommunication services, and only secondarily personal data.*" Since being unable to fulfil our request, the data protection officer agreed to continue the legal dispute before the NDPA. Accordingly, on 5 March 2014, we initiated an investigation of the NDPA pursuant the Data Protection Act[70] alleging that the company had infringed our right to access our own personal data.

The denial of providing access to location and other data (internet traffic data, list of incoming calls) and the firm resistance regarding these data (including the disingenuous and misleading legal argumentation, which may sound absurd for professionals) shows the danger of downplaying the importance and exercisability of this right in cases when the provision of the requested data might be cumbersome or inconvenient for the data controller. The position of the NDPA in this case will certainly be decisive in how the data controller and similar service providers may restrict subject access rights in the future. Although the investigation should already have been terminated (the time limit for investigation is 2 months), at the time of publishing, no response has yet arrived to the researcher's complaint from the NDPA.

Facebook, Google and Microsoft

Requests to multinational companies were sent in our native language (i.e. in Hungarian). To those organizations which had a national office in Budapest, namely Google and Microsoft, the requests were sent there. In case of Facebook, the request was submitted to the European headquarters based in Ireland.

Requests submitted to Google and Facebook followed a very similar path, in the sense that we could not provoke any reaction from these companies to our requests despite repeated submissions. In the case of Google, our attempts to get in touch with the national office (Google Budapest) failed twice and both ordinary letters we sent were returned with the notice that "*the recipient has not taken delivery*". Similar to Google, Facebook has also been reluctant to deal with our request. From the perspective of the enforceability of access rights, the only difference between the two cases is that while in the case of Google, we exactly know what happened to our letter (i.e.: it was returned to her), in the case of Facebook, the fate of the letters is unknown; we do not even know whether they have reached their addressees or not.

Microsoft showed a somewhat more responsive attitude than its counterparts, however, our attempts to gain access to our personal data relating to a Skype account also failed. As stated above, the data request to Microsoft was sent to the national office (Microsoft Hungary). One month later (one day after the expiry of the 30 days

[70] Section 52 (1) of Data Protection Act.

deadline) we received a very short letter in return, informing us that Microsoft Hungary has not been controlling our Skype data. The respondent noted that Microsoft's privacy policy related to its Skype products is available on the internet (the exact link to this was also put into the letter). For the remaining questions regarding the processing of personal data, we were advised to turn to the Skype Customer Support. Accordingly, we submitted the request to the Microsoft Customer Support. On the day of submission, we received a reply from "Rocky" (Microsoft Customer Service Representative – as presented) written in English. The letter said: *"At this time, I would like to let you know that we are only able to respond using the English language. Please provide your information in English, so that we can provide you the required support option*." This linguistic inflexibility, despite the fact that Microsoft has a national office in Hungary, therefore restricted our attempts to continue a dialogue with the organisation.

Advanced Passenger Information

By contrast, the national office of the airline to which we submitted our request for advanced passenger information data willingly helped us in receiving a substantial response to her request, although ultimately the procedure did not result in receiving the requested data.

The request to the Budapest office of the company was made on a week day at 6:03 a.m. via e-mail, and was answered in 2 h, at 8:06 a.m. This e-mail informed us that the data processing regarding the personal data of the passengers is subject to the German data protection law, since the seat of the company is located in the territory of Germany, and its branch offices and service organizations in foreign countries are under the jurisdiction of German law. According to the German data protection law, the company is entitled to provide access to personal data of passengers only to German authorities, in the case of police and judicial procedures. Consequently, the requested data can only be received from the competent German authorities. For further information, we were advised to contact the Security and Data Protection Department of the company; contact details thereof were also provided.

Since we wanted to receive further information about the data processing (exact legal grounds of processing, legal restrictions etc.), we turned to the given department in a letter which, having received no reply, we sent again a month later. However, no reply arrived to these letters. This shows that although a positive response was elicited from the company initially, follow up responses were not forthcoming and only a partially successful outcome was obtained in this case.

Credit Card Records

This case concerned a major commercial bank belonging to an international network of financial institutions. The letter was sent by us both by e-mail and ordinary mail.

An automated e-mail reply arrived almost in the same minute, acknowledging the message, and promising a substantial response within 3 days. The next day a polite response arrived by e-mail, according to which the request had been forwarded *in the form of a complaint* to the competent branch of the bank. This suggests that organizations which receive a large number of complaints but only a few access requests under the data protection law, have developed a routine procedure of handling complaints, and regard all other types of requests as complaints and process them accordingly.

About a month later a reply arrived by ordinary mail which provided the following information:

- listed our bank accounts and the general types of data processed in connection with such accounts,
- listed in detail our personal identification and communication data,
- as regards the forwarding the data to third persons, the letter referred only to the outsourced banking activities, and – rightly – quoted the relevant acts, according to which data processors do not qualify as third persons.

This meant that the letter provided only partial information about forwarding personal data. The letter also contained an attachment in which the relevant data protection provisions of the bank's internal regulation were included.

To our surprise, another reply arrived a few days later from the branch office where we also have bank accounts, signed by two advisors of the bank. The letter informed us that the processing of the request had begun, however it was "not identifiable" what kind of data we wanted to access. Therefore we were advised to attend the branch office of the bank in person at our earliest convenience (we did not do so, because we did not want to reveal our "double identity" as a citizen and an expert in data protection). Nevertheless, it could be established that the procedure was adequate, despite treating the request as a complaint, the provided data were correct, albeit not complete, and – to be on the safe side – the customer service department forwarded the request also to the branch office in order "to identify" the real content (and intent) of the request.

Banking Records

We submitted an access request to a multinational bank with offices in Hungary. However, the reply of the bank had been sent not to the mailing address indicated in the request but to the mailing address registered in the bank, and since we moved to a new address (which we indicated in the request), the reply had not arrived. After we conducted a long investigation through telephone in order to learn the reasons of

the non-response to our request, the bank eventually found the undelivered letter and promised us that they would re-mail it to the correct address. However, the letter has never reached us.

There are several reasons why the bank's behaviour can be considered as restrictive. Firstly, the bank (in contrast to the mobile service provider) did not take any pro-active steps to reach us when realising that delivery had failed. This is especially unreasonable when taking into account that the bank frequently calls us (as a customer) on the phone providing direct marketing offers, and holds many types of contact details for us in its databases. Secondly, we made it clear in our request to which address we expected the letter but the bank ignored this information. Thirdly, we also submitted our request in e-mail, which raises the question of why the bank was unable to send its response electronically, too. This procedural inflexibility was surprising, particularly given the size of the data controller as one of the leading banking organisations in the world.

7.2.6 CCTV

The handling of access requests submitted to public and private sector entities in the area of CCTV surveillance made ambivalent impressions on us. Whilst the purpose of the relevant sector-specific laws appears to ensure the enforceability of subject access rights regarding CCTV surveillance, the practical realization of these rights turned out not to be free from anomalies. As the following findings will demonstrate, the vague wording of the laws and certain unresolved questions of legal interpretation left a wide area of uncertainty concerning the scope of subject access rights regarding CCTV footages. In addition, even where the law set forth clear terms, a significant level of reluctance could be observed on the side of data controllers to obey the provisions concerned.

The Presence and Quality of CCTV Signs and Privacy Notices

From the perspective of data subjects exercising their access rights, the possibility to swiftly identify and localise data controllers are of utmost importance in the case of CCTV footages. This is so because, in order to follow the principle of purpose limitation, the relevant laws specify a very short period for the retention of personal data, and footages must be deleted immediately after the expiry of this period. Consequently, any difficulty that might be encountered in practically submitting an access request potentially jeopardises one's efforts to obtain the footage before its deletion. With this in mind, the presence and quality of CCTV signs will be analyzed below in a separate section.

We did not find a single CCTV signage which displayed information about the data controller regardless of which sector (private or public) the surveillance was being performed in. This is partly because in certain areas of CCTV surveillance, lawmakers have failed to enact particular provisions detailing what should be included in CCTV signage. For instance, the Police Act and the Act on Public Space Supervision, which had relevance when we examined CCTV surveillance in the Ministry of Public Administration and Justice and in a public space, provide that it is mandatory for data controllers to inform citizens about the use of video surveillance cameras via well-visible notices. These Acts, however, do not determine any legal requirement for what should be included in the signage (i.e. the identity of the data controller, contact data etc.).

But even when the law in force contains the requirement to post both a warning signage (image or pictogram) and a privacy notice in order to convey information to citizens on the processing of personal data, data controllers did not even fulfil this legal obligation.

For example, the Passenger Transport Services Act to be applied to CCTV surveillance on public transport settings and the Personal and Property Protection Act to be applied to the use of CCTV in certain governmental buildings, banks etc., do contain provisions on what information should be displayed where CCTV cameras are in operation. According to these Acts, such a notice should cover, among other information, the legal basis and the purpose for electronic surveillance, the place where the footage is stored and the period of storage, the person using (operating) the system, and the persons authorized to access these data, and also information on the legal rights of data subjects including the procedures for enforcing such rights. In the light of these precise requirements, it is hard to find a reason for the patent lack of such information in the case of the data controllers acting under the scope of these Acts.

As well as the lack of disclosure of relevant information on data processing related to CCTV surveillance, the location and form of CCTV signs were also matters of concern from the perspective of access rights. According to the Act on Public Space Supervision CCTV signs should be located *in a way that facilitates the recognition of surveillance cameras*. The Private Property Act prescribes that the warning sign and the above detailed information shall be displayed in a *clearly visible place*, and in an easily understandable fashion, while the Passenger Transport Services Act specifies that CCTV signs and information shall be placed at every station entrance, stops, platforms and – in certain vehicles – on board, too. As can be seen in the images below, data controllers apparently had not put much effort into designing CCTV signs. Such signs may be sufficient for data controllers to refer to, in case of legal disputes concerning the legal grounds of data processing, but in fact, they do not support citizens' ability to recognise the presence of CCTV cameras. This practice undermines or at least makes questionable the fulfilment of the requirements of informed consent.

CCTV in a government building (inside)

CCTV in a government building (outside)

CCTV in a public space of Budapest

CCTV warning sign on the bus

CCTV in a bank

Picture 7.1 CCTV signage is various settings

As per Picture 7.1, oftentimes, CCTV operators do not provide accurate information on CCTV footage disclosure procedure (CCTV in public space, CCTV in public transport setting, CCTV in a bank). Things got worse when one CCTV operator appeared to display a resentful acceptance that the researcher does indeed have a legitimate right to access his/her data (CCTV in public space), or directly challenged it (CCTV in a bank – see below).

Twisting the Law – Emerging Questions of Legal Interpretation of Access Rights

Requests submitted to CCTV data controllers have implicated several questions of legal interpretation that thwarted us in our attempts to realise our access rights. True enough, apart from one CCTV site, at the end of the research, none of the CCTV

data controllers questioned that under certain circumstances we do indeed have legitimate rights to gain access to our personal data. However, two issues led to constant dispute: (1) what conditions one should meet in order to exercise the right to access personal data, i.e. when an access request is considered to be legitimate; and (2) to what extent such a right provides the data subject with access to his/her personal data, i.e. what is to be meant by "access". Based on the results of the research, behind the air of uncertainties about the interpretation of these two issues, three particular questions of law to be further refined may be identified:

1. *Third party rights:* Decisions regarding disclosure of CCTV footage were basically influenced by the question of how the fulfilment of the request would affect the rights of third parties. This interpretation issue comes from the characteristic of CCTV recordings that data included in the footage rarely relate to a single person. Consequently the data processor has to maintain a balance between the conflicting fundamental rights of different persons. Whilst the person submitting the data request shall be entitled to know the data relating to him, the other persons concerned can legitimately expect that, as main rule, access to their personal data shall not be granted to other persons than the data controller himself.
2. *The relationship between general and sector-specific legislation:* Difficulties in the enforcement of access rights in this context have emerged from the fact that whilst the Data Protection Act, in accordance with the Data Protection Directive of the EU, does not link the information requested on personal data to any purpose or proof of legal interest, the access rules set out in the sector-specific regulations on CCTV do contain such restrictions.

   As such, several data controllers expected us to confirm our right or lawful interest. In this respect, data controllers were not satisfied with referring to access rights as set out in the Data Protection Act; we were also supposed to demonstrate the initiation of an administrative or court proceeding in order to obtain the recording.

3. *Restrictive vs extensive interpretation of the right of access:* Some CCTV operators did not share the view that we had the right to view the recordings or request a copy thereof because of the wording of the Data Protection Act, which, contrary to that of the Data Protection Directive, does not literally include the right of "access", stating instead, under the general heading "Rights of data subjects; enforcement" that "The data subject may request from the data controller: (a) information on his personal data being processed…" [Section 14] This provision was interpreted by certain data controllers in a way that meant that the obligation of the data controller would only cover the provision of information, but not access to the data.

As the following findings will demonstrate, the lack of clarity of these questions of interpretation played a major role in influencing the success of our access requests. Therefore, in almost all cases, we had to invest significant energy in formulating adequate legal argumentations when negotiating with the data controllers. It is questionable whether lay persons would possess such knowledge, meaning that

the success of an access request appears to be the preserve of those data subjects with significant data protection law expertise/awareness.

CCTV in a Government Building

In the case of requesting CCTV footage from the Ministry of Public Administration and Justice, we sent our claim to the Department for Social Contacts. Shortly thereafter, we were informed that after consulting with the Department of Personnel and Security Management, the Social Contact Department forwarded the request to the data controller of the CCTV footage, i.e. to the Reserve Police Force. This letter thoroughly explained the legal background of the sharing of duties among the Ministry and the Police relating to video surveillance (in terms of equipment, operation, and data processing). Shortly after, we received a response from the Reserve Police Force. The reply contained the whole range of the information we had asked for (the legal basis of data processing, retention time, third party sharing, automatic decision-making process) and an accurate and very detailed description of what could be seen on the recording relating to the researcher: "*Applicant approached the ministry building in Akademia Street from the direction of the Kossuth Square corner at 15:31:41, (…) entered the building at 15:33:26, left the building at 15:50:58 etc*." However, our request for receiving a copy of the footage had been denied. The reason for this was, according to the letter, the very fact that the wording of the Data Protection Act does not include "access" among the rights of the data subject: "*The Data Protection Act itemizes the legal rights you – as a person concerned – are entitled to. Hereby I inform you that there is no possibility of forwarding the recording to you since the provision of the Act on the catalogue of legal rights quoted before does not include such a legal right.*"

CCTV in a Government Building

By contrast, when attempting to access the CCTV footage recorded in the other government building, namely the Office of Land Administration, we were granted the opportunity to see the footage. We received a reply to our request from the Head of the Office. The letter stated that the Office had got in touch with the NDPA in order to answer the legal uncertainty that emerged in relation to the access request. As stated in the letter, this consultation resulted in the following decision: "*In compliance with your request and the concerning law, my Office is required to provide you information on the footage. What more I can offer to let you see the footage. I am not allowed to send you a copy of the recording since you are not the only person depicted on it (…). If I forwarded the footage to you, it would violate the rights of third parties.*"

CCTV on Public Transport

We asked for a copy of the CCTV footage recorded of us on a bus on way to work. In the absence of privacy notices, we submitted the request to the public office responsible for transport services. In its reply, which was only six lines long, the respondent informed us that at the time and place specified in the request the cameras were not in operation, and in any case, on the basis of the concerning law (which was not specified in the response letter), only the police and the judicial authorities are allowed to gain access to CCTV footage.

Following this reply, we sent a further letter to the service provider in which we wrote that passengers can apparently never know for sure whether a camera on board is in operation or not, thus, we could not challenge the statement that no personal data related to us was being processed. We added that in the absence of specifying the concerning law, we could not accept that only the police and the judicial authorities are allowed to gain access to CCTV footage. To prevent the data controller from not responding to this question, we presented a new data request in our letter hoping that this time we had managed to take a bus on which the surveillance equipment was in operation.

The second e-mail of the service provider informed us that the bus specified in the second access request was travelling with working cameras at the given time. Nevertheless, the data controller did not provide any other information on processing our personal data in its response. The respondent argued that according to the relevant rules included in the Act on Passenger Transport Services, the requested recording may contain personal data related to us was not under the control of the service provider but the control of a different – private – company (the bus operator). For that reason the respondent refused to answer our questions about the third party data sharing and automatic decision-making process, too.

As such, the public office responsible for transport services basically hid behind the argument that the transfer of personal data is only allowed upon the request of public authorities. This argument, however, exonerates the data controller from the obligation to send a copy of the recording only, the other obligations relating to informing the data subject remain in force (e.g. whether the data subject has been recorded at all, or which third parties the recording had been shared with). This is the obligation the data controller failed to comply with by presenting itself as an entity outside of the system of data processing. Although the Act on Passenger Transport Services does not explicitly define who the data controller of the CCTV recordings shall be, it imposes the obligations relating to the data processing in connection with surveillance (including the posting of CCTV signage and privacy notice) on the service provider, and not on the operator. Thus, even if it is not the public department but the bus operator who is in possession of the data, the public office qualifies as data controller. The fact that the public office is the data controller – in contrast with the information provided by the company – can also be observed in the wording of its letter, since the respondent used first-person plural throughout the whole letter in which he explained to us why we could not access our own personal data. This reveals that the decision regarding data processing had been

made by the public office itself. We quote verbatim: "*To your question about why we only provide personal data to requests coming from judicial or governmental authorities: For your information, we set out that in our view , it can be unambiguously established on the basis of the Act on Passenger Transport Services (…) that the suspension of destruction of video recordings may only be requested by those whose legal right or lawful legal interest is prejudiced by the footage, and who can also provide proof of having the right or lawful interest he refers to. In our opinion, such right or lawful interest – with respect to the Act on Passenger Transport Services – can only be established if the consulting of the recordings is necessary for the successful concluding of a judicial or administrative procedure."* (emphasis added by the authors). This raises the question: if the public office is not the data controller, what is the relevance of its position in handling subject access requests? Consequently, in our view, the denial of the data controller status was based on a misinterpretation of the law.

In summary, the organization prevented us from gaining any kind of access to the requested CCTV footages upon three different grounds, including claims that (1) cameras were not working, (2) personal data may only be shared with public authorities, and (3) the public office is not in the position of data controller. This variety of denial reasons, especially the confusing mixture of the latter two, suggest that in the second round the respondent was seeking ways to avoid granting access to the data, rather than seeking ways to at least partially satisfy our request.

CCTV in a Public Space

To gain access to a CCTV footage taken in a public space of Budapest city centre (District IX), we submitted a request to the Public Space Supervision Authority of Ferencvaros 4 days after we had been recorded. The access request was sent to the general contact e-mail address of the authority (also by ordinary mail). Contrary to our expectation of an immediate or at least swift reaction, we only received a reply almost 2 weeks later. This informed us that storage time for CCTV footages taken in public spaces is 8 days in accordance with the law, and thus the recording specified in the request had already been deleted. The very short reply also contained some information on the legal basis of the operation of electronic surveillance in public spaces, and set out that the CCTV footage related to the researcher had not been transferred to any third party before its deletion.

In our response, we accepted the fact that the footage was no longer accessible but due to the lack of provided information we put further questions to the organization. We reminded the data controller that we had submitted the request 3 days before the expiry of the retention period, and the request was sent to an e-mail address we had previously been instructed to use. With this in mind, we asked the organization to provide information about its procedure for processing access requests, and the conditions under which such a request can have a chance to be fulfilled. Shortly after the letter was sent, we received a phone call from the author-

ity. The member of staff at the end of the phone line wanted to enquire about the number plate of our car in order to identify us case since she was not able to find it. When we told the administrator we had not been in our car at the time of the recording (we were just walking by), the administrator got confused and asked (somewhat angrily): "*Then what's your problem? I really don't understand your point.*" When we replied that we only wanted to exercise our access rights, the administrator replied: "*Anyhow, I am going to forward your request to the Legal Department of our organization.*"

The organization's written reply brought an interesting twist to the case. The director of the authority wrote to us advising that the access request was managed in normal course of administration which started only after the retention time limit. As such, there were no special administrative provisions or procedures to receive and process subject access requests as a matter of priority. Nevertheless, even if they would have noticed the request earlier, they could not have provided a copy of the recording in any case, since the Act on Public Space Supervision stipulates that this can be done only in case of instituting a judicial or administrative procedure, and this special provision supersedes the provisions of the Data Protection Act.

This case has served to expose several weaknesses of the enforceability of access rights regarding CCTV surveillance. Firstly, the Supervision Authority has evidently failed to work out a special procedure for handling subject access requests. The lack of such self-regulation undermined the possibility of exercising our access rights by bringing it down to the luck factor of how fast the administration is able to react to the requests in normal course. Secondly, the reluctance on the part of the organization to process the request before the expiry of the retention time has turned out to be a possible strategy of denial: the second reply of the director revealed that the authority would have not intended to provide access to the footage even if our request was processed in time. Given the fact that the data controller totally concealed this reason for denial from us in its first reply, and taking also into account that it had 3 days to process the request within the retention time, it would be naive not to assume that the authority sought to cut the 'Gordian knot' of conflicting laws on access rights by hiding behind the legal obligation of deletion. Thirdly, to a data subject who is not as determined as we were in this case, phone calls like the one described above might give the impression to him/her that the request is illegitimate.

CCTV in a Department Store

In relation to access to CCTV recordings, we certainly engaged in the liveliest dialogue, which included the most turns, with the data controller for the large department store during the research. The department store first responded to our request by phone. The call came from the head of the security service who advised he was calling merely to indicate that the organisation had sent their letter by mail including "their request". The man seemed very responsive, but also suspicious and

mysterious, leading us to feel as though were were being tested as to whether we were 'normal' and mentally intact. The essence of the short written response received from the organisation was that we should come to the company for the purpose of personal identification: "*You surely understand that based on a letter (…) without establishing the identity of the person, we do not have the possibility of sending data by mail.*" As such, we attended the site in person shortly thereafter. Having confirmed our identity, the head of security said that they had never received such a request before, but they immediately saved the data and would send their substantive written answer soon. He also informed us that we were recognisable on the CCTV footage based on the detailed description specified in the request. However, in a subsequent letter, the organisation claimed that they operated their CCTV system under a sector-specific law (the Condominiums Act) and as such access requests for CCTV footage needed to be justified by us. With no resolution in sight, the company decided, without supplying our personal data, to turn to the NDPA itself. The data controller asked the Authority to advise as to how the request of a natural person can be duly fulfilled in a case where such request is directed to the disclosure of camera recordings in which other persons can be seen in large number whose consent cannot be obtained and their continuous wiping out of the images would not be technically feasible or would cause unjustified and unreasonable expenses. The request for the release of a position was drafted by a law firm and was also mailed to us some weeks later.

Although the company has not disclosed the footage at the time of writing, the manner in which it processed the subject access request, with special regard to the progressive step of initiating the procedure of the NDPA convincingly demonstrates readiness and willingness to fulfil individual subject access requests. In our view, as far as the legal position of a data controller is not *contra legem*[71] but reasonably correct, and clearly represented to the data subject, the mere fact that one data controller provides narrower interpretations to the scope and application of the right to access personal data than the total dimension of this right (i.e. to get a copy of the footage), especially with respect to third parties' rights cannot be considered as a restrictive practise. Moreover, the fact that the data controller has turned to the NDPA instead of engaging in a further (eventually legal) dispute with us can be read in the way that the data controller did not expect a citizen to fight for the enforcement of a possibly legitimate aspect of access rights. This behaviour can be regarded advantageous for compensating the information imbalance between the parties.

CCTV in a Bank

We contacted the bank in order to gain access to the CCTV recordings taken of us during the use of the cash machine placed within the building of the branch office. In the absence of any other possibility, the request was submitted online using the

[71] Against the law.

template for all kinds of enquiry. We received an acknowledgement mail on the same day advising that the request was qualified as "complaint" and being processed. The substantive answer of the bank was received some weeks later and consisted of quite incoherent sections. The first paragraph informed us that "*(the bank) is only able to provide information on banking transactions to customers after customer identification or requests from public authorities. Recordings may only be forwarded to authorities."* The second paragraph provided certain information on the legal basis of processing personal data (individuals' consent) and the related relevant laws. In connection with the specific question of whether the bank shared our personal data with any third party, the next paragraph declared: "*Should you believe that the recording was supplied to a third party in an unauthorised manner or an abuse occurred, you might submit a criminal report."* Finally, the letter contained the possibilities of legal remedies available to us, and the position of the bank according to which our complaint appeared to be investigating a breach of *consumer protection rules* (emphasis added by the authors). This incorrect categorization of the request might serve as explanation for why the list of remedy forums only included the existing financial supervisory authorities, and did not mention the most adequate forum, namely the NDPA.

We replied shortly thereafter and stated that it was not entirely clear to us whether the request was denied, and if it was, then for exactly what reason was the request found illegitimate. As regards the client status, we set out that since the use of a cash machine is considered to be the use of a banking service, even if the user has an account agreement with another bank, and anyone using a banking service of the bank is qualified as client in accordance with the General Business Conditions of the company, we were certainly a client in this case. Besides, we also noted that the enforceability of subject access right cannot logically be subject to client status, since the bank may also capture and store images of persons who may not necessarily make use of the banking services and do not request the provision of such service. With respect to third party data sharing, we wrote that we would only become aware whether the recordings got in the possession of unauthorised persons, if the bank as data controller, by meeting its statutory obligation, informed us as to whom it forwarded the recordings taken of her, if those were forwarded.

Soon afterwards, we received a phone call from the head of security at the bank. The aim of the call was to inform us about the existence of the footage and provide information on what could be seen on the picture. The head of security informed us that we were not entitled by law to receive a copy of the footage. He behaved in a very friendly and helpful manner during the call. As a matter of fact, he was sometimes too friendly, making comments that could be characterised as sexist (such as commenting on our appearance). As the head of security could not exactly specify the legal basis for denying the forwarding of the footage, we asked the bank to send its position on this issue in a written form. This subsequently sent reply explained that the reason for denial of provision of a copy was the protection of *bank secret (*emphasis added by the authors).

In summary, the bank showed an ambivalent attitude towards us, in which the ways of avoidance and willingness to act in accordance with the law were mixed.

The company inherently appeared to discourage us in our attempts to access the CCTV footage by representing a blurry, incoherent legal reasoning in the reply. It cannot be ruled out but it is unlikely that the organization was actually incompetent in handling the request. Even if such requests are uncommon in the course of normal administration of the organization, it would still be hard to believe that in such a large-scale organization as a bank, no legally qualified individual could recognise a subject access request, especially in a case where we referred to the legal basis of our request to the data controller. For that reason, qualifying the access request as consumer complaint can reasonably be considered as restrictive practices. Most probably, the turn in the course of communication was the result of our decided manner and our legal preparedness – after this, the bank became significantly more responsive. It can be reasonably supposed that in other circumstances, lay persons may have by then already given up the case, not to mention the fact that the CCTV recordings would have not been retained in time.

7.2.7 Conclusions

Three concluding thoughts of long term relevance can also be drawn from the experience accumulated in the course of this empirical research in the Hungarian context.

The first conclusion has relevance from the aspect of dogmatics of constitutional law, according to which fundamental rights should be interpreted broadly, while restrictions of these rights should be interpreted in a narrow sense. In practice, some of the data controllers seem to follow the opposite approach: they tend to interpret the right of access narrowly, and the restricting provisions broadly, especially in the area of CCTV surveillance.

The second conclusion has implications regarding national and EU-level data protection regulation: the wording of the Hungarian Data Protection Act follows the wording of the EU Data Protection Directive, according to which the data subjects have a right to obtain "*information* at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed", "*communication to him* in an intelligible form of the data undergoing processing and of any available information as to their source", and "*knowledge* of the logic involved in any automatic processing of data concerning him" [emphasis added by the authors].[72] The Hungarian law reads: "Upon the data subject's request the data controller *shall provide information* concerning the data relating to him, including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to

[72] Art. 12 of 95/46/EC Directive.

data processing, and – if the personal data of the data subject is made available to others – the legal basis and the recipients." [emphasis added by the authors].[73]

The only important difference between the wording of the two legal documents is that the relevant section of the EU Directive has a title: "Right of access" while the Hungarian law does not contain this title. It is questionable whether providing information about the personal data includes access (and receiving a copy of) the data themselves, especially in the area of CCTV recordings, where the selecting and separating of the data subject's personal data require specific technical and organizational efforts. Two arguments could be raised in favour of granting access (and providing copies of) CCTV footage: first, the right of rectification and erasure may become meaningless if the subject has no access to the data themselves (although rectification can hardly be realized in this area); second, certain European guidelines on CCTV surveillance emphasize the right of the data subjects to access the recordings, and/or possess a copy thereof. The video-surveillance guidelines issued by the European Data Protection Supervisor (EDPS) on 17 March 2010 (EDPS 2010) provide that "If this is specifically requested, access needs to be given to the recordings by allowing the individual to view the recordings or by providing a copy to him/her. In this case the rights of third parties present on the same recordings need to be carefully considered and whenever appropriate, protected (for example, by requiring consent for the disclosure or image-editing such as masking or scrambling). Protection of the rights of third parties, however, should not be used as an excuse to prevent legitimate claims of access by individuals" (Section 12, "How to fulfil access requests by members of the public") These guidelines should be interpreted and promulgated by the national data protection authorities in order to achieve standard practice in this area.

Finally, the third conclusion is the realization of the fact that without coherent guidance issued for data controllers in the area of processing subject access requests, the requesters are subject to the arbitrarily restrictive interpretation of the relevant legal provisions by the data controllers. The issuance of such guidelines would be the task of the national data protection authorities, who could also assist organizations representing or supervising certain data processing sectors, such as financial institutions or telecommunication service providers, in drafting their own sectoral guidelines.

The newly democratic legal and institutional framework had been developed in the early 1990s, the decisive characteristics of which were the inclusion of the right to privacy and data protection in the Constitution, the German model of informational self-determination, and, until recently, an ombudsman-type parliamentary commissioner as data protection supervisory authority. Despite recent controversial changes, this system is in force today essentially unchanged. It can be established that Hungarian law implemented all substantial elements of the EU data protection directive, in a structure of a general law/sectoral law model, with high penetration of sectoral and area-specific legal regulation into various branches of the legal

[73] Section 15 (1) of Data Protection Act.

system. This was coupled with a highly successful parliamentary commissioner as DPA, which has recently been replaced with a government authority.

The findings outlined above suggest that subject access requests *per se* are extremely rare in Hungary, in some cases the researchers' test requests were the first of this kind in the practice of the data controllers concerned. Consequently the number of court cases involving subject access complaints are low, and the researchers did not find any case in which the court ruled that compensation should be paid for denying access to the plaintiff's own personal data. The parliamentary commissioner, while it existed, was actively supporting the enforceability of access rights, and the legal obligation of data controllers to inform the DPA about the denied requests also helped the commissioner and the general public alike to learn the state of affairs in this area. Similarly, the central registry of data controllers (which is in recent years unavailable online), could help data subjects learn the identity and connections of data controllers.

Identifying data controllers proved to be relatively easy, and this may give a false impression that access as a whole is an easy exercise. Finding *specific* information about how and where to submit access requests was more difficult and showed the lack of knowledge of the personnel at some sites. It was difficult to assess how up to date the information found in online privacy policies was and indeed in several cases the information was evidently outdated. As for locating data controllers of CCTV systems, the researchers did not find a single CCTV signage which displayed information on the data controller regardless of which sector (private or public) the surveillance was being performed in. Once requests were submitted to organisations, researchers found that certain central government offices had high quality facilitation strategies, due to the well worked-out nature of their general customer service procedures. There were also some private companies where the quality of information and the facilitation strategies were satisfactory. However in both the public and private sectors the overall picture was varied; in particular, the processes and responses of multinational companies were unsatisfactory, partly because of the lack of communication in the national language.

The success and ease of submitting an access request was highly dependent on the knowledge and personal character of the contact persons within each organisation. The strongest strategies of denials were found amongst CCTV operators, who misinformed the requester that only the police had right to access the recordings; did not know who the actual data controller was; or kept asking why the researcher needed her own data. Furthermore, in one case a well educated internal data protection officer at a telecommunication service provider used his skills and knowledge to try to convince the requester about the legal and practical impossibility of fulfilling her request rather than use his expertise to facilitate her right of access.

It should be noted however that in a small country like Hungary, where the number of subject access requests are low, and there are only a few specialized privacy/data protection experts whose identity is easily detectable, it is questionable whether the researchers could play the role of lay requesters convincingly in all cases. Therefore in future empirical investigations it seems advisable to use volunteers for submitting access requests, if considerations of research ethics permit this.

Finally, some supplementary conclusions emerged. Firstly, a positive side-effect of submitting access requests was that in some cases it generated a learning process at the data controller: they overruled their earlier decisions, organized an internal course about these issues, or turned to the NDPA for guidance. Secondly, where there exists a general customer service procedure, access requests can be handled according to this procedure. At certain private companies there is no such general procedure, therefore these companies interpreted the requests as "complaints".

References

Legislation and Case Law

ABI-2136-3/2010/K.
ABI-1470/A/2006.
Act No. CXII of 2011 on the right to informational self-determination and on the freedom of information.
Act No. CLXI of 2011 on the Organisation and Administration of Courts.
Act No. CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing.
Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators.
Act CXXXIII of 2003 on Condominiums.
Act No. XLVII of 1997 on the Handling and Protection of Medical and Related Data.
Act No. XX of 1996 on the Identification Codes and Methods Superseding the Personal Identification Number.
Act No. CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing.
Act No. CXXV of 1995 on the National Security Services.
Act No. LXVI of 1992 on the Register of Personal Data and Addresses of Citizens.
Commission v Hungary, Case C-288/12.
Decision No. 15/1991 (IV. 13.) AB.
Decision No. 24/1998 (VI. 9.) AB.
Decision No. 44/2004 (XI. 23.) AB.
Fovarosi Torvenyszek P.25905/2010/26.
Metropolitan Court 26.K.32.704/2012/5.
Resolution No. 2643/2012 (11.28.) of the Metropolitan Assembly.

Articles and Reports

'Ajánlás a munkahelyen alkalmazott elektronikus megfigyelorendszer alapveto követelményeirol', http://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf (accessed 17 September 2014
Atlatszo.eu(2014a)'AdatvédelmiBiztos',http://abi.atlatszo.hu/index.php?menu=beszamolok/(access 17 September 2014)
Atlatszo.eu (2014b) 'About Us', http://atlatszo.hu/about-us/(accessed 17 September 2014)
Dajko, P. (2012) 'Camera Surveillance in Hungary', *IT Cafe*, 29 January 2012, available at http://itcafe.hu/cikk/adatvedelmi_nap_2010_kameras_megfigyeles/kameraellenes_vagy_kamer-aparti.html [in Hungarian].

EDPS (2010) 'The EDPS video-surveillance guidelines', https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf (accessed 17 September 2014).

European Commission (2012) 'Press Release - European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary', http://europa.eu/rapid/press-release_IP-12-24_en.htm?locale=en (accessed 7 October 2014).

Halmai, G. and Scheppele, K. L. (eds.) (2012) 'Opinion on Hungary's New Constitutional Order: Amicus Brief for the Venice Commissions on the Transitional Provisions of the Fundamental Law and the Key Cardinal Laws', available at https://docs.google.com/viewer?a=v&pid=sites-&srcid=ZGVmYXVsdGRvbWFpbnxhbWljdXNicmllZmh1bmdhcnl8Z3g6NWU4NWIwYjUwOTI0MzQzNw

Hungarian Civil Liberties Union (2014) 'About Us', http://tasz.hu/en/about-us (accessed 17 September 2014).

Javorniczky, I. and Majtenyi, L. (eds.) (1999), *Stories from Tukory Street* [in Hungarian], Information and Documentation Center for Human Rights, Budapest.

Laszlo, G. (2005) 'Magyarorszagi weboldalak adatvedelmi nyilatkozatainak elemzese [Analysis of privacy notices of websites in Hungary]', in Szekely, I. and Szabo, M. D. (eds.), *Szabad adatok, vedett adatok [Open data, protected data]*, Department of Information and Knowledge Management, Budapest University of Technology and Economics.

Ministry of Justice (2014) 'Az Igazságügyi Minisztérium közleménye' http://os.mti.hu/hirek/98715/az_igazsagugyi_miniszterium_kozlemenye (accessed 17 September 2014).

NDPA (2012a) 'Annual report of 2012' available in Hungarian at http://naih.hu/files/NAIH_BESZaMOLo_2012_net3.pdf (accessed 17 September 2014).

NDPA (2012b) 'Ügyszám: NAIH-4384-2/2012/V', http://www.naih.hu/files/4384_V_2012-2.pdf (accessed 17 September 2014).

NDPA (2012c) 'Ügyiratszám: NAIH-1318-5/2012/V', http://www.naih.hu/files/1318_V_2012-5.pdf (accessed 17 September 2014).

NDPA (2013a) 'Állásfoglalás a Google Street View szolgáltatás. Magyarországon történo bevezetésével kapcsolatban', http://www.naih.hu/files/Adatvedelem-NAIH-5711-162012B-Google-SV.pdf (accessed 17 September 2014).

NDPA (2013b) 'A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a munkahelyen alkalmazott elektronikus megfigyelő rendszer alapvető követelményeiről' http://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf

Szabo, M. D. (2014) 'Szelektiv szigor az informacios szabadsagjogok ervenyesulesenek ellenorzeseben' [Selective rigour in supervising the enforcement of information rights], MTA Law Working Papers 2014/32, Hungarian Academy of Sciences.

Szabo, M. D. and Hidvegi, F. (2014) 'Ket itelet es vegrehajtasuk' [Two judgments and their enforcement], *Fundamentum* No. 4, 2014, pp. 69–82.

Szabo, M. D. and Szekely, I. (2005) 'Privacy and data protection at the workplace in Hungary', in S. Nouwt and B. R. de Vries (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, IT & Law Series, T. M. C. Asser Press, The Hague, pp. 249–284.

Szekely, I. (2007) 'Central and Eastern Europe: Starting from Scratch' in A. Florini (ed.), *The Right to Know. Transparency for an Open World*, Columbia University Press, pp. 116–142.

Szekely, I. (2008) 'Hungary', in J. Rule and G. Greenleaf (eds.): *Global Privacy Protection: The First Generation.* Edward Elgar Publishing Ltd., pp. 174–206.

Szekely, I. (2016) 'From a model pupil to a problematic grown-up: Enforcing privacy and data protection in Hungary' in David Wright and Paul de Hert (eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer International Publishing, pp. 79–104.

Szigeti, T. and Vissy, B. (2012) 'Ombudsman', in *Corruption Risks in Hungary 2011 – National Integrity Study*, Budapest, Transparency International, pp. 146–157.