INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

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

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

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

HUNGARY COUNTRY REPORTS

EÖTVÖS KÁROLY INTÉZET, HUNGARY

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN HUNGARY – DR IVAN SZEKELY & BEATRIX VISSY

LOCATING THE DATA CONTROLLER IN HUNGARY – DR IVAN SZEKELY & BEATRIX VISSY

SUBMITTING ACCESS REQUESTS IN HUNGARY – DR IVAN SZEKELY & BEATRIX VISSY

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN HUNGARY

Introduction

Hungary is one of the so-called new democracies of the European Union, and this fact needs to be taken into consideration when mapping the legal and administrative frameworks of the country in the area of informational rights in general, and data protection and subject access rights in particular. The present legal and administrative framework had not been developing in a long term organic process but was created in the turbulent period of the great political changes, and the further developments of the system took place in the milieu of a transitional society.[1]

The informational-legal system, which is in force today essentially unchanged, had been codified during the political changes in 1989 and the early 1990s, following long decades of a Soviet type legal and administrative system, and reflected a profound change to the domestic political concept of the informational rights.[2] Inserting stipulations regarding these rights into the Constitution of 1989 not only proved to be a symbolic denial of the totalitarian regime, but the establishment of enforceable rights played a key role in the process of Hungary's constitutionalisation, too. To recall the words of the first Parliamentary Commissioner for Data Protection and Freedom of Information – also called as the data protection ombudsman –, winning these rights by the revolution of the rule-of-law was "the axis, or, at least, one of the axes on which the world turned here".[3]

The main characteristics of this system[4] 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 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.

[1] For more about this process, see 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.
[2] For a detailed description see Szekely, I. (2008), "Hungary", in J. Rule and G. Greenleaf (eds.): *Global Privacy Protection: The First Generation.* Edward Elgar Publishing Ltd., pp. 174–206.
[3] Majtenyi, L. (2006), *Information freedoms* [in Hungarian] Budapest, Complex.
Solyom, L. and Brunner, G. (eds.) (2010), *Constitutional Judiciary in a New Democracy. The Hungarian Constitutional Court.* University of Michigan Press.
p. 17.
[4] See 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.

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:[5] among others, it abolished the Constitution and the combined data protection and freedom of information law of 1992 and replaced them 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,[6] and restricted 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.

In the following we take the present state of data protection law, and within this subject access rights and the enforcing possibilities, as the basis of our overview. However, due to the above changes, there is a certain discontinuity in case law: neither the case law of the Constitutional Court, nor that of the Parliamentary Commissioner can be regarded as legal reference[7] (although using their argumentation is not formally forbidden). Therefore in our analysis the corpus of case law we refer to can be taken into consideration only with limited relevance.

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

In Hungary, the most important principles of data protection were 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.[8]

[5] For a broader critical overview about the changes, see 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

[6] 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 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/24&format=HTML&aged=0&language=EN&guiLanguage=en (last accessed 18 July 2013).

[7] A recent amendment to the Basic Law invalidated all Constitutional Court decisions in which reference were made to the (then existing) Constitution, while according to the new data protection (and freedom of information) act the newly established government authority is not the legal successor of the former institution of the parliamentary commissioner, consequently it is not bound by the case law that have been developed throughout the preceding period.

[8] Decision No. 15/1991 (IV. 13.) AB. The decision is available in English at http://www.alkotmanybirosag.hu/letoltesek/en_0015_1991.pdf (last accessed 18 July 2013). See also Decisions No. 29/1994 (V. 20.) and No. 46/1995 (VI. 30.) AB.

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. These acts play a significant role in putting into effect the principles defined in the Data Protection Act both in the public and private sector (identification codes, address registration, health information, police information, school results, national security services, employment, telecommunications, insurance, human genetic data etc.).[9]

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 report above). This concept 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 personal data.[10] In exceptional cases, personal data may also be processed if required by law (an Act of Parliament or a Decree of a local government).[11] 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.[12] The Data Protection Act establishes, as a main rule, an opt-in regime: personal data may only be collected and processed after obtaining the freely and explicitly given, informed consent of the person concerned by which the individual signifies his/her unambiguous agreement to having personal data processed fully or to the extent of certain operations.[13] However, the concept of informational self-determination is undermined by a newly introduced provision in the Data Protection Act which stipulates that personal data may be processed also if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary either for compliance with a legal obligation pertaining to the data controller, or for the purposes of the legitimate interests pursued by the controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.[14]

[9] In Hungary nearly 1.000 sector- and area-specific legal statutes contain provisions on the processing of personal data, including exceptions to the general principles and details of processing of data.
[10] Section 5 a) of Data Protection Act.
[11] Section 5 b) of Data Protection Act.
[12] 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".
[13] Section 3 point 7 of Data Protection Act.
[14] Section 6 (1) of Data Protection Act.

Exceptionally, in the area of postal direct marketing, there is an opt-out system applicable to direct marketing companies (or companies using direct marketing methods for advertising their products and services). Similarly to the postal direct marketing acts of other countries, these companies are authorized by this act to process citizens' name and address data without their consent in order to establish contact with the data subjects. The companies are obliged to provide written information in the mailings about the source of the data, the purpose of processing the data and the possibilities to object to the further processing of the data. The same applies, with slightly different guarantees, to organizations conducting public opinion research and scientific research.[15] It should be noted, however, that in the area of electronic communications (for example, e-mail or telemarketing) it is necessary to obtain preliminary consent of the data subjects.

The consent can be given in any form, except in the case of processing "special data" (in the wording of the EU Data Protection Directive: special categories of data).[16] These categories of data may only be processed where the subject has consented in writing or if it is based on an international agreement or required by law for the purpose of enforcing a constitutional right, national security purposes, crime prevention, or a criminal investigation.[17]

To have an appropriate legal ground (either the consent of the data subject or legal authorization) is not sufficient for the processing of personal data to be lawful; data processing has to be proportional, too. Accordingly, the Data Protection Act declares that personal data may be processed only for specified and explicit purposes, when it is necessary for the exercising of certain rights and fulfilment of obligations. The purpose of processing must be satisfied in all stages of data processing operations, which means that only the personal data necessary to accomplish the purpose may be collected, and it may only be stored until that purpose is fulfilled.[18] As it was confirmed by the Hungarian Constitutional Court, the adherence to the purpose to be achieved is a precondition of exercising the right to informational self-determination.[19] The data subject must be fully informed of the purpose of the data processing.

Other fundamental data protection principles are also reflected in the Data Protection Act. The act prescribes that personal data must be accurate, complete, and if deemed necessary in the light of the aim of processing, up-to-date (data quality principle).[20] It also provides that the data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique (security safeguards

[15] Section 4 (1) point c) of the Act No. CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing.
[16] Special data is defined in the Data Protection Act as personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, personal data concerning sex life, health, pathological addictions, or criminal record. (Section 3 point 3 of Data Protection Act).
[17] Section 5 (2) of Data Protection Act.
[18] Section 4 (1)-(2) of Data Protection Act.
[19] Decision No. 15/1991 (IV. 13.) AB on the processing of personal data and the unconstitutionality of the universal personal identification number.
[20] Section 4 (4) of Data Protection Act.

principle).[21] If the data subject, in the event of any infringement of his or her rights, turns to court action against the controller, the burden of proof to show compliance with the law lies with the data controller (accountability principle).[22] The data protection register containing information about the data controllers is open to the general public, it may be inspected by any person, including taking notes (openness principle).[23] The most important principle in the area of the right of access to one's personal data, the individual participation principle is reflected in several provisions of the act (see below).

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

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.[24] 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."[25] 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 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.[26] The

[21] Section 7 (3) of Data Protection Act.
[22] Section 22 (1)-(2) of Data Protection Act.
[23] Section 65 (4) of Data Protection Act.
[24] Decision No. 15/1991 (IV. 13.) AB.
[25] Decision No. 15/1991 (IV. 13.) AB.
[26] Section 14 of Data Protection Act.

data subject also has the right to object to the processing of data relating to him/her.[27] The legal right to inspect the Data Protection Register can also be qualified as a data subject right.[28] 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,[29] the Personal Identifiers Act,[30] the Medical Data Act,[31] the Direct Marketing Act,[32] and in the specific provisions relating to data processing, of other acts: the Police Act,[33] the Health Act,[34] the Security Services Act[35], the Electronic Communication Act[36] 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.[37] 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.[38] 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 more than thirty days.[39] 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.[40] 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.[41]

[27] Section 21 of Data Protection Act.
[28] Section 65 (4) of Data Protection Act.
[29] Act No. LXVI of 1992 on the Register of Personal Data and Addresses of Citizens.
[30] Act No. XX of 1996 on the Identification Codes and Methods Superseding the Personal Identification Number.
[31] Act No. XLVII of 1997 on the Handling and Protection of Medical and Related Data
[32] Act No. CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing.
[33] Section 91/B of the Act No. XXXIV of 1994 on the Police.
[34] Section 24 of the Act. No. CLIV of 1997 on Health.
[35] Sections 29-32 of the Act No. CXXXIII. of 2005 on Security Services and Private Investigators.
[36] Sections 154-156 of the Act No. C of 2003 on Electronic Communications.
[37] Section 15 (1) of Data Protection Act of 2011.
[38] Section15 (2) of Data Protection Act.
[39] Section 14 (4) of Data Protection Act.
[40] Section 14 (5) of Data Protection Act.
[41] Section 17 (1) of Data Protection Act.

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.[42] 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.[43]

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.[44] 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 thirty days of receipt of the request.[45]

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).[46] The data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the NDPA.[47] 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.[48] Moreover, the NDPA may intervene in the action on the data subject's behalf.[49] 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.[50]

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.[51] 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

[42] Section 17 (4) of Data Protection Act.
[43] Section 17 (2) of Data Protection Act.
[44] Section 18 (1) of Data Protection Act.
[45] Section 18 (2) of Data Protection Act.
[46] Section 22 (1) of Data Protection Act.
[47] Section 18 (2) of Data Protection Act.
[48] Section 22 (2) of Data Protection Act.
[49] Section 22 (4) of Data Protection Act.
[50] Section 23 of Data Protection Act.
[51] Decisions No. 24/1998 (VI. 9.) AB and No. 44/2004 (XI. 23.) AB.

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.[52] 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.[53] 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.[54] The Act sets out that apart from mandatory processing, data processing may not commence prior to registration.[55] 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 on its website.[56] 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.[57]

Case law

Insofar as can be established from open sources,[58] individual cases aimed explicitly at enforcing subject access rights occur only sporadically in Hungary. In a recent lawsuit

[52] 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 18 July 2013).
[53] Section 65 (4) of Data Protection Act.
[54] Section 65 (1) of Data Protection Act.
[55] Section 66 (1) of Data Protection Act.
[56] 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."
[57] Section 411 (6) of the Act No CCI of 2011.
[58] 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 18 July 2013) Summaries of potentially relevant court rulings can be found in

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. 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.[59] 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.[60]

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 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."[61]

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.[62] 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

---

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.

[59] Annual report of 2012 by the NDPA, available in Hungarian at http://naih.hu/files/NAIH_BESZaMOLo_2012_net3.pdf (last accessed 18 July 2013).

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

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

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

frame specified in the user's request. In the said cases, the law also provides for the option of intercepting, tapping and taping calls.[63] 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 a lawsuit of 2010, 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.[64] 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.[65]

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.[66] 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.[67] On 28 November 2012, the Budapest Metropolitan General Assembly passed a resolution in support of allowing Google to launch the service in Budapest,[68] with the proviso that Budapest may only be featured on Google Street View in compliance with the guidelines of the NDPA.[69] Now anyone is able to report his/her concern

[63] 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 18 July 2013).
[64] Section 24 (3) of Act No. CLIV of 1997 on Health.
[65] 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.
[66] Available in Hungarian at http:// 81.183.229.204:51111/abi/index.php?menu=0/Sajtokozlemenyek&dok=20090507_ABI_ (last accessed 18 July 2013).
[67] 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 18 July 2013).
[68] Resolution No. 2643/2012 (11.28.) of the Metropolitan Assembly.
[69] See http://www.naih.hu/files/Adatvedelem-NAIH-5711-162012B-Google-SV.pdf (last accessed 18 July 2013).

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).[70]

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

Section VI of the Data Protection Directive lists the exemptions and restrictions from the provisions of Directive 95/46/EC. According to Article 13 of the Directive, Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in the Articles referring to the collection of personal data, the finality of processing, the information to be given to the data subject in advance of data processing, the right of access to data, and the publicizing of processing operations, when such restrictions are necessary to safeguard national security, defence, public security, crime prevention and prosecution, important economic or financial interest of a Member State or of the European Union, and the protection of the data subject or of the rights and freedoms of others.

The Hungarian Data Protection Act implements these provisions of the directive at national level. 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. [71] 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.[72]

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

[70] 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.

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

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

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.[73] 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.[74] In addition, once a year, data controllers shall notify the NDPA) on the annual information regarding refused requests, by 31 January of the following year.[75]

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.[76]

Compatibility of national legislation with Directive 95/46/EC

Hungary, similarly to the other Member States of the European Union, has implemented the provisions of the data protection Directive. Since the country joined the EU in 2004, and the system of its data protection legislation had been developed already in the 1990s, Hungarian legislators were prepared for issues of compatibility in advance of the accession. It is worth mentioning that the Council of Europe granted membership to Hungary in 1990, and the country had signed the Data Protection Convention of the Council of Europe in 1993. Hungary had ratified and promulgated the Convention only in 1997 and 1998, respectively, because the competent authorities did not want to ratify the Convention until the appropriate regulations for the data processing sectors had been implemented, according to the recommendations of the Council of Europe. All this resulted in a situation whereby meeting the requisites of the Directive did not demand any major amendments in domestic law. The European Union had already recognized Hungary as a country offering adequate level of data protection. Thus, in 2000 Hungary became the second non-EU country after Switzerland to secure this recognition. The minor amendments of the data protection act which were necessary to enact during the harmonization process included the broadening of the powers of the (later abolished) institution of the Parliamentary Commissioner for Data Protection and Freedom of Information, and clarifying of the categories of "special data".

However, in January 2012, the European Commission launched accelerated infringement proceedings against Hungary before the European Court of Justice, among others, over the

[73] Section 48 (1) of Act No. CXXV of 1995 on the National Security Services.
[74] Section 27 (1) of Act No. CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing.
[75] Section 16 (3) of Data Protection Act.
[76] Report of the National Authority for Data Protection and Freedom of Information on its activities in 2012, p. 31, http://www.naih.hu/files/NAIH_BESZaMOLo_2012_net3.pdf [in Hungarian] (last accessed 18 July 2013).

independence of its data protection authorities.[77] 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.[78] 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.[79] This was reflected in the Court's judgement delivered on 8 April 2014. In its decision the Court declared that Hungary had 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.[80]

Surveillance and access rights: codes of practice at national level. CCTVs and credit ratings

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

[78] For a brief fact sheet regarding the controversial institutional changes see: http://www.ekint.org/ekint_files/File/data-protection_independence_fact_sheet_ekint_hclu_hcc.pdf (last accessed 18 July 2013). The letter of NGOs to Mr Jose Manuel Barroso analyzing the developments is available here: http://www.ekint.org/ekint_files/File/barroso_dpa_independence_20111106_printed%281%29.pdf (last accessed 18 July 2013). For a more complex analysis on the structural changes which affected the institutional set of data protection see: Szigeti and Vissy (2012).

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

[80] 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 7 May 2014).

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 seventeen 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.[81] 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 monitoring systems at the workplace.[82] 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.

The *Central Credit Information System* (KHR) is a national database operated by a specialized company (BISZ Zrt.) together with over 450 financial institutions and banks in Hungary, managing customer and agreement data and providing credit information to the member organizations. KHR was originally designed for sharing information on past events of credit default and fraud, however, the new legislation regulating the operation of the KHR Service[83] provides for the mandatory registration of positive credit data on natural persons in the KHR, too. Where not associated with default, individuals' credit data are automatically deleted when their legal relationship is terminated.

[81] 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.

[82] Recommendation of the National Authority for Data Protection and Freedom of Information on the basic criteria of operating electronic monitoring systems at the workplace http://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf [in Hungarian] (last accessed 18 July 2013).

[83] Act CXXII of 2011 on the Central Credit Information System.

The Central Credit Information Act provides that "persons registered in the KHR shall have unlimited access to their own data in the KHR and to information on access to such data, which shall be granted free of any charges or fees."[84] Request for access to own data may be submitted at any of the member organizations which submits customer data to the KHR or directly at BISZ Zrt. To do so, the customer has to complete a downloadable Own Credit Report Request Form and submit it at a branch of the credit institution. The credit institution forwards the request to BISZ Zrt. via the KHR. BISZ Zrt. prepares the form containing the Own Credit Report, and sends it in a sealed envelope to the headquarters of the credit institution forwarding the request. The unopened envelope is delivered by the credit institution to the customer who requested the report. The Own Credit Report includes all credit data on the customer, the names of the credit institutions registering those data in the KHR, and information on the use of and queries for the data.

Associations of private companies operating in trade and marketing sectors or in property protection and private investigations generally created their codes about the fair practices in the professions concerned. These codes may contain provisions on the processing of personal data and the access rights of the data subjects.

The *Hungarian Distance Selling Trade Association* (an organization consisting of 10 regular and 8 supporting member companies representing about 40% of the total turnover of retail distant selling trade in the country) was established in 1993, with the aim of establishing, supporting and controlling fair practices in the distant selling sector in Hungary. Section 8 ("Data Protection") of its Code of Ethics[85] contains only general provisions about the processing of personal data, including the duty of the members to inform data subjects of the data protection implications of their online marketing practices. However, provisions about subject access rights are not included in the Code.

The *Hungarian Advertising Association* is the national organization of institutions, companies and individuals active in marketing communications. The primary objective of the Hungarian Advertising Association, which was established in 1975, and today has 70 individual and 200 institutional members, "is to safeguard the interests of its members and promote the prosperity of the industry." (Mission Statement,[86] Art. 1.) The Association also "codifies, endorses and applies the ethical standards of the advertising profession." (Art. 4.) The first Hungarian Code of Advertising Ethics was created already in 1981. The present version of the Code[87] was drafted in 2005. Art. 11 of the Code (Protection of personal rights) contains some general provisions regarding the handling of personal data: "(1) Advertisements shall not use a person's name, portrait, sound recording and pronouncements in an unauthorized way;" and (3) "Consumers/Receivers shall be informed about handling

[84] Art.15 (7) of the Central Credit Information System Act.
[85] Code of Ethics of the Hungarian Distance Selling Trade Association, http://www.arukuldok.hu/upload/2013_05/28/1369747224347578 17/mae_etikai_kodex.pdf [in Hungarian] (last accessed 18 July 2013).
[86] The Hungarian Advertising Association's Mission, http://mrsz.hu/mission.php?cmssessid=T43d7d27611947028667d6995f843c5f0cc84a8d9057788e45fa755e85232a57 (last accessed 18 July 2013).
[87] Hungarian Code of Advertising Ethics, http://www.mrsz.hu/index.php?set_lang=en;cmssessid=T63678265e7b8b247d1b690845c85320e4606ead0ecbdef472398aa0609a76f6] (last accessed 18 July 2013).

their personal data before they approve of receiving advertisement. Solely those personal data shall be handled during the advertising activity which are necessary to sending the advertisement, and solely for the time of carrying out the aim." Provisions on subject access are not included in the Code.

The *Direct and Interactive Marketing Association* (previously: Direct Marketing Association) was established in 1995 in order to distinguish companies representing fair practices in marketing from those operating in an unfair way. The Code of Ethics (2012) of the Association[88] contains relevant professional information in a wide range of marketing practices and technologies. However, provisions regarding the processing of personal data do not go beyond the provisions of the data protection law; in the area of subject access "the data subject may request information about the processing and forwarding of his/her data" free of charge once per year.

The *Association of Hungarian Content Providers* (MTE), a self-regulating body, was founded in 2001 by Hungarian internet content providers in order to support the Hungarian Internet business market with verified and professionally supported commitments, and with the tools of self-regulation. MTE is striving to achieve the regulation of the Internet with the least state intervention possible, and that emphasis is placed on self-regulation.[89] The Association created the professional code of internet content providing, and the code of ethics describing a generally accepted system of ethical norms for Hungarian content provision. The Code of Content Providing is a long and detailed document,[90] Appendix No. 2 of the Code is a "Declaration of Data Protection". The Appendix is also very detailed (in our opinion, unnecessarily detailed, containing long cut-and-paste sections from the data protection act), and contain provisions on subject access. However, these provisions simply repeat the general provisions of the data protection act, no further guarantees of procedures are included. At the request of the data subject, the data controller is obliged to provide information on the personal data processed, in a written and easily understandable form, as soon as possible, but no later than within 30 days from the submission of the request (Appendix 2, III. d). Although the last update of the Code is from 2007, and consequently the text of the Code does not reflect recent changes in data protection legislation, provisions regarding subject access are still in line with the current law.

The *Chamber of Bodyguards, Property Protection and Private Detectives* – the organization representing private companies, which, among other tasks, operate CCTV systems where property protection is outsourced – has its own Code of Ethics. The only provision regarding data protection is included in the regulation of ethical investigations, in the course of which

[88] Code of Ethics of the Direct and Interactive Marketing Association, available at http://www.dimsz.hu/anyagok/DIMSZ_Etikai_Kodex_12_11_28.pdf [in Hungarian] (last accessed 18 July 2013).
[89] Association of Hungarian Content Providers: History and Goals, http://www.mte.hu/eng_egyesulet.html (last accessed 18 July 2013).
[90] Code of Content Providing: Regulation of operations, ethics, and procedures with respect to content providing, issued by the Hungarian Association of Content Providers, available at http://www.mte.hu/dokumentumok/mte_kodex_eng.doc (last accessed 18 July 2013).

"protection of business, economic and private secrets, the data protection provisions and the respect for personality rights shall be observed".[91]

The Code of Ethics of the *Hungarian Detective Association* does not contain provisions on the handling of personal data.[92]

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[93] and the Condominium Act.[94] 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.[95] 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.[96] Such surveillance systems may not be used in a place where surveillance is likely to violate human dignity (dressing rooms, toilets, hospital wards etc.).[97] 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.[98] The provisions of the act do not specify how data subjects (the identifiable persons on the recordings) may exercise their access rights.

The Condominium Act includes provisions on implementing and operating of video surveillance systems in the common property sections of condominiums. Video cameras may only be operated for the purpose of protecting human life and safety, prevention of unlawful

[91] Code of Ethics of the Chamber of Bodyguards, Property Protection and Private Detectives, available at http://www.szvmszk.hu/files/Etikai_szabalyzat_2008-12-05.pdf [in Hungarian] (last accessed 18 July 2013).
[92] Code of Ethics of the Hungarian Detective Association, available at http://www.detektivszovetseg.hu/images/pdf/etikai_kodex_2013.pdf [in Hungarian] (last accessed 18 July 2013).
[93] Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators.
[94] Act CXXXIII of 2003 on Condominiums.
[95] Section 1 (1) of Security Services Act.
[96] Section 30 (2) of Security Services Act.
[97] Section 30 (2) of Security Services Act.
[98] Section 31 (2)-(4) of Security Services Act.

activities and the protection of common property. Cameras may not be directed to doors or windows of private property. Recordings must be preserved for 15 days, and after this period the recordings must be deleted.[99] Again, this act does not contain regulations on access rights, only a provision referring to the rights of the data subjects as regulated in the Data Protection 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.[100] In 2000 the Commissioner issued a recommendation on image recording devices[101] 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.[102] 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.[103]

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

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

[99] Section 25 of Condominium Act.
[100] See the annual reports of the Parliamentary Commissioner for Data Protection and Freedom of Information, published in English in printed format (ISSN 1416-9762), currently available on the archived website of the commissioner at https://81.183.229.204:51111/dpc/index.php?menu=reports (last accessed 18 July 2013).
[101] Recommendation of the Data Protection Commissioner on the use of image recording devices in surveillance and information collection, in *Annual report of the Parliamentary Commissioner for Data Protection and Freedom of Information*, Budapest, 2000, pp. 54-63.
[102] See a detailed report on the conference in Hungarian: Dajko, P., "Camera Surveillance in Hungary", *IT Cafe*, http://itcafe.hu/cikk/adatvedelmi_nap_2010_kameras_megfigyeles/kameraellenes_vagy_kameraparti.html (last accessed 18 July 2013).
[103] NAIH-4384-2/2012/V, in Hungarian: http://www.naih.hu/files/4384_V_2012-2.pdf (last accessed 18 July 2013), and NAIH-1318-5/2012/V, in Hungarian: http://www.naih.hu/files/1318_V_2012-5.pdf (last accessed 18 July 2013).

regarding the last two 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.[104]

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 move to improve the level of enforceability of these rights. Such movements has not been typical of the predecessor of the NDPA either. However, the Commissioner had been involved in some 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.[105] To help the 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,[106] and data subjects were also able to search in the register.[107] 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. The book contained various short stories about how data protection rights can be enforced.

Role of NGOs in ensuring access rights

In the new democracies of the Central and Eastern European region, for historical reasons, the non-governmental sector is underdeveloped and lacks the necessary resources, compared to well-established democracies. Naturally it is not the form of the NGOs that counts but their activities. Many organizations are formally non-governmental but supported or even established by the government, or represent specific political or business interests. Here we discuss the activities of independent civilian organizations specialized in the protection of informational rights.

As Szekely observed[108], 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.

[104] Annual reports of the Parliamentary Commissioner for Data Protection and Freedom of Information, *ibid.*
[105] Report of Peer Review on Data Protection – Hungary**.** Evaluation mission (peer review) with TAIEX support (2002). Available at https://81.183.229.204:51111/abi/index.php?menu=beszamolok/2002/6/2 (last accessed 18 July 2013).
[106] https://81.183.229.204:51111/abi/index.php?menu=180 (last accessed 18 July 2013).
[107] https://81.183.229.204:51111/abi/index.php?menu=adved_kereses (last accessed 18 July 2013). This link does not work anymore but it proves that such a webpage was working until the abolishment of the office of the Data Protection Commissioner.
[108] Szekely, I. (2008), "Hungary", in J. Rule and G. Greenleaf (eds.): *Global Privacy Protection: The First Generation.* Edward Elgar Publishing Ltd., pp. 174–206.

Conversely, where official supervision is inefficient or nonexistent, NGOs will undertake the missing function of enforcement on their own. 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.[109] 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 hours a day, online counseling, and impact litigation.

Among these litigation cases, the 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.[110]

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

[109] Homepage of the Hungarian Civil Liberties Union, www.tasz.hu/en (last accessed 18 July 2013).
[110] Map of public CCTV cameras in Budapest, http://geospace.hu/map2 (last accessed 18 July 2013).

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.[111] Atlatszo.hu has won more than 60 percent 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. We need to note that both the request and the requested information can be regarded as public information under the freedom of information acts. However, the name of the requester cannot. Unfortunately the system does not allow easy modification in order to mask the identity of the requesters. In a new democracy and a political situation such as in Hungary, this unwanted publicity may deter some citizens from using this online tool.

Nevertheless, freedom of information requests may help citizens in exercising their right of access to their own personal data. A request on when the data protection register will be again available online – a request, which is being drafted at the time of writing – would certainly call the attention of the website's visitors.

[111] Atlatszo.hu – About Us, http://atlatszo.hu/2011/07/01/about-us/ (last accessed 18 July 2013).

LOCATING THE DATA CONTROLLER IN HUNGARY

Introduction

This country profile summary covers the experiences encountered during the researchers' attempts to locate data controller contact details of 31 sites in Hungary. In particular, the examples below are illustrative of the individual researchers' experiences and do not attempt to reflect the practices of *all* data controllers in Hungary. This report also identifies some general trends observed alongside the examples of good and bad practices encountered during the course of this research.

Methodological thoughts

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 levels (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 details:

(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 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. For a lay person it is not self-evident at all that subject access requests shall be submitted with and answered by the latter one and not the Police itself. In the light if the above, one may argue that, on the one hand, the data protection registry aimed at identifying data controllers, as well as its easy accessibility and propagation, has an increased importance; on the other hand, the significance of the data controllers' attention to making their organizational relationships transparent, as well as the existence of mechanisms prescribed by law, or exercised without legal obligation, to help citizens exercising their rights (e.g. forwarding their 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 localised 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 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 analyzing of the websites was much more of a continuous or parallel procedure than separate procedures.

We were supposed to carry out the research as lay persons, like ordinary citizens would usually do it, in the sense that we should have not revealed our affiliation or expertise to interlocutors. Nevertheless, investigations conducted in such a way, pretending to be lay persons, usually ended with limited success. In order to obtain data controller details we often had to highlight that we were exercising our *legal right* to know who the data controller was for a given site. If this was not enough to achieve our purpose, we referred to the legislative basis of our enquiry (in general), which undoubtedly confirmed a certain expertise in terms of what is to be meant by subject access rights and the obligations following from these rights.

Overall impressions

Data controller contact details successfully	24 of 31 cases (75 %)

identified in first round of visits	
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

Findings regarding the online content

As presented above, locating data controller details was most often successful online through browsing the respective organisations' official websites. All of these websites included privacy policies which provided varying degrees of detail on processing of personal data and data subjects' legal rights.

In our subjective standard of evaluation, apart from two exceptions, privacy policies that came under scrutiny contained adequate information about what type of personal data is routinely collected and processed. However, on certain websites this information was provided in a laconic style. For instance, the privacy policy of the online gaming company fails to list the types of data processed. Instead, it declares that "certain personal data including name, address etc." can be processed.[112]

As regards the information provided about subject access rights, we were specifically informed about how and with whom exactly to submit a subject access request only in 5 of the 17 successful cases. However, 4 of these sites belonged to the same data controller which means that only two of the online located data controllers did provide precise guidelines on how to exercise subject access rights [driving license records, passport records, police records, ID card, *(Kozigazgatasi es Elektronikus Kozszolgaltatasok Kozponti Hivatala* – Central Office for Public and Administrative and Electronic Public Services); credit reference check (*Kozponti Hitelinformacios Rendszer* – Central Credit Information System). All of these 5 sites included a form or a template for users to make their subject access requests.

[112] Quoted from the company's privacy policy.

Some private organisations also provided templates but these could not be considered as templates that definitely served for submitting subject access requests, rather "general privacy queries" (e-mail data – Google, Facebook). In the latter cases we supposed that the data controllers received requests for subject access through this general template, since the identity of the data controllers was not questionable, and we successfully contacted the controllers, thus we regarded the controllers localizable. Both service providers informed us that we could request the deletion of our incorrect data, and this could hardly be done without learning which personal data about us were processed by the service provider concerned.

We applied the same supposition for those sites the website of which did not include a template/form for submitting data requests but provided either a specific address to send privacy queries to the mobile phone carrier; online gaming; insurance records; ISP; search engine data, or general contact information *and* specific, detailed references to access rights such as the deadline, costs and methods of this kind of requests (all the rest of the online located data controllers). However, when only general contact details of the concerned institution, organisation or company were available, without adequate reference to access rights, we did not consider the data controller as online localisable. In such circumstances, we turned to them directly by phone, in person or via e-mail.

As a general conclusion, it was difficult to assess the up-to-dateness of the information included in the privacy policies, since data about when these policies had been posted or updated were rarely published. However, we did find evidence of outdated information, due to recent changes in legislation: we found two websites where the information provided referred to the 1992 Data Protection Act – revoked almost two years ago – that is, these data controllers had failed to update their privacy policies according to the new act, which entered into force in 2011.

Although the quality of the information provided on websites ranged from poor to good in the standards of evaluation, we found that the vast majority of the websites we analysed did not provide satisfactory information on access rights, or even if they did, they did not publish them unequivocally.

Several negative practices could be identified in this regard:

- Information on subject access rights in the privacy policy presented in a misleading terminology to data subjects. (Google)
- Incomplete information in Hungarian by service providers domiciled abroad (Google, Facebook)
- "Hiding" information on the rights of data subjects in several different legal statements

In our view, these practices can be considered as strategies of denial of the right of access to data as discussed below.

Findings regarding the attempts to localise the data controller by phone or in person

In the case of data types where online identification of the data controller was not possible or was ambiguous, we made inquiries on the phone and in person. Information provided to our inquiries was vague in all but two cases, where we were given exact and comprehensive information on the parameters of our online and personal data request submission (police records, Central Office for Public Administrative and Electronic Public Services –

(hereinafter: COAES) and CCTV in a national supermarket network). Several times attempts were made to redirect communication to the website or to email, or the staff promised to call us back, instead of providing the requested information. Supposedly, it was due to the lack of information, and the staff might want to discuss the response with a legal expert or a superior. In one case, as it was later found, this technique was just a way of trying to get rid of us [CCTV in a small store]. In four cases we were definitely misinformed at first [ANPR; Europol; CCTV in public space, CCTV in bank]. We were almost always asked for what reason we wanted to access our personal data; as mentioned above, our answer was that because we were curious. When this did not work, we emphasized that we have the right to do so. Finally, in several cases we were informed that we were the first to have made such a request.

Data controllers were finally identified in almost all cases by using several different methods, but many times it required a lot of effort. In the following section those cases are highlighted which we considered as strategies to facilitate or obstruct the exercise of subject access rights.

Public Sector

Strategies of facilitation

We would like to mention as a remarkable strategy of facilitation within the researched government sites the case of the COAES. As an integral organisation of the Hungarian public administration, this Office is responsible for managing and processing data of the central and authentic national registries including, among others, Hungarian ID card, Hungarian independent ID card Holders Register (ID cards), Travel Documents Register (Passport service), Road Traffic Register (driving license records), Criminal Register (police records). Making personal data accessible on request from these databases falls under the scope of the duties of this Office. On its website the Office provides detailed information, broken down by database, on the conditions, channels and deadline of providing data subjects with information about data in different registries. In some registries provision of data may be initiated electronically – upon online identification – with a few clicks. To sum up, apparently the Office strives to provide reliable information on personal data not only to the authorities and courts but to the data subjects as well.

We did not notice any other noteworthy strategy of facilitation or best practice when analysing public sites. However, Border Police should also be mentioned since, even though no information on the availability of personal data processed by the Border Police was available online, and no exact information was provided when we first inquired on the phone, we were contacted within a day as promised, and were informed which data we should provide in our request and who we should address our request to in order to obtain information on personal data related to border control.

Two cases of access request addressed to public schools also deserve mention here. In both cases we contacted the schools using the central telephone numbers provided on their respective websites and asked to whom we could turn to in order to get our personal data as former students of the school. In the first case – a primary school – a person from the secretariat answered our call and asked whether we needed this information (our own data!) in order to organize a class reunion. We said that it was not the case. She then promised to call us back in a few days after she would have found the requested documentation in the

basement, which she actually did. In the other case – a secondary school – the school secretary answered our call and promised to search for the requested data in the school archives. She asked for our e-mail address where she sent a message a few days later, informing us that she had found the requested information, and how could we request a copy of the documents concerned. In both cases, although no information about processing personal data or subject access could be found on the website, the personal helpfulness of the staff was exemplary.

Strategies of denial

Apart from the COAES, the online content of websites of the public sector concerning the information on data protection and access rights in particular should be considered as meagre, and thus as a sort of strategy of denial. With the exceptions of the data managed by the COAES and the National Health Insurance Fund (nationally-held patient health records), websites of the examined sites within the public sector did not mention any information about data protection and access rights.

As to CCTV cameras installed in public areas, operated jointly by the district police and local self-governments on a contractual basis, we could not find any information about the possibilities and ways of access to the recorded images, at least in the district where we conducted our research (District XI of the capital city). On the website of the public area inspectorate we could identify only the physical location of the CCTV cameras; publishing of this information is a legal obligation prescribed by law, which the data controller evidently complied with. [113] In lack of other information we contacted the inspectorate via telephone and asked for guidance on how we can exercise our subject access rights. A lady first informed us that only the police was authorized to access the footage. This information was contradictory not only to the provisions on subject access of the Data Protection Act, but also to the more narrow provision of the act on public area inspectorates. When we called the lady's attention to the fact that we have a right to be informed about the processing of our personal data, she finally concluded that we needed to send our request to the central e-mail address of the District XI public area inspectorate.

Customer service assistants at the state-run motorway management company, which processes ANPR, were confused by our inquiry. During our first call the assistant informed us that the Motorway Management Company did not process personal data. We asked in utter confusion how they can then impose fines for unauthorized road use. The lady was obviously hesitating, recognized her lack of competence and advised us to request information in writing as she was not able to help us. We repeated our call, trying to speak with another customer service assistant. The man who replied our repeated call did not deny that the company does process personal data but he could not inform us about details on subject access rights either. Therefore, we sent an email to the company. The answer arrived three weeks later. It stated that the company had a privacy policy; however, no information on its availability was provided. The reason the letter provided for this was that according to the Data Protection Act the company complied with its obligation to provide information on data processing by publishing a reference to the relevant legislation in force.[114] As the main acts and regulations providing for toll payment and payment monitoring are listed on the

[113] Section 7 (4) of the Act No. LXIII of 1999 on the Maintenance Law and Order in Public Spaces.
[114] Section 20 (3) of the Act No. CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.

company's website and flyers, in their opinion no further information on data processing is necessary. However, by simply listing the rules of toll payment and payment monitoring the company did not comply with the cited provision of the Data Protection Act. According to the act, information to be provided by data controllers shall include *all aspects* of the processing of one's personal data, *including the information on the data subject's rights and remedies*. The letter finally stated that upon identification the company provides information in writing to requests through any channel. Despite of these negative findings, our research had a positive outcome as well: according to the responding letter an extra training on data protection was organized for the customer service staff so that in the future they might be able to provide the necessary information on data processing.

In the case of the Hungarian Europol Unit it was not the Unit's employees who informed us about the processing of our personal data, but we ourselves informed the Unit's employee in this matter. The lady whom we contacted by telephone informed us, not completely understanding our request, that such a request should surely be addressed to the Data Protection Office of the central Europol office. When we asked her how to do this if one does not speak English, she replied that we should make the call together with somebody who speaks English and that this should be easy since everybody has such an acquaintance. Following the telephone conversation we visited the Europol website the privacy policy of which made it clear that such requests should be submitted to national units, in national languages. We called the lady again who was now willing to give the contact details of her superior, where we could request access to our personal data.

Private Sector

Strategy of facilitation

In general, we could not identify best practices in the private sector organizations examined. Private companies seem to have different standards as regards the quality and quantity of information about access rights and data protection in general.

Based on the assumption that non-professional data subjects are not necessarily aware of the *legal right to access* their personal data, i.e. that they actually *exercise their legal rights* when asking for information, we paid special attention to whether or not this is reflected in the wording and terminology of privacy policies. In other words, we examined to what extent privacy policies made it clear that access to one's own personal data as a right results in an indisputable obligation on the controller's side, i.e. the controller cannot deny such requests. With this in mind, the overall impression was positive as several privacy policies made it clear that everyone has the right to access their personal data and consequently the controller shall provide those data and cannot decline requests.

> "A Felhasznalonak jogaban all, hogy tajekoztatast kerjen a regisztracio soran kezelt szemelyes adatai allomanyarol" / "User has the right to request information on user's

personal data processed by controller." [115] [Insurance records] (translation and emphasis added by authors).

"A SuperShop koteles a kerelem benyujtasatol szamitott legrovidebb ido alatt, legfeljebb azonban 30 napon belul irasban, kozertheto formaban megadni a tajekoztatast." / "Upon request from card holder SuperShop shall provide understandable information in writing as soon as possible within 30 days of submission of the request."[116] [Loyalty card scheme for a supermarket (translation and emphasis added by authors)]

"A kerelemben foglaltaknak megfeleloen minden esetben reszletes tajekoztatast nyujtunk a kezelt szemelyes adatokrol, az adatkezeles celjarol, jogalapjarol, idotartamarol es az adatkezelessel osszefuggo tevekenysegrol." / Whenever requested, we provide detailed information on the personal data processed, the purpose, the legal basis and the duration of data processing and activities related to data processing." [Search engine (translation and emphasis added by authors)]

"A felhasznalok barmikor irhatnak nekunk annak erdekeben, hogy adataikrol tajekozodjanak, azokat megvaltoztassak, a nalunk tarolt adatokrol masolatot kerjenek, illetve azokat modositsak vagy kijavitsak (...) torvenyben biztositott jogaik ertelmeben".[117] / Customers can write to us at any time to review, change, obtain a copy of their personal information or have your details altered or corrected in accordance with their rights." [Online gaming (translation and emphasis added by authors)]

Consequently, we deemed it a good practice that privacy policies of the investigated sites within the private sector made it clear that when requesting information on managing personal data, data subjects do not ask a favour but exercise a *legal right*.

Strategies of denial

In direct contradiction to the above detailed practice, the terminology of Google's privacy policy suggests that accessing personal information is not a legal right but a *favour*, *a courtesy* that on Google's side depending upon their intentions and capacities:

"Arra torekszunk, hogy On minden esetben hozzaferhessen szemelyes adataihoz, amikor igenybe veszi szolgaltatasainkat." / "Whenever you use our services, we aim to provide you with access to your personal information."

"Amennyiben az ilyen szemelyes adatai tevesen szerepelnek rendszerunkben, igyekszunk lehetoseget teremteni arra, hogy On ezeket a teves adatokat mielobb frissithesse vagy torolhesse." / "If that information is wrong, we strive to give you ways to update it quickly…"

[115] Quoted from company's privacy policy.
[116] Quoted from company's privacy policy.
[117] Quoted from company's privacy policy.

> "Ha biztositani tudjuk az adatokhoz valo hozzaferest es az adatok helyesbitesenek lehetoseget, akkor ezt dijmentesen tesszuk, kiveve, ha ez aranytalan erofeszitest igenyelne a reszunkrol." / "Where we can provide information access (…), we will do so for free, except where it would require disproportionate effort."[118] (Emphasis added by authors)

It is a shortcoming of the Hungarian content of both Google and Facebook regarding data processing that even though the full text of their privacy policies are available in Hungarian, sites that direct users to sub-sites where the data controller may be contacted – in order to access personal data, etc. – are only available in English, and the form one has to fill in is also in English.

During the course of the research we had a deepening impression that the success of localising data controllers heavily depends on the requester's knowledge about the publication practice of the organizations concerned. For example, we found the information relevant for our research in diverse legal notices: in the case of the CCTV in a bank, such information had to be found in the "General Contractual Provisions" (Altalanos Szerzodesi Feltetelek". Moreover, the ISP company published its privacy policy under the title "Jogi kozlemeny" ("Legal notice") at the bottom of the webpage, while the insurance company rightly posted its privacy policy under "Adatvedelem" ("Protection of personal data"). However, in this case the information about subject access could be found under the misleading title "Adatbiztonsag" ("Data Security").[119]

The most remarkable strategies of denial in accessing data controller details were found when analysing the CCTV sites. We conducted an online examination of CCTV sites run by private companies, and we only found information on video surveillance in the business rules of the bank. However, even here there was no information about the right to access personal data. Taking into consideration that the business rules practically copied the provisions of the Personal and Property Protection Act on data processing of video recordings,[120] it is conspicuous that the rules do not contain the provisions of the same section of the act on participation rights. The obligation to place a warning sign about electronic surveillance in a clearly visible place is incorporated in the rules, but provisions on data requests are missing. On top of this, the branch of the bank was the only one of the five CCTV sites we personally visited where there was no signage or written warning about surveillance. To our personal inquiry the bank assistant – after a 15 minute discussion with her colleagues – gave the incorrect information that the Personal and Property Protection Act governing their operation contains provisions different from those of the data protection act, and we have no right to access the recordings. However, the Personal and Property Protection Act in fact guarantees

[118] http://www.google.com/intl/hu/policies/privacy/ (last accessed 12 December 2013).

[119] This observation shows that the situation has not changed much in this regard since 2005, when a study was published on the analysis of privacy notices on websites of Hungarian data controllers. According to the findings of the study, privacy notices were published, among others, under the following titles: "Data protection", "Our data protection principles", "Data protection statement", "Data protection aspects", "Declaration on the protection of personal data", "Disclaimer", "Terms of use", "Home regulations", "Legal notice", "Rights and data protection", "Rights", "Help", "Customer service". (Laszlo, G., 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, 2005.)

[120] Act No. CXXXIII of 2005 on Personal and Property Protection Activities and Private Investigation.

the right of data subjects to access data with reference to the Data Protection Act,[121] so we were misinformed by the assistant.

At this point we thought that it would not have made sense to struggle with her any longer as she evidently had no expertise on the matter, similarly to the head of the security guard she discussed the case with, so we asked her for contact details on how and with whom to submit our request for more information about subject access rights. She gave the instruction to call the call centre of the bank which we followed. The staff member of the call centre directed us to the website where we started our research with limited success. Since here we did not find specific information on subject access rights but only a template for submitting our general query, as explained under the heading of the methodological thoughts, we concluded that the data controller could not be localized. Since the assistant provided us with the incorrect information after having consulted with her boss, we did not deem paying a repeated visit reasonable.

We were able to find the contact details of the CCTV controller in a supermarket in the first round of visit by getting surprisingly accurate information from the security guard on site. We do not exaggerate when saying that he answered our request as he would face this question every day. While he provided precise information of the way to access the camera footage, he was however not sure whether we may access the footage "just because we want" and he assumed that we should define not only the date and time of our presence but also the reason that would legitimise our request. Since this question can be regarded controversial in the light of the legal environment in Hungary, we concluded that we had been adequately informed by the guard and the data controller could be localised. The CCTV sign at the door, however, did not contain any contact information.

Things went less smoothly in the case of the local store and transport CCTV. As for the local store, first we did not find the CCTV sign because it was not placed at the entrance door as usual, but under the pay desk. The employees there had no idea about access rights. One of the employees decided to call his boss who also had no clue about the information we were seeking. We were asked to give our phone number to the staff with a view to getting a call back later, but we did not get a call in the next two weeks, so we returned to the store (second round of visit) where the same scenario happened (apart from calling the boss which did not happened again). Since the CCTV sign did not include any contact information, and we were not called back later either, we concluded that the data controller could not be localised. We concluded that it is not reasonable for anyone to visit a store three times in order to find out who the data controller is and how to get in touch with it. In the case of the transport company, the employee at the call centre was ready to inform us about whether video surveillance was applied on the buses, however, he could not give information about how to access the footage. He informed us that all passenger requests should be submitted through a central e-mail address, consequently access requests should also be submitted there, since he has no information about specific possibilities.

CCTV and signage

We examined the circumstances of video surveillance at all CCTV sites in person. Out of the five sites we found signage calling the data subjects' attention to camera surveillance at four sites (the odd one out was the above-mentioned bank). In contrast to the UK practice there

[121] Section 28 (2) point e).

was no site where general information or contact details of the data controllers had been published together with the signage. Therefore we had to contact somebody personally at each site. In our view, this practice makes the success of localizing data controllers dependent on the willingness and preparedness of the personnel at the sites.

The installation and use of CCTV in Hungary are regulated by sector-specific laws. The relevant rules regarding the use of CCTV in public spaces can be found in the Police Act,[122] the Act on Public Space Supervision,[123] and the Passenger Transport Services Act. According to these acts it is mandatory for data controllers to inform citizens about the use of video surveillance cameras by well-visible notices. The act does not determine legal requirements for what should be included in these notices (i.e. the identity of the data controller, contact details).

The regulation concerning other CCTV sites examined in this research can be found in the Personal and Property Protection Activities Act[124] and the Passenger Transport Services Act.[125] Although these Acts also fail to determine that identity and contact details of the data controller shall be included *in the CCTV signage*, they do prescribe however, precisely what information shall be made available for data subjects. Warning or information sign must be posted in a clearly visible place, written in an easily understandable fashion to convey useful information about the use of an electronic surveillance system, the purpose of surveillance using electronic security system and sound and video recording facilities containing personal data, and the purpose for which these data are processed, including legal authorization for processing, the place where the recordings are stored and the period of storage, the person operating the system, the persons authorized to access these data, as well as the provisions of the Data Protection Act concerning the rights of data subjects and the procedures for enforcing such rights.

CCTV notice in a supermarket

("Area controlled by cameras connected to the

CCTV notice on a bus

("Area under camera surveillance" – in English: *"Security cameras in*

CCTV notice in the underground

("Area under camera surveillance" – in English: *"CCTV in operation")*

[122] Section 42 of the Act No. XXXIV of 1994 on the Police.
[123] Section 7 Act No. LXIII of 1999 on the Maintenance of Law and Order in Public Spaces.
[124] Act No. CXXXIII of 2005 on Personal and Property Protection Activities and Private Investigation.
[125] Act No.XLI of 2012 on Passenger Transport Services.

police") *operation")*

Concluding thoughts

On the basis of our experience accumulated during the course of this empirical research we hypothesize that the localizability of the 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, 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[126] 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.[127]

We believe that conducting similar empirical researches, and publishing of their findings, could promote the establishment of standards of accessibility of such information. The research findings may be helpful both for the data protection supervisory authorities and the data controllers themselves. A tangible consequence of our inquiry at the ANPR site was that, triggered by our inquiry, special training on data protection has been organized for the customer service staff, as we were informed in a follow-up letter from the company.

[126] 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.

[127] 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).

SUBMITTING ACCESS REQUESTS IN HUNGARY

Introduction

This report describes, analyses and summarises the experience gathered during the empirical research conducted in Hungary from September 2013 to January 2014. In this period the researchers submitted 19 subject access requests to a wide range of data controller organizations 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, including methodological notes, 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 do not only summarize their findings but also identify some possible outcomes of their research, and formulate suggestions for practically utilizing the findings of this research at the national level, and for improving the level of enforceability of the right of access to one's own personal data in general.

Methodological issues

The subject access requests were submitted by the researchers in their own name. Involvement of third persons was necessary only in one case: one of the access requests was delivered to the Ministry of Public Administration and Justice where entering the building is restricted to those who already have an ongoing official affair with the ministry. However, a relative of the researcher was working in the ministry and he could arrange entry into the building. Nevertheless, in order to avoid compromising the research results by revealing the relationship between the researcher and the relative, the researcher entered into the building together with a third person who then submitted the access request in her own name.

Similarly to the first phase of this research (aimed at locating data controllers), researchers attempted to carry out the research as lay persons. Accordingly, researchers submitted their access requests the way ordinary citizens would do so, i.e. they did not reveal their affiliation or special expertise to the addressees. But even so, they had to show some knowledge of subject access rights anyway when referring to the legislative basis of access rights in the data requests. Moreover, when a data controller's response was not in compliance with the law, in order to achieve an adequate reply, the researchers undoubtedly confirmed a certain expertise in terms of what is to be meant by subject access rights and the obligations following from these rights in their subsequent responses.

The danger exists of detecting the real identity of the researchers who try to pretend that they contact the data controllers as laymen or ordinary citizens. This is the case in particular in countries where the number of privacy/data protection experts is limited, their professional profile is well-known or easily accessible online, and in organizations where the number of subject access requests is low or such requests are exceptional. Hungary is a small country where there is only a dozen or so high-profile experts (professors, consultants or advocates) specialized in issues of privacy and data protection, including the two researchers who participated in this empirical research. One of them (Beatrix Vissy) has a name of which only one exists in the country, according to the central population register, and her professional profile is easily accessible through the internet, along with the projects she has participated in, and the research and advocate organizations she is affiliated with. The other researcher

(Ivan Szekely) is also easily identifiable since he is one of the founders of the newly democratic legal and institutional framework of informational rights in Hungary, and he has a long record of publishing, teaching and acting as consultant in the area of data protection.

In one case, the contact person from the data controller organization openly admitted such identification when saying "*I googled you, and I know that this is not a 'simple' data request"* (CCTV in large department store). Nevertheless, in cases where the identification of the researchers was not explicitly admitted, but the subject access requests were exceptional or even surprising in the practice of the organization, the easy identifiability of the researchers might seriously influence the organizations' response. Even in the public sector, where organizations have a well-established procedure of handling citizens' requests, including subject access requests, the possibility that department leaders, especially when receiving repeated requests, checked the identity of the learned requester who seems to have been educated in data protection law, cannot be excluded either. This possibility may distort the findings of the research, and the researchers are sceptical of whether they are able to draw well-grounded conclusions from these responses regarding the normal procedure of handling such requests. However, it may equally be argued that even in cases where there was no explicit recognition of the requester's status as a researcher, the easy identification of the requester may well have influenced the response of the data controller in a positive way. As a result, the case summaries in this report may in fact hide some even poorer practices than those identified in the research.

Although based on empirical research, several of the findings below – besides being compared to subjective standards – can be regarded as speculative. This partly follows from the ambitions of the research, which extended beyond simply describing factual experience and identifying certain trends: its aim was to analyze and evaluate data controllers' attitudes and strategies. This means that this report draws conclusions on processes which the researchers could not observe themselves, thus the conclusions could be drawn only on the basis of "reflected images", i.e. the responses given to subject access requests. The authors, however, made every effort to ground these speculative findings on rational assumptions based on data controllers' responses.

Overall summary

As listed below, in September and October 2013, 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).

	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

	Site	**Data controller**
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

Table 1. List of addressees of subject access requests

Each access request contained requests for providing specific personal data being processed; the date of recording that data, the legal basis and aim of processing the data; information about which of the requested personal data had been shared with exactly which third parties; and, if using automated decision making in the processing of personal data, then how this was applied. In the case of CCTV surveillance, researchers requested the CCTV footage itself.

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		

Table 2. Main qualitative findings

In *Table 2* above 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.

Access requests did not always find their way in the first attempt. In cases when the researchers tried to contact data controllers which had not been successfully located in the first phase of this research, the requests were addressed to a wrong site. This fact reinforces the anomalies found in the first phase of the research. In such cases the more proactive data controllers forwarded the requests to the competent data controller organization (district office of the government authority of the capital city; CCTV in a government building), in other cases the requester was only informed about the identity of the real data controller (Microsoft Hungary; CCTV in public transport setting). Since the researchers interpreted the latter two cases as strategies of denial, these will be analyzed in detail in further sections of this report.

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. The decided manner of the requesters and threatening with a complaint to be submitted to the data protection supervisory authority also had a positive effect on the willingness of data controllers to fulfil the access requests (banking records).

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, referring to concrete legal provisions by the researchers 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 the requester's position and changed its earlier decision. The attitudes and procedures of the multinational companies again constitute a special category: here the researchers 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. (It deserves mentioning that in Hungary there are around a thousand laws and legal regulations which contain provisions regarding the processing of personal data in various domains.)

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.

Case by case analysis

Public sector

In the public sector the researchers submitted access requests to five data controller organizations from different domains: a local government office, the central office for

electronic public services, the state-owned organization for controlling motorways, the international criminal cooperation unit of the national police, and the national office of the Schengen information system.

General impressions

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. Since the requested data belong to the core business of the contacted organizations, and the organizations seem to be well-trained in such cases – in addition, they do not regard the requested data "personal" in the general sense of the notion as defined in the data protection law, instead as data the handling of which is clearly regulated by the laws and internal orders regulating their specific activities –, therefore administering the requests did not require special efforts from these organizations.

This request-handling routine of the public sector organizations also resulted in offering facilitative means to the requesters, such as downloadable forms for requesting information, and in most cases this was accompanied by a higher level of preparedness and legal knowledge – not in data protection law but 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.

<u>Public – Facilitative Practice</u>

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

In the first – and perhaps the most informative – case the researcher requested his personal data related to his ownership of motor vehicles from the district office of the government authority of the capital city. The request included the date of recording the data, the purpose and legal grounds of processing the data, and the expected date of deleting the data, as well as detailed information on which personal data have been forwarded to which third parties, and for which purpose. The office responded in writing (in ten days, well within the deadline of 30 days defined in the data protection law), informing the requester that his 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 a notice to the requester calling him to pay a sum of HUF 1.650 (cca. EUR 6) as administrative service fee, in order to process his request. The researcher paid the fee by postal order but failed to send the copy of the dispatch note as

requested by the department.[128] Instead, he sent another letter to the department, repeating his original subject access request, and explained his position, according to which demanding an administrative service fee was unlawful and against the provisions of the data protection law. He 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. Although in the meantime the department informed the requester about the termination of the case by reason of missing the deadline of sending the dispatch note as proof of paying the fee (the mailings evidently crossed each other in the post), the 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 the requester in which she included two, interrelated decisions. The first decision annulled the termination of the case, the second decision ordered the re-payment of the administrative service fee the actual paying of which she had double-checked in the internal financial system of the authority. In the explanation the head of the superior department confirmed that in such cases the provisions of the data protection law apply, and demanding the fee was unlawful. In addition, she regarded the repeated request as an appeal in the legal sense, which also has an appeal fee (HUF 3.000, cca. EUR 11) that is higher than the originally demanded administrative service fee, but it would have certainly been absurd to order the reimbursing of the original fee at the expense of a higher fee, thus she also waived this obligation in her decision. In sum, the office accepted the requester's position, changed its decision, and re-paid the unlawfully demanded fee. 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 the researcher's criminal personal data from the national headquarters of the police, submitting the request and receiving the response was a seamless procedure. The researcher limited his request to criminal personal data processed by the police in the period from 1 September 2012 to 1 September 2013, excluding the data pertaining to prior criminal convictions, since such data are processed by the COAES. The request was sent to the office of the national police headquarters. The head of the office responded to the request, informing the requester that he 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 the requester's person had been processed in the given period.

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 included all personal data of the researcher processed in the criminal

[128] A copy of the dispatch note is generally required by the authorities as a direct proof of paying postage fees, although authorities are naturally able to find the paid fees in their accounting systems, as shown in the following. As such, sending a dispatch note should not be deemed as crucial in terms of completing the postal process.

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 three weeks and called the requester to furnish additional personal identification data (mother's maiden name, date and place of birth) which the requester provided by return of mail. A few days later a short reply arrived from the same department head, according to which no data about the requester were processed in the criminal registration system; however, information about forwarding the requester's data to third parties would be sent in a subsequent letter, since investigation in this matter was under way.

More than a month later the requester sent a letter asking when could he expect the promised additional reply about forwarding his data to third parties, and if no data about him 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 the requester that his 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 the requester wanted to know what sort of data forwarding about him took place in the five-year period from 25 September 2008 to 25 September 2013. 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 personal data of the requester forwarded to third parties in 19 cases during the five-year period, indicating the exact types of data, the dates and the legal grounds of forwarding.

ANPR

A request about the researcher's 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 the requester was informed that no data about her were processed in the ANPR system, nor about the car she indicated in her 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 two years after the termination of the case. Since the requester had no such incident, her data were not stored in the system. The letter also indicated the legal references relevant to the case.

Border Control – Schengen Information System

The subject access requests submitted to the international criminal cooperation unit of the national police, and to the national office of the Schengen Information System resulted in fast and efficient replies. In the first case the director of the international criminal cooperation unit of the national police informed the requester just one day after receiving the request that in the previous year the International Criminal Cooperation Center did not process personal data about her. 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. The researcher submitted such a form to the competent authority, the government authority of the capital city. The form contains personal identification and contact data only since the subject of the request submitted this way is standardized. 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 the requester in a letter that according to the examination conducted on 8 October 2013 no data or warning about the requester was processed in the Schengen Information System.

In all the five above cases the procedure was adequately simple and understandable for an average requester. As noted earlier, the public sector organizations have an established organizational structure and procedure for handling citizens' requests. In particular the police and the offices of the Central Office for Public Administrative and Electronic Public Services (COAES) seemed to have such a routine. As to the preparedness of the substance of the subject access requests, most of the officers were well educated in the matter, consequently the responses were in compliance with the law. Two cases deserve special mention in this regard: in the first case the lower level decision (requesting an administrative service fee) was unlawful but the superior of the department annulled the wrong decision; in the second case the criminal records authority either misunderstood or over-performed its duties and forwarded the request to the population register, too. In both cases, however, the requester received the requested (or even more) personal data. The balance of power between citizen and data controller was adequate in all the above cases; the State Motorway Company added some extra courtesy to the process and furnished additional information about the operating of the ANPR system.

<u>Public – Restrictive Practices</u>

No significant examples of restrictive practices were found in the public sector in the course of this research when requesting non-CCTV data.

Private sector

General impressions

In the course of the research, the researchers 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 the researchers' access requests, others showed strongly or relatively restrictive practices.

Private – Facilitative Practices

Loyalty card (transport)

The researcher made a request to access her personal data relating to her loyalty card on 19/09/2013 to the company via e-mail by writing to the data controller's general contact address as she had been advised when attempting to locate the data controller's contact details. 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 hours. 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 on 07/10/2013, many days before the 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 collected and generated personal data, the company also informed the researcher 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 the researcher's personal data had been disclosed. As explained in the letter, personal data relating to the researcher's loyalty card have 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 the researchers' subjective standard of evaluation, the data controller showed a particularly high degree of facilitation of subject access rights when looking at the full sample of responses to data requests. 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 the researcher 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, Shell performed such an accurate, efficient, but also simple processing of access requests that is exemplary compared to all other data controllers in this research.

Private – Restrictive Practices

Mobile Phone Carrier

The request for mobile carrier data was sent on 18/09/2013 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 the researcher asked the

company to provide all her personal data generated at the data controller in connection with her mobile phone use (including locational information) between the period of 01/03/2013 and 01/09/2013. Since this site presented the most exhaustive and absurd explanation of the reasons why the data request was – partly – rejected, this case deserved to be described in detail.

Due to certain postal delivery anomalies described below, the response letter to the request dated on 1/10/2013 only reached the researcher on 27/11/2013. It turned out that the reply had been sent not to the current mailing address of the respondent 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 made an inquiry to the requester by telephone. (A similar thing happened in the case of the request for banking records, too, however, the bank did not show such a proactive approach, therefore for a longer period it was not clear that the bank had responded to the request.)

The envelope included a list of calls made on the researcher's cell phone within the period specified in the access request and a response letter. The letter stated that the researcher could find attached her call itemization, however, the company was not in the position to provide the requested locational (cell) information. It also declared that none of the researcher's personal data has been shared with third parties, and addressed that the company does not use automatic decision making process. The explanation of the grounds for denial of the requests to access cell 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:

As the legal basis for the denial of the claim, 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 data controller's DPO, 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, for what kind of data management purpose and for how long is managed by the service provider. According to the letter, the 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 by the letter 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 the researcher appear as a person exercising its right 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 data protection officer "*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 the researcher about the uselessness of cell information with the argument that these technical data do not allow the exact localization of cell phones.

The researcher replied to the letter on 14/01/2014 in a long response demanding access to all the undisclosed information (cell information, internet traffic data, list of incoming calls). She explained that in her 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. The researcher 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). The researcher also added that she wanted to have a reply within seven days with a threat to make a complaint to the NDPA if the request will be rejected again.

Shortly thereafter the researcher received a response letter explaining that despite all the arguments explored 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 the researcher's request, the data protection officer agreed to continue the legal dispute before the NDPA. Accordingly, on 5 March 2014 the researcher initiated an investigation of the NDPA pursuant the Data Protection Act[129] alleging that the company had infringed her right to access her own personal data.

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

Given the fact that company has paid much attention to the researcher's request by processing it in a timely and professional manner, performing also proactive steps to fulfil it (phone calls were made to locate the researcher when the postal delivery of the response failed), and that the company did actually fulfil it to a restricted extent, demonstrate that the company basically has not questioned subject access rights.

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 two months), at the time of closing this manuscript (9 May 2014) no response has yet arrived to the researcher's complaint from the NDPA.

Facebook, Google and Microsoft

Certain multinational companies, such as Facebook, Google and Microsoft are frequently characterised by low performance in good practices regarding privacy rights. As our findings illustrate below, these organizations did not refute this perception in the course of the research. Following the instructions of our agreed research proceedings, requests to multinational companies were sent in the researcher's native language (i.e. in Hungarian) on 13/10/2013. To those organizations which had a national office in Budapest, namely to 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 the researcher could not provoke any reaction from these companies to her requests despite repeated submissions. In the case of Google, the researcher's attempts to get in touch with the national office (Google Budapest) have failed twice, both ordinary letters she sent have been returned with the notice that "*the recipient has not taken delivery*". (The second letter was sent on 27/11/2013 and returned on 11/12/2013.) In order to succeed the submission of the request, the researcher browsed the Internet (forums, blogs) to seek more information on Google's local office and to find out whether anybody has ever successfully contacted with a living person from there. The researcher found several angry comments on this topic complaining bitterly that contacting Google Budapest is virtually impossible.[130] 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, the researcher exactly knows what happened to her letter, in the case of

[130] http://www.gyakorikerdesek.hu/szamitastechnika__internet__256973-hol-talalom-a-google-magyar-email-cimet The researcher also found an article discussing the infrastructure and actual functioning of the local department. According to this article: "*One boss, four employees, fifty square meters – this is the local garrison of the coolest company of the world. (...) Google Budapest Ltd. is situated on the fourth floor of the Obuda Gate office building, functioning almost in secret, so that even the company's name has not been written at the entrance*." See Kis orszag, kis Google ('Small country, small Google'): http://index.hu/tech/2009/10/14/kis_orszag_kis_google/ (Last accessed on 27 January 2014.

Facebook, the fate of the letters is unknown; the researcher does not even know whether they have reached their addressees or not.

Microsoft showed a somewhat more responsive attitude than its counterparts, however, the researcher's attempts to gain access to her personal data relating to her Skype account have also failed, at least in the way the researcher wanted to. As stated above, the data request to Microsoft was sent on 13/10/2013 to the national office (Microsoft Hungary). One month later (one day after the expiry of the 30 days deadline) the researcher received a very short letter in return, informing her that Microsoft Hungary has not been controlling her 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, the researcher was advised to turn to the Skype Customer Support. Accordingly, the researcher submitted the request to the Microsoft Customer Support. On the day of submission, the researcher 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*." Taking into consideration that the specific aim of this research with submitting data requests to Microsoft and other multinationals from various countries was to test how these companies handle data requests formulated in different languages of states in which they provide their services, we decided not to submit our request in English.

As it can be seen, the fact that Google and Microsoft maintain offices in Hungary, did not help the researcher in any way access to her e-mail and Skype data, and did not make easier to communicate her access request in her mother tongue.

Advanced Passenger Information

By contrast, the national office of the airline to which we submitted our request for advanced passenger information data willingly helped the requester in receiving 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 23/09/2013 at 6:03 a.m. via e-mail, and was answered in two hours, at 8:06 a.m. This e-mail informed the requester 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, the requester was recommended to contact the Security and Data Protection Department of the company; contact details thereof were also provided.

Since the researcher wanted to receive further information about the data processing (exact legal grounds of processing, legal restrictions etc.), she turned to the given department in a letter on 10/10/2013, which, having received no reply, she sent again on 27/11/2014. 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

One of the subject access requests submitted to private sector organizations was addressed a major commercial bank belonging to an international network of financial institutions. The letter sent by one of the researchers on 26 September 2014 both by e-mail and ordinary mail contained requests regarding the researcher's personal data relating to his person and his banking card in the period of one year preceding the access request, the date of recording the data, the purpose and legal grounds of processing the data, and the expected date of deleting the data, as well as detailed information on which personal data have been forwarded to which third parties, and for which purpose.

An automated e-mail reply arrived almost in the same minute, acknowledging the message, and promising a substantial response within three 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 shows that data controlling 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 the bank accounts of the requester and the general types of data processed in connection with such accounts,

– listed in detail the personal identification and communication data of the requester,

– 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 the surprise of the researcher, another reply arrived a few days later from the branch office where the researcher has bank accounts, signed by two advisors of the bank. The letter informed the requester that the processing of the request had begun, however it was “not identifiable” what kind of data the requester wanted to access. Therefore the requester was advised to turn to the branch office of the bank personally at his earliest convenience (the researcher did not do so, because he did not want to reveal his “double identity"). 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

In the last case the researcher 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 the researcher moved to a new address (which she indicated in the request), the reply had not arrived to the requester. After a long investigation by the researcher through telephone in order to learn the reasons of non-response to her request, the bank eventually found the undelivered letter and promised the researcher that they would re-mail it to the correct address. However, the letter has never reached the researcher.

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

CCTV

General impressions

The handling of access requests submitted to public and private sector entities in the area of CCTV surveillance made ambivalent impressions on the researchers. Whilst the purpose of the relevant sector-specific laws appear 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. Denials of subjects' equal access to video recordings, even if these denials were not or not clearly unlawful, appeared to violate the principle of informational equality between the data subject and the data controller.

The presence and quality of CCTV signs and privacy notices

The present research pointed out that, from the perspective of the subjects exercising their access rights, the possibility to swiftly identify and localise data controllers, including the disclosure of the policy for handling subject access requests, are of utmost importance in the case of CCTV footages. It 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. (This was experienced first-hand by the researchers when trying to access CCTV footage taken in public space – this case

will be analysed below in detail.) With this in mind, the presence and quality of CCTV signs will be analyzed below in a separate section.

For a citizen wishing to make a subject access request, it probably raises problems that 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. This is partly because in certain areas of CCTV surveillance, lawmakers have failed to enact particular provisions for what should be included in the CCTV signage. 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 processing of personal data, data controllers did not fulfil this legal obligation.

The Police Act and the Act on Public Space Supervision, which had relevance when researchers examined CCTV surveillance in one government building (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.). Naturally, it is not self-evident that in the absence of specific legal provisions data controllers are not expected to facilitate the enforcement of subject access rights by providing more information than a sign indicating the operation of CCTV. However, the researchers did not encounter a single practise that would have met any degree of the requirements of facilitation in this regard.

In contrast to the above mentioned laws, 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, take-off 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

Opportunities to realise subject access rights were even more undermined by the fact that oftentimes CCTV operators could not provide accurate information on CCTV footage disclosure procedure (CCTV in public space, CCTV in public transport setting, CCTV in a bank). Showing such ignorance might discourage one's further attempts to access personal data, especially in case of non-professional data subjects who are not necessarily aware that they actually exercise their legal rights when asking for information. Things got worse when the 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).

However, in one case a well-seen improvement deserves mentioning here: A few weeks after the researcher's data request for transport CCTV footage had been denied by the company operating the service (see below under '*CCTV on public transport'*), the company posted a new kind of warning sign in its transport settings containing information about the identity of the data controller and the applicable law (however, the contact details of the controllers or information about the rights of the data subjects were not indicated on the signage). The researchers could not be sure that this was a direct implication of their correspondence with the company, but the coincidence in time suggests that this was one of the possible achievements of the research.

New CCTV warning sign on a bus

"CCTV in operation.
Surveillance is conducted to protect persons, valuables and the condition of the vehicle in line with Act XLI of 2012 on Passenger Transport. Audio and video recordings are stored by the operator of the vehicles… in the manner and for the time period specified by law."

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 the researchers in their attempts to realise their 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 the researchers do indeed have legitimate rights to gain access to their personal data. However, two issues constituted

subjects 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 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 the fulfilment of data requests were basically influenced by the question of how the fulfilment of the request would affect the rights of third parties. (CCTV in a large department store, CCTV in a bank) 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 keep 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 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. To give two examples:

The Personal and Property Protection Act, which is to be applied to the banks, and to one of the researched government building, stipulates:

Any person whose right or lawful interests is prejudiced by any sound and/or video recording, or by the recording of any of his personal data may (...) request within three working days or within thirty or sixty days, respectively, following the date when the sound and/or video recording or the recording of any of his personal data was made, by providing proof of the said right or lawful interests, the processor of such data not to abolish or delete the data. At the request of the court or another authority the sound and/or video recording or the recording of personal data in question shall be sent to the court or authority without undue delay. [emphasis added by the authors]

The Condominiums Act, the scope of which one of the researched CCTV sites (CCTV in a large department store) extends to, declares:

Any person whose right or lawful interests is prejudiced by any recording made by the video surveillance system may request within fifteen days following the date when the recording was made, by providing proof of the said right or lawful interests, the processor of such data not to abolish or delete the data. At the request of the court or another authority the recording shall be sent to the court or authority without undue delay. If the request is not submitted within thirty days from the day when the request for refraining from the abolishing procedure was made, the video recording must be erased permanently without delay, without any possibility of recovery. [emphasis added by the authors]

Based on the conventional legal formula ("providing proof of the said right or lawful interests"), several data controllers expected the researchers to confirm their 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; researchers were also supposed to demonstrate the initiation of an administrative or court proceeding in order to obtain the recording. As for the statutory interpretation, in case of possible conflicts between a specific and a general rule, the former is to be seen as a derogation of the general rule. However, in our view, it is doubtful whether there is inconsistency between the particular statutory provisions referred to above and the general Data Protection Act. If lawmakers want to repeal a general rule by enacting a particular one, they need to be explicit in this regard, otherwise the general rule is not allowed to be ignored. As a matter of fact, the relevant sector-specific laws are particularly confusing in this respect, especially if examined at system level: most sector-specific laws contain an explicit reference to the rule that CCTV surveillance may only take place if observing data subject's rights set out in the Data Protection Act. However, these acts do not converge in terms of which act should apply to access rights of the data subjects (i.e. which act shall supersede the other one). Two examples to demonstrate the inconsistencies explained above:

(a) according to the Personal and Property Protection Act:

The security guard shall be authorized to make - and process - sound and/or video recordings through an electronic surveillance system within the framework of the Contract laying down provisions for his obligations, for the purpose of discharging his contractual obligations, in due observation of the provisions of the Data Protection Act pertaining to data protection, and the limitations set out **in this** Act. [emphasis added by the authors]

(b) whilst the Condominiums Act contains the following provision:

Where the data subject shown on the recording is a natural person, he/she shall be able to exercise all relevant rights afforded under the Data Protection Act, taking into consideration the restrictions specified **therein**. [emphasis added by the authors]

3. *Restrictive vs extensive interpretation of the right of access:* Some CCTV operators (Cf. the cases of CCTV in public space, CCTV in a government building) did not share the view that researchers 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 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 the researchers' access requests. Therefore, in almost all cases, the researchers 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. However, these legal uncertainties were not solely the reasons of limited success of the access requests.

Case by case analyses

CCTV in a government building

The researchers selected two different government buildings as addressees of their subject access requests. The requests were sent on 25/09/2013 in both cases. In the case of requesting CCTV footage from the Ministry of Public Administration and Justice, the researcher sent her claim to the Department for Social Contacts being responsible for correspondence with civil society. On 02/10/2013 the researcher was 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, on 09/10/2013 the researcher received a response from the Reserve Police Force. The reply contained the whole range of the information the researcher 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 on 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, the researcher's 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 – Budapest No. 1, the researcher has been granted the opportunity to see the record. The researcher received a reply to her request on 03/10/2013 from the Head of the Office. The letter stated that the Office had got in touch with the NDPA in order to answer the question of laws 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."*

As can be seen, access request procedures related to government buildings basically went smoothly. After the submission of requests there was no need for any interaction on the part of the researcher to gain satisfactory information on data processing both in quantitative and qualitative terms. Replies were delivered in a timely fashion and a professional, exemplary manner. The detailed response letters (2-3 pages in length) covered not only the information requested but also the description of the way in which requests are processed (forwarding it to the competent body, consulting with the NDPA). Although neither organization let the researcher receive a copy of the CCTV footage, both of them provided plausible and legal argumentation supporting this decision. By doing so, these public entities demonstrated not

only transparency but also willingness to have their performance measured (accountability). True enough, the degree of facilitation in the area of access rights was not at the same level in the case of the two data controllers. While the Office of Land Administration turned to the NDPA for consultation, and provided access to the recordings for the data subject, the Reserve Police Force denied access (in its literal sense) with a restrictive legal reasoning adhering to the letter of the law. As a further conclusion, it can be established that until no binding guidance will be adopted in this area, the data subject's opportunities to exercise his rights will be dependent on the data controllers' individual interpretation of the law.

CCTV on public transport

On 16/09/2013 the researcher asked for a copy of the CCTV footage recorded of her on a bus on way to work. In the absence of privacy notices, the researcher submitted her request to the public office responsible for transport services on 18/09/2013. In its reply, which was only six lines long, dated 25/09/2013, the respondent informed the researcher that at the time and place specified in the request the cameras were not in operation on board of the bus, 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 footages. We note in parentheses that in this reply the researcher's request was qualified as "request to access public data" which makes the interlocutor's preparedness regarding subject access procedures questionable.

Following this reply, the researcher sent a further letter to the service provider on 28/11/2013. She wrote that passengers can apparently never know for sure whether a camera on board is in operation or not, thus, she could not challenge the statement that no personal data related to her was being processed. She added that in the absence of specifying the concerning law, she could not accept that only the police and the judicial authorities are allowed to gain access to CCTV footages. To prevent the data controller from not responding to this question, the researcher presented a new data request in her letter hoping that this time she had managed to take a bus on which the surveillance equipment was in operation.

The second e-mail of the service provider dated on 21/12/2013 informed the researcher 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 the researcher's 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 that may contain personal data related to the researcher 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 the researcher's 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 avoided 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 the researcher why she could not access her 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 CBT is not the data controller, what is the relevance of its position in handling subject access requests? Consequently, in the researchers' view, the denial of the data controller status was based on a misinterpretation of the law. This response can be regarded as a strategy of denial, especially because the data controller did not use this argument when the researchers requested information by phone about where access requests could be submitted to, nor when they denied access the first time.

In summary, the organization prevented the researcher 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 for the requester, rather than seeking ways to at least partially satisfy her. This assumption had not been compensated by any positive circumstances in the course of the procedure. Although the company almost fully used the 30 day deadline at its disposal in both rounds, its replies were laconic. The company did not attempt to assist the requester: although it revealed the name of the data controller in its interpretation, it did not forward the request to that organization. These reasons let the researchers conclude that data controller had showed a very low propensity to facilitate the realization of subject access rights.

CCTV in a public space

To gain access to a CCTV footage taken in a public space of Budapest city centre (District IX), the researcher submitted a request to the Public Space Supervision Authority of Ferencvaros on 18/09/2013, four days after she had been recorded. As the researcher had been advised in the first phase of this research, the access request was sent to the general contact e-mail address of the authority (also by ordinary mail). Contrary to the expectation of

the researcher who was waiting for immediate or at least swift reaction, she only received a reply on 30/09/2013. This informed the researcher that storage time for CCTV footages taken in public spaces is eight 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 her response the researcher accepted the fact that the footage was no longer accessible but due to the lack of provided information she put further questions to the organization. She reminded the data controller that she had submitted her request three days before the expiry of the retention period, and the request was sent to the e-mail address as she had previously been instructed by phone. With this in mind, the researcher 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, the researcher received a phone call from the authority. The member of staff at the end of the phone line wanted to enquire about the number plate of the researcher's car in order to identify her case since she was not able to find it. When the administrator was told that the researcher was not in her car at the time of the recording (she was just walking by), the administrator got confused and asked (somewhat angrily): "*Then what's your problem? I really don't understand your point."* When the researcher replied that she only wanted to exercise her 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 the researcher 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. Nevertheless, even if they would have noticed the request earlier, they could not have provided a copy of the recording either, 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. In the last sentence of the letter the director appeared to close the debate on his part: "*The access request based on the provision of the Data Protection Act you referred to was completed by the Supervision Authority when and with providing information on data processing in its letter dated on 30/09/2013."*

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 realizing 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 the researcher's request was processed in time. Given the fact that the data controller totally concealed this reason for denial from the researcher in its first reply, and taking also into account that it had three 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 the researcher was in this case, phone calls like the one described above might give the impression to him that the request is illegitimate. To sum up, the manner in which the researcher's request was processed with respect to the lack of transparency of the process, the unreasonable delay in answering and the cover-up of the fact that access rights may only be enforced in a very narrow range of circumstances before the authority, illustrate restrictive practices on behalf of the data controller. This impression is offset to some extent by the willingness of the authority to remain in dialogue with the researcher and the fact that the data subject was informed about the question of third party data sharing.

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 the request submitted on 18/09/2013 by phone on 11/10/2013. The call came from the head of the security service, and its explained aim was merely to indicate that they had sent their letter by mail including "their request". The man seemed very responsive, but also suspicious and mysterious, leading the researcher to feel as though she was being tested as to whether she was 'normal' and mentally intact. The essence of the short written answer dated on 10/10/2013 (but delivered only on 14/10/2013) was that the requester 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."* This request was met by the researcher on 29/10/2013. There, the head of security said that they had never received such kind of request before, but they immediately saved the data and would send their substantive written answer soon. He also informed the researcher that she was recognisable on the CCTV footage based on the detailed description specified in the request. The head of security argued that they would also fulfil the request just by providing information since giving a copy of the recordings is not required under the Data Protection Act. It was an unexpected turn for the researcher in the case that the company is operated as a condominium so that it is also subject to the rules of the Condominiums Act on CCTV surveillance, which is not common for a department store. At the same time, the head of security also mentioned that he 'googled' the requester and found out that he was not dealing with a lay person (this was tolerated by the researcher in silence).

The subsequently sent reply dated on 31/10/2013 asked the researcher to confirm her right or lawful interest based on which the blocking of such records was requested by her. In reply to this, the researcher explained to the data controller that the request was only based on her right to access to personal data which right shall also be respected pursuant to the Condominiums Act and thus she had no intention to indicate any right or lawful interest going beyond that.

Then, the company wrote in its further reply mail dated on 10/12/2013 that it wanted to comply with the acts in all respects and did not want to prevent the researcher from exercising her rights, but at that time it could not see how that could be carried out taking into consideration the rights of third parties. With regard to the fact that certain provisions of the

Data Protection and Condominiums Acts do not provide for a clear guidance, the company decided, without supplying the researcher's 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 the researcher on 14/01/2014.

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 the researchers' view, as far as the legal position of a data controller is not *contra legem*[131] 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 the requester can be read in the way that the data controller did not expect from 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. True enough, one may also perceive this behaviour as an attempt to flee ahead of the legal challenge.

CCTV in a bank

On 23/09/2013, the researcher turned to the a bank in order to gain access to the CCTV recordings taken of her during the use of the cash machine placed within the building of the branch office (including the recordings made by the cameras placed within the branch and inside the cash machine). In the absence of any other possibility, the request was submitted online using the template for all kinds of enquiry. The researcher 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 sent on 16/10/2013 and consisted of quite incoherent sections. The first paragraph informed the researcher 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 the researcher's 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 for the researcher, and the position of the bank according to which the researcher's complaint appeared to be investigating the breach of *consumer protection rules* (emphasis added by the authors). This incorrect categorization of the request might serve as explanation

[131] Against the law

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.

The researcher stated in her reply sent on 24/11/2013 that it was not entirely clear for her from the letter whether the request was denied, and if it was, then for exactly what reason was the request found illegitimate (in the absence of client status, adequate identification, or official proceeding?). As regards the client status, the researcher set out that since the use of 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, she is certainly a client. Besides, she 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. (For example, this is the case when a client of the bank arrives at the branch with an attendant.) With respect to the third party data sharing, the researcher wrote that she 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 her as to whom it forwarded the recordings taken of her, if those were forwarded. Ultimately, the researcher added a threat of turning to the NDPA if no reply is received.

On 10/12/2013 the researcher received a phone call from the head of security. The aim of the call was to inform the researcher about the existence of the footage and providing information on what could be seen on the picture. The head of security informed the researcher that she was 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 he should have not afforded (such as sexist remarks on the appearance of the researcher). As the head of security could not exactly specify the legal basis for denying the forwarding of the footage, the researcher asked the bank to send its position on this issue in a written form. This subsequently sent reply contained 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 the researcher, in which the ways of avoidance and willingness to act in accordance with the law were mixed. The company inherently appeared to discourage the researcher in her 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 the bank, none of the lawyers could recognise a subject access request, especially in a case where the researcher referred to the legal basis of her request to the data controller. For that reason, qualifying the access request as consumer complaint and redirecting it to the National Bank of Hungary can reasonably be considered as restrictive practices. Most probably, the turn in the course of communication was the result of the decided manner of the researcher and her legal preparedness – after this, the bank became significantly more responsive. It can be reasonably supposed that by then lay requesters have already given up the case, not to mention the fact that the CCTV recordings would have not been retained in time.

Concluding thoughts

Besides the factual observations and the evaluative findings presented in a concise form in the *Overall summary* section of this report, three concluding thoughts of longer term relevance can also be drawn from the experience accumulated in the course of this empirical research.

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].[132] 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 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].[133]

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 CTTV 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[134] provides 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,

[132] Art. 12 of 95/46/EC Directive.
[133] Section 15 (1) of Data Protection Act.
[134] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf (last accessed 9 May 2014).

"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 a coherent guidance issued for data controllers in the area of serving 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.

SIGNIFICANCE OF FINDINGS - HUNGARY

The complex empirical study of subject access rights in Hungary resulted in important findings, partly because the country represents a specific legal, political and social development in the post-dictatorial historical period, and partly because this has been the first comprehensive study in Hungary in this area.

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

The main rules of subject access can be found in the combined Act on Informational Self-determination and Freedom of Information. A number of sector-specific laws and regulations contain provisions on subject access, of which the most relevant laws for the purpose of this study were the Personal and Property Protection Act, the Electronic Communication Act, the Police Act, the Passenger Transport Act, and the Public Space Supervision Act. The analysis revealed the absence of general codes of practice or other soft laws regulating surveillance in general and the use of CCTV in particular, and the existing codes – for example in the area of distance selling, direct marketing or property protection – do not contain provisions on subject access.

The study confirmed the general experience that subject access requests *per se* are extremely rare, 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, until 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, hopefully temporarily), could help data subjects learn the identity and connections of data controllers.

In the first phase of the empirical research the researchers attempted to locate data controllers at 31 sites, and in the second phase they submitted access requests to 19 controllers. According to the quantitative analysis, Hungary belongs to the mid-range of countries with less than 50% positive outcome in these areas. 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 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 footages, 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. This is partly because in certain areas of CCTV surveillance, lawmakers have failed to enact particular provisions for what should be included in the CCTV signage. But even when the law in force contained the requirement to post a signage conveying information to citizens on processing of personal data in a privacy notice, data controllers did not fulfil this legal obligation.

In the request phase, 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 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, and in particular in the case of multinational companies was 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. Certain sector-specific laws stipulate that the requester needs to prove her legal interest, and this was an obstacle of a legal nature in submitting the requests.

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 convince the requester about the legal and practical impossibility to serve her request rather than facilitate her right of access.

General conclusions:

- From a methodological point of view, it was an illusion to employ educated researchers to act as lay requesters in several cases: their knowledge had to be revealed during negotiations with the controllers. In a country where data controllers receive few such requests, they tend to investigate first who the requester is. In addition, in a small country where the number of experts in data protection is low and their identity is publicly known, this may significantly distort the results of the study. Such studies in the future could use volunteers, similarly to studies in submitting freedom of information requests.
- A general experience was that 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.
- 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.
- 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".

- Some data controllers tend to interpret the right of access narrowly, and the restricting provisions broadly, contradicting to the dogmatics of constitutional law, according to which fundamental rights should be interpreted broadly, while restrictions should be interpreted in a narrow sense.
- The study revealed that the very content of subject access right is ambiguous: there is a slight difference between the wording of the EU data protection directive and the Hungarian law, thus leaving room for interpretation which is unfavourable for the requesters. Lawmakers both at the EU level and in national law need to clarify whether access to one's own personal data means receiving *information* about the data, or access to (a copy of) the data themselves. This has particular relevance in the area of CCTV recordings where granting access necessitates specific technical and organizational measures.
- Finally, the empirical study confirmed that without coherent guidelines 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 data controllers in drafting their own sectoral guidelines.

References

Anarki (blogger), "Kis orszag, kis Google [Small country, small Google]", http://index.hu/tech/2009/10/14/kis_orszag_kis_google/ (Last accessed on 27 January 2014)

Dajko, P., "Camera Surveillance in Hungary", *IT Cafe*, 29 January 2012, available at http://itcafe.hu/cikk/adatvedelmi_nap_2010_kameras_megfigyeles/kameraellenes_vagy_kameraparti.html [in Hungarian]

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

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

Laszlo, G., "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, 2005.

Majtenyi, L. (2006), *Information freedoms* [in Hungarian] Budapest, Complex.
Solyom, L. and Brunner, G. (eds.) (2010), *Constitutional Judiciary in a New Democracy. The Hungarian Constitutional Court.* University of Michigan Press.

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.

Szigeti, T. and Vissy, B. (2012), "Ombudsman", in *Corruption Risks in Hungary 2011 – National Integrity Study*, Budapest, Transparency International, pp. 146–157.
The EDPS Video-surveillance Guidelines, Brussels, 17 March 2010, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

List of Abbreviations

ANPR - Automatic Number Plate Recognition
BISZ Zrt. - a specialized company operating the Central Credit Information System (Hungary)
BKK Zrt. - Budapest Transport Company
CCTV - Closed circuit television
COAES - Central Office for Public and Administrative and Electronic Public Services (Hungary)
DPO - internal data protection officer
EDPS - European Data Protection Supervisor
EU - European Union
HCLU (or TASZ) - Hungarian Civil Liberties Union
HUF - Hungarian Forint (national currency)
ISPs - Internet Service Providers
KHR - Central Credit Information System (Hungary)
MTE - Association of Hungarian Content Providers
NAIH - Hungarian National Authority for Data Protection and Freedom of Information
NDPA - National Data Protection Authority
NGOs - non-governmental organizations
NMHH - National Media and Infocommunications Authority (Hungary)
PSZAF - Hungarian Financial Supervisory Authority