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

SLOVAKIA COUNTRY REPORTS

UNIVERZITA KOMENSKÉHO V BRATISLAVE, SLOVAKIA

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN SLOVAKIA – DR ERIK LÁŠTIC

LOCATING THE DATA CONTROLLER IN SLOVAKIA – DR ERIK LÁŠTIC

SUBMITTING ACCESS REQUESTS IN SLOVAKIA – DR ERIK LÁŠTIC

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN SLOVAKIA

Introduction

Compared to Hungary,[1] where data protection was brought to attention and gained importance after 1989 by an influential group of intellectuals, "data protection" as such has never been an "issue" in recent Slovak history (since 1989). Although there were dozens of cases that involved, to smaller or larger extent, data protection,[2] and general principles of personal data protection were included in Slovakia's 1993 Constitution, the dominant angle was focused on other aspects such as intelligence agencies; files of former secret police; corruption. As a result, the legal regulation of data protection was introduced in Slovakia as a part of accession process to the EU, especially during 1998 and 2002.

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

Article 19(3) of the 1992 Constitution of Slovakia protects personal data stating that "everyone has the right to protection against the unwarranted collection, publication, or other illicit use of his personal data."[3] The general data protection law, No. 428/2002 Coll. on the Protection of Personal Data[4] (hereafter 'the law') establishes the Office for the Protection of Personal Data as the national regulatory authority. The law was passed as a direct result of Slovakia's accession and demand by the EC to properly implement Directive 95/46/EC. It repealed Act No. 52/1998 Coll. on Personal Data Protection in Information Systems. Since its adoption in 2002 the law has been amended four times,[5] with the 2005 amendment being the most significant as it fully harmonized the law with the Directive.[6] In May 2013 the Slovak parliament passed a new data protection law that repealed the 2002 law. The new law is effective from July 1, 2013, with the exception of several transitional periods for compliance ranging from 6 to 12 months. While the overall legal regime for data protection remains the same, several specific changes were introduced, such as a minimum content requirements for

[1] For comparison see: Szekely, Ivan (2008), Hungary, in James B. Rule and Graham Greenleaf (eds.), Global Privacy Protection: The First Generation, Edward Elgar Publishing Ltd., Cheltenham, UK, pp. 174–206.

[2] The topic of surveillance repeatedly resurfaces in political and public debates, and is usually connected to workings of country's intelligence services and political (lack) of overview. As a result, since 1994 there is an ongoing series of cases that are result of mismanagement of information, leaks and (ill) legal wiretaps, mostly used as means for political advantage. The "surveillance" is therefore considered as the "means" for other actions and behavior, and is only rarely a subject of political and media debate itself. For more see report on Slovakia for IRISS WP4 on general history of surveillance in Slovakia.

[3] The 1992 Constitution of Slovak Republic, available in English at: http://www.nrsr.sk/web/Static/en-US/NRSR/Dokumenty/constitution.doc (last accessed 13July 2013).

[4] The law was valid till 30/6/2013. For full English version of the consolidated version of the law see: http://www.dataprotection.gov.sk/buxus/docs/act_428_2002_01_09.pdf, accessed 27/06/2013

[5] The law was directly amended by Act No. 602/2003 Coll., Act No. 576/2004 Coll., Act No. 90/2005 Coll. and Act No. 583/2008 Coll.

[6] According to the explanatory report for the 2005 amendment to the Protection of Personal Data Law, the main aim of the "euroamendment" was to fully harmonize the law with the Directive. The amendment introduced/changed several legal terms, clarified the obligations of data controllers, introduced changes in registration procedure of information systems and strengthened the powers of the DPA. (in Slovak, available at:http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-29206?prefixFile=m), For legal overview of changes introduced see: http://www.fifoost.org/slowakei/recht/sfln/2005/node55.php, (last accessed 25June 2013).

the appointment of a data processor by a data controller; the requirement to appoint a responsible data officer for data controllers only for companies that process data concerning 20 and more persons (previously 5 persons); the facilitation of cross-border transfers of personal data; and strengthening of sanction powers of the Data Protection Office (DPA).[7]

Definitions

The law defines *personal data* (§ 3), as "any information relating to an identified or identifiable natural person, while such person is one who can be identified, directly or indirectly, in particular by reference to an identifier of general application or by reference to one or more factors specific to his physical, physiological, psychic, mental, economic, cultural or social identity."

Data controller, §4 (2), is a "state administration authority, territorial self-government authority, other public authority body or legal or natural person, which alone or jointly with others determines the purposes and means of the processing of personal data." *Data processor*, §4(3), is defined as "state administration authority, territorial self-government authority, other public authority body or other private legal or natural person processing personal data on behalf of the controller or controller's representative".

The law defines *processing* (§4(2,a)) as "any operation or set of operations which is performed upon personal data such as obtaining, collection, recording, organization, adaptation or alteration, retrieval, consultation, alignment, combination, transfer, use, storage, destruction, transmission, provision, making available or making public". By *filing system* (§4,(1)g) it identifies "any structured set, system or database containing one or more personal data, which are systematically processed for the needs of achieving the purpose according to specific criteria and conditions, while using automated, partially automated or other than automated means of processing, disregarding the fact whether the system is centralised, decentralized or dispersed on a functional or geographical basis, e.g. card- index, list, register, file, record or a system containing files, documents, contracts, certificates, references, assessments, tests".

Case law: Constitutional Court

Neither the 1998 nor 2002 law on data protection were ever subjected to the review by the Constitutional Court of Slovakia. However, the Constitutional Court ruled on three notable cases that were connected to the constitutional rights for privacy and data protection as introduced by the 1992 Constitution of Slovakia. In all these three cases the Constitutional Court had to decide if, and to what extent, the right to privacy and data protection is constrained by the constitutional right to information.

In the first case, II. ÚS 44/00, the Constitutional Court held that protesters who made video recordings of policemen performing their official duties in open public space did not invade

[7] For legal overview of changes introduced see: Slovakia: new data protection regulation - overview of main changes, available at: http://www.schoenherr.eu/news-publications/legal-insights/slovakia-new-data-protection-regulation-overview-of-main-changes, Accessed 25/06/2013; for political background see: Protection of personal data gets revamp, Slovak Spectator, 11/3/2013, available at: http://spectator.sme.sk/articles/view/49355/24/protection_of_personal_data_gets_revamp.html (last accessed 25 June 2013).

policemen's right to privacy and were not required to obtain their permission to make recordings.[8]

This case law was reinforced by the second case, IV. ÚS 40/03, which was decided by the Constitutional Court in 2003.[9] The case involved a decision by the local parliament in the city of Považská Bystrica to forbid a citizen who was attending public session of the parliament to take pictures of MPs. The citizen tried to document the controversial voting of MPs on selling the city's real estate. The Constitutional Court ruled in favor of the citizen and his right to information that was essential in a situation when public authority (local parliament) failed to provide voting records.

In a third case the Constitutional Court reviewed the constitutionality of the 2006 amendment to the free access to information law that allowed access to salary and compensation data of public officials. The Justice Ministry initiated the constitutional review, arguing that the 2006 amendment violated the constitutional right to privacy. In 2011, the Constitutional Court upheld the 2006 amendment and confirmed that "the purpose of the implementation of the fundamental right to information is with regard to its constitutional relevance able to justify interference" with other fundamental rights.[10]

Case Law: Local, Regional and Supreme Court

In 2005, as a part of a broader investigation that focused on national identification numbers, the Slovak DPA ordered the Justice Ministry to end the disclosure of national identification numbers[11] and to remove those previously published from two databases operated by the Ministry.[12] Both databases (the Official Journal of the Slovak Republic and the Commercial Bulletin), were accessible online and compiled various legal information about private companies and businesses registered under the Slovak Commercial Code. After unsuccessfully appealing the order before the Chairman of the DPA, the Justice Ministry filed a petition with a regional court, asking for nullification of the DPA's order. The court dismissed the petition and upheld DPA's order, arguing that it was based on appropriate grounds, and was in line with the powers granted to the DPA by the law.[13]

The most publicized case in the last decade, in which the DPA played a significant role, was connected to the national census in 2011, organized by the Statistical Office of the Slovak Republic.[14] A few days before census forms were distributed, a "blogger and security expert" (in his own words) pointed out a potential misuse of census data because their anonymity was

[8] IV. ÚS 44/00, The Constitutional Court of Slovakia. The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2001a/10_01a.pdf

[9] IV. ÚS 40/03, The Constitutional Court of Slovakia, The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2003a/190_03a.pdf (last accessed 25 June 2013).

[10] PL. ÚS 1/09, The Constitutional Court of Slovakia, The English summary of the ruling can be found: http://portal.concourt.sk/Zbierka/2011a/1_11a.pdf (last accessed 25 June 2013).

[11] Birth number. It is unique for every citizen.

[12] The case is analyzed by the DPA in its written opinion from 2006. The opinion is available at: http://www.dataprotection.gov.sk/buxus/docs/MSSRst150306v2.pdf, (in Slovak), (last accessed 25 June 2013). The order itself is not available online.

[13] Article 29 Working Party, 11th Annual Report of the Article 29 Working Party on Data Protection, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf

[14] Slovak Spectator, 30/05/2011, Anonymity of census data questioned.

compromised by a unique numerical code used on every census form.[15] The blogger involved a national TV channel and filed an official complaint against the Statistical Office with the Slovak DPA. The DPA released a press statement a couple of days later (only few days before the official start of the census), in which it asked the Statistical Office to fully "inform the residents of Slovakia that the data collected for the 2011 census is not anonymous and to cancel residents' obligation to place the numerical code on their respective census form."[16] The Statistical Office responded with its own statement, calling DPA's release "manipulative" and accused the DPA of endangering the results of the census. After the intervention of Prime Minister Radicova, the DPA softened its stance and later cancelled it after formal review by the Attorney General's Office. The controversy influenced returns of the census forms, especially in Bratislava, in which almost 20% of residents did not return their forms.[17]

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

Subject access rights to personal data are stipulated in § 20 of the law.[18] Firstly, subject access requests must be made in writing. Moreover, citizens are entitled to request from the data controller (§ 20(1)):

> "a) information about the state of processing of his personal data in the filing system, b) exact information about the source from which the controller obtained his personal data for their processing, c) a copy of his personal data which constitute the subject of the processing, d) rectification of inaccurate, incomplete or not updated information, e) destruction of his personal data, f) destruction of his personal data, which constitute the subject of the processing, provided that the law was breached".

The rights of the data subject may be restricted only under d), rectification and e), destruction, provided that such restrictions results from a special law or if exercising of this right would infringe the protection of the data subject or the rights and freedoms of others.
Furthermore, the data subject is entitled to object[19] to the processing of personal data for the purposes of direct marketing without his consent. Also, the data subject is entitled to object to the data controller (Section 20(4)) anytime upon a free-of charge written request or personally, provided that the matter cannot be postponed to the processing of personal data in the cases when personal data may be processed without consent.[20]

All requests listed above are free of charge with the exception of requests made under § 20(1) b) and c)[21], which necessitate payment of a fee in the amount not exceeding the amount of

[15] For more see original blog post that started controversy, available at: https://www.iseco.sk/scitanie-2011/, In Slovak, (last accessed 13 July 2013).
[16] The official opinion of the DPA on 2011 Census, May 2011, available at: http://www.dataprotection.gov.sk/buxus/docs/Stanovisko_Uradu_k_scitaniu.pdf (last accessed 19 July 2013).
[17] For more on influence see: SME, http://www.sme.sk/tema/scitanie-obyvatelov-2011, In Slovak, (last accessed 30 May 2013).
[18] Section 28 of the new law. The new law allows for data request to be submitted in person and also allows to submitt request in person to the data processor.
[19] Section 20(3) of the law
[20] Section 7(4) of the law that stipulates personal data that may be processed without consent.
[21] I.e. b) the information about the source from which the controller obtained his personal data for their processing; c) a copy of his personal data which constitute the subject of the processing.

material costs accrued in connection with the making of copies, providing technical carriers and sending the information to the data subject. No maximum limit on a fee is established.
The data controller has to satisfy the request in writing within 30 days from the day of their receipt and the response provided by the data controller has to be in "generally intelligible form".

Case law

Although citizen's awareness about access rights is increasing in Slovakia, they have still to find their way to courts to claim access rights. As highlighted by the 2013 Linklaters report,[22] there is no relevant case law in this respect at national level. On the one hand, the data protection framework is changing and evolving. On the other, there are still significant inconsistencies in the interpretation of existing legislation on data protection. While the definition of personal data given by the DPA is closely based on standards laid down in the European Directive, in practice "the DPA often interprets the definition of personal data more narrowly and only considers that information (a set of information) can be personal data if the individual is either identified or identifiable based on such particular (set of) information (and not other information that might be held by the data controller now or in the future)".[23] Slovak courts have not tested this approach yet.

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

The law includes several provisions that specify the scope of the law, obligations of data controllers and rights of data subjects. The most important and general exception is defined in paragraph 2 of the law. It provides that several provisions of the law[24] shall not apply (including subject access requests) to the processing of personal data necessary *for safeguarding of the public interest*. In this case the data controller has to fulfil not only the obligations stipulated by the law, but also additional obligations by a special laws[25] in areas enumerated by the §2 of the law: "a) security of the Slovak Republic, b) defence of the Slovak Republic, c) public policy and security, d) preventing, precluding, detecting and documenting of criminal offences, disclosing their perpetrators, investigating and prosecuting of criminal offences, e) important economic or financial interests of the Slovak Republic or of the European Union, including monetary, budgetary and taxation matters, f) inspection, internal supervision, external supervision or regulatory function connected with exercise of official authority in cases referred to in Subparagraphs c), d) and e), org) protection of the data subject or of the rights and freedoms of others."

The exception from paragraph 2 of the law impacts directly upon the right of access to the data recorded by video or audio devices (e.g. CCTV). Paragraph 10 (7) of the law specifies that "the premises accessible to the public may be monitored by means of a video recording or audio recording **only** for the purposes of the public policy and security, disclosing criminal

[22] Linklaters, *Data Protected*, 2013. For the full report see https://clientsites.linklaters.com/Clients/dataprotected/Pages/Slovakia.aspx, (last accessed 30 May 2013).
[23] Ibid.
[24] I.e. Provisions of Section 5 Paragraph 4, Section 6 Paragraphs 1 to 4, Section 10 Paragraphs 1, 2 and 8, Section 20 Paragraph 1, Section 27 and Section 32
[25] E.g.: the law No. 46/1993 Coll. Z. z. on Slovak Information Service; No. 319/2002 Coll. on defense of Slovak Republic; No. 564/1991 Coll. on Local Police; No. 171/1993 Coll. on Police Force.

activities or interference with the State's security, provided that the premises are clearly marked[26] as being monitored".[27] Furthermore, if the recording is not used for the purposes of criminal/misdemeanour proceedings it has to be destroyed within seven days[28] from the day following the recording.[29]

Paragraph 2a of the law also excludes application of the law of protection of personal data that is processed by a person for their own needs, such as correspondence and personal data that was "obtained accidentally without prior determination of the purpose and means of processing, without the intent of their further processing in an organized system according to special criteria and which are not further systematically processed". Other exceptions[30] are stipulated for personal data that may be processed without consent. These include processing necessary for the purpose of artistic or literary expression; for the purpose of informing the public by means of the mass media; or in situation when the subject of the processing is constituted solely by the title, name, surname and address of the data subject without a possibility of adding his other personal data.

Specific exception: National Memory Institute and transitional justice in Slovakia

Slovakia, along other former Communist regimes in the region, had to deal with its past by using legal and political instruments. The most significant of them was the establishment of the Nation's Memory Institute in 2002. The law[31] sets the rules on disclosure of documents regarding the activity of state security authorities from 1939 to 1989, a period that includes both the First Slovak Republic (1939-45), a close ally of Hitler's Germany, and the Communist era (1948-1989). The main activity of the Institute is to systematically research and disclose documents from 1939 to 1989, instead of bringing criminal evidence for prosecution against former members of security forces. The Institute systematically publishes information on former regimes, such as databases[32] of persecutors and persecuted. This activity involves the processing of personal information (e.g. files of former members of secret police) and its publication without written consent of data subjects.

The disclosure of the documents is subject of ongoing legal challenges from individuals who are identified by files as persecutors (active members of secret police, agents, conspirators, etc.) A first complaint connected to the law No. 553/2002 Coll. was addressed to the DPA in

[26] The signage that the premises are being monitored is not required if it is not stipulated by a special law. E.g. law No. 483/2001 on Banks, Section 93s(7) " The premises of a bank, branch of a foreign bank and the National Bank of Slovakia, and ATM machines and currency exchange machines not located in the premises of a bank or branch of a foreign bank, may be monitored by video or audio recordings even where there is no notice that the area is under surveillance". For English version of the law see: http://www.nbs.sk/_img/Documents/_Legislativa/_BasicActs/A483_2001.pdf (last accessed 29 June 2013).

[27] This exception remains unchanged in the new law of 2013, where it is defined in §15 (7).

[28] Unless otherwise stipulated by a special law, e.g. the Law No. 483/2001 on Banks, Paragraph 93a (7) allows for 12 months period. For English version of the law see: http://www.nbs.sk/_img/Documents/_Legislativa/_BasicActs/A483_2001.pdf (last accessed 29 June 2013).

[29] Paragraph 13(7) of the law

[30] Paragraph 7 (4) of the law

[31] Law No. 553/2002 Coll. on declassification of documents concerning activities of security bodies of the state in the period 1939- 1989 and on establishment of the Nation's Memory Institute allows National Memory Institute, available in English at: http://www.upn.gov.sk/data/pdf/553_2002_en.pdf (last accessed 5 July 2013).

[32] E.g. the organizational structures of intelligence and counter-intelligence services of communist secret police that are published online, See: http://www.upn.gov.sk/utvary-stb-a-ps-na-slovensku/zoznam-osob.php?pismeno=B) (last accessed 11 July 2013).

2004 by an individual who argued that the Slovak intelligence agency (SIS) had delivered his personal file to the Institute in an unauthorized way and without the knowledge and consent of the complainant.[33] The complaint also argued that the Institute held his file in an unauthorized way and asked for the return of his file. The whole complaint was refused by the DPA, arguing that the law on data protection clearly established an exception for the activities of the Institute, which in this case also functions as a data controller that is obliged to process this type of data under the law.

However, the scope of the powers of the Memory Institute was challenged, and, subsequently limited, in a 2009 case decided by the Supreme Court of Slovakia.[34] The plaintiff challenged the public disclosure of his personal data from secret police archives that were stored under the category of "confidants".[35] In this category secret police registered people that were of interest, but who were not knowingly collaborating with the secret service as in other categories, e.g. informants and agents. The ruling of the Supreme Court confirmed the previous line of decisions of lower courts that prohibited the Memory Institute to publicly disclose personal data of the plaintiff without his explicit consent.[36]

Compatibility of national legislation with Directive 95/46/EC

Slovakia's accession was heavily influenced by EU conditionality, as Slovakia was the only country left out from the initial round of the enlargement due to political reasons.[37] After the 1998 parliamentary election, in which pro-European parties won a constitutional majority, Slovakia was forced to "catch-up" on the accession, a process that led to a limited debate on the nature of accession and its conditions. Slovakia had to behave obediently in order to catch-up and join the EU with neighbouring countries in 2004, which led to executive-dominated accession negotiations supported by the technocratic nature of legal harmonization by Slovak government.[38]

During Slovakia's accession to the EU and its first years of membership, there was an on-going debate between the EC and the Slovak government on the transposition and implementation of the Directive. As a part of accession negotiations that dealt with conditions under which future members will adopt, implement and enforce EU legislation, several chapters that were part of the negotiations included data protection. The main condition was

[33] For more about the complaint see: The 2004 Annual Report of Slovak DPA, in English, available at: http://www.dataprotection.gov.sk/buxus/docs/status_report_2004.pdf, pp. 34-35 (last accessed 11 July 2013).

[34] The Supreme Court of Slovakia, case No. 5 Cdo 83/2008, available in Slovak at: http://www.nssr.gov.sk/data/att/7858_subor.pdf, accessed (last accessed 11 July 2013).

[35] In this category secret police registered people that were of the interest, but who were not knowingly collaborating with the secret service as other categories (informants, agents).

[36] For more on the case, see Privacy International, *Report: Slovakia*, available at: https://www.privacyinternational.org/reports/slovakia/iv-governance-issues, (last accessed 11 July 2013).

[37] For reasons see European Commission, *Agenda 2000, Commission Opinion on Slovakia's Application for Membership of the European Union*, 15. 7. 1997, http://ec.europa.eu/enlargement/archives/pdf/dwn/opinions/slovakia/sk-op_en.pdf (last accessed 25June 2013).

[38] This is not unique for Slovakia. One of the most influential studies on EU law compliance by Falkner and Treib (2008, 308) argued that all new member states belonged to the world of dead letters. "Countries belonging to this cluster ... may transpose EU Directives in a compliant manner, depending on the prevalent political constellation among domestic actors, but then there is non- compliance at the later stage of monitoring and enforcement. In this group of countries, what is written on the statute books simply does not become effective in practice." See also Staroňová and Láštic (2012) on civil service reform failure in Slovakia after 2004.

to fully harmonize Slovak legislation in the area of data protection, namely with Directive 95/46/EC. Together with the demand for harmonization, the EC also pressured all accessing countries to establish central authorities to oversee data protection matters nationally. This reflected similar requests that were addressed in other policy areas, e.g. telecommunications and network industries. The EC pushed for an independent authority with sufficient financial and administrative capacity to implement and enforce the legislation. At that time, the effective Slovak law on data protection provided no such status for the DPA. The 1998 law on Personal Data Protection in Information Systems established the Commissioner, appointed by the Government,[39] as a governmental official responsible for data protection. In the 1999 Progress report, the EC criticized the lack of "progress made in regard to this office" and stressed a need for "further legislative fine-tuning".[40] This position was repeated in the 2001 report, where the European Commission demanded that the "degree of independence" of the DP Commissioner "should be strengthened" and that the law "needs to be brought fully in line with the directive on the protection of personal data and the free movement of such data has not yet been transposed and a significant number of operators are not registered".[41] Slovakia responded by passing the 2002 law on Personal Data Protection that established an independent Data Protection Office and strengthened the position of the Commissioner, who was appointed by the Parliament on a proposal by the Government. In a 2002 report ,[42] the EC concluded that Slovakia "has advanced in the area of the protection of personal data and the free movement of such data both as regards legislative alignment and administrative capacity", but warned "that further efforts will be needed to implement the new Act on personal Data Protection and public-awareness raising will be key for ensuring actual compliance with the law". In the final monitoring report[43] from 2003 the EC acknowledged that Slovakia had "completed its legislative alignment in the field of data protection", but "a number of shortcomings in the Slovak legislative transposition still need to be addressed".

As illustrated above, the law has been amended four times since its adoption in 2002, with the 2005 amendment being the most significant as it fully addressed shortcomings from the final monitoring report in the transposition of the Directive. According to the explanatory report[44] for the 2005 amendment to the Protection of Personal Data Law, the main aim of the "euro amendment" was to fully harmonize[45] the law with the Directive. The amendment introduced

[39] On a proposal by the President of Statistical Office.

[40] European Commission, *Progress Reports from the Commission on Progress towards Accession by each of the candidate countries*, October 13, 1999, p. 31 Available at: http://ec.europa.eu/enlargement/archives/pdf/key_documents/1999/slovakia_en.pdf (last accessed 27 June 2013).

[41] European Commission, ibid., p. 41 and European Commission, *Regular Report on Slovakia's Progress Towards Accession*, 2001, p. 80, available at: http://ec.europa.eu/enlargement/archives/pdf/key_documents/2001/sk_en.pdf

[42] European Commission, *Regular Report on Slovakia's Progress Towards Accession*, 2002, p. 57, available at: http://ec.europa.eu/enlargement/archives/pdf/key_documents/2002/sk_en.pdf (last accessed 29 June 2013).

[43] European Commission, *Comprehensive monitoring report on Slovakia's preparations for membership*, 2003 p. 19, available at: http://ec.europa.eu/enlargement/archives/pdf/key_documents/2003/cmr_sk_final_en.pdf, (last accessed 28 June 2013).

[44] Explanatory report for the 2005 amendment to the Protection of Personal Data Law, in Slovak, available at:http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-29206?prefixFile=m_), For legal overview of changes introduced see: http://www.fifoost.org/slowakei/recht/sfln/2005/node55.php (last accessed 25 June 2013).

[45] Table of compliance with the Directive is available at http://ec.europa.eu/justice/policies/privacy/docs/implementation/slovakia_compliance_en.pdf, (last accessed 27 June 2013).

and changed several definitions, e.g. the meanings of third country, third party and public interest. It also clarified the obligations of data controllers, introduced changes in registration procedure of information systems and strengthened the audit powers of the DPA. Finally, the amendment added a new §23a on the cross-border flow of personal data in the EU.

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

The website of the Slovak DPA is static with a very dated design. It has no interactive features and provides no online forms.[46] The website has a section concerning the rights of data subjects[47] that features eight subsections that vary in length (from several paragraphs to few sentences). Each section provides descriptive, mostly legalistic information, and copies frequently from the law. The first link in the section provides "ten commandments" on data protection, e.g. "Do not throw your documents that contain personal data (invoices, old credit cards) to the garbage, but destroy them." Other links in the section include information on subject access rights[48] and time limits,[49] as well as an explanation of access rights in relation to the filling systems operated by the police.[50]

The central government operates a one-stop portal that aims to be an interactive platform for help with various real-life situations. There is no direct link for data protection on the main page and users must use a search function. The search for the term "data protection" results with four links, with only two of them providing relevant information about data protection, role of the DPA and subject access rights.[51]

Based on the review of annual reports by the Slovak DPA, the office provides constant service to public, including legal persons, via email, phone and in-person consultations. According to the latest report by the DPA, in 2011 and 2012 it provided 1490 written replies (including emails).[52] The data on other forms of consultation are not provided by the DPA.

[46] According to the 2007-2008 Annual Report of the DPA the website "is a modern electronic presentation tool.When designing and executing this website, the emphasis was put on combination of individual solutions, including content, user comfort, graphical design and navigation for website visitors and administration of the Office"s website." p. 83, Available in English at: http://www.dataprotection.gov.sk/buxus/docs/status_report_2008.pdf, (last accessed 26 June 2013).

[47] In Slovak, http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=861 (last accessed 27 June 2013).

[48] In Slovak: http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=1148, (last accessed 13 July 2013).

[49] In Slovak, http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=968, (last accessed 13 July 2013).

[50] In Slovak, http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=969, (last accessed 13 July 2013).

[51] One of the links actually provides comprehensive information about data protection and access rights, see: https://www.slovensko.sk/sk/agendy/agenda/_ochrana-osobnych-udajov1, in Slovak, (last accessed 25 June 2013).

[52] Slovak DPA, *The Report on Data Protection for 2011 and 2012*, (in Slovak), p. 58, available at: http://www.dataprotection.gov.sk/buxus/docs/Sprava_o_stave_ochrany_osobnych_udajov_za_roky_2011_a_2012.pdf, (last accessed 11 July 2013). The report does not provide more specific information about the subjects asking questions. It does, however, provide a brief overview of the content of the questions. For 2011 and 2012 they included areas e.g. obligations of data controller, biometric data, cloud computing, CCTV or publication of personal data.

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

The official website of the DPA provides no guidance for data controllers on how to deal with citizens exercising their access rights. While a proactive communication strategy by the DPA is absent here, the DPA must get involved in cases when data controllers fail to grant data access. In such cases the law allows data subjects to file a complaint with the DPA. The review of DPA's annual reports shows that it is only rarely that the DPA deals with complaints that are specifically about data access. The latest report for 2011-12[53] mentions 10 cases (five for each year) in which subject data requests were not granted and complaints were filed with the DPA. By law, the DPA is obliged to investigate the complaint. In all above-mentioned cases the DPA found that complaints were factually true and that the data controllers violated the law. The report mentioned no sanctions against these data controllers.

Compliance with the law is strengthened by investigations and audits of data controllers and operators by the DPA. The investigations and audits may be initiated by the complaints of data subjects, legal persons, ex-officio by the DPA, or are pre-planned by the DPA for a given year. The DPA's annual reports provide a lot of details, ranging from statistics to factual findings that originated from audits. According to the latest report by the DPA for 2011 and 2012, the DPA received and investigated 421 complaints from data subjects and legal persons and initiated another 121 investigations. The DPA also conducted 200 audits of data controllers and operators.[54] According to the report, the audits predominantly focused on prevention, resulting in 247 recommendations and only limited sanctions; in 14 cases the DPA issued monetary penalty notices in total sum of 26, 850€.[55] The audits in 2011 and 2012 focused on data processing for tax bonus purposes, loyalty cards, big supermarket chains, pharmacies, real-estate agencies and foster homes.[56]

[53] Slovak DPA, *The 2011-12 report*, p. 41, (in Slovak), available at: http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=382666, accessed 30/06/2013
[54] Ibid, p. 33
[55] Ibid, p. 33
[56] Ibid, pp. 34-41

LOCATING THE DATA CONTROLLER IN SLOVAKIA

Introduction

This country profile summary concerns the experiences encountered whilst attempting to locate data controller contact details of 34 Slovak-based sites. In particular, the examples below are illustrative of the individual researcher's experiences conducted in Bratislava and do not claim to reflect the practices of *all* data controllers in Slovakia. This report illustrates some general trends noted alongside examples of good and bad practices encountered during the course of this research.

Overall Impressions[57]

Data controller contact details successfully identified after first round of visits	28 of 34 cases (82%)
Data controller contact details unable to identify after first round of visits	6 of 34 cases (18%)
Data controller contact details successfully identified after second round of visits	34 of 34 cases (100%)
Data controller details unable to identify after second round of visits	0
Contact details identified via online privacy policy	28 of 34 (successful) cases
Contact details identified after speaking to member of staff on phone/via email	3 of 34 (successful) cases
Contact details identified after speaking to member of staff in person	3 of 34 (successful) cases
Average rating given to visibility of privacy content online	1 – Poor
Average rating given to the quality of information given by online content	1 – Poor
Average rating given to visibility and content of CCTV signage	1 – Poor

Overall, the quality of information was rated as 'poor', with only a small number of sites providing detailed information about data controllers, rights of data subjects and access requests. One of the reasons for this may be linked to the nonexistent explicit legal obligations in Slovakia for data controllers about publicity and lack of any official guidelines on what constitutes good practice in data protection policy. The sites investigated as part of this research generally provided incomplete information about data protection and subjects'

rights. If information was available, it tended to be general and usually directly quoted or paraphrased parts of the data protection law in Slovakia.

Of the 34 cases in which we successfully located data controller details, this information was located online in 28 instances. However, in most of the cases the quality of information was evaluated as 'poor', as only a limited number of sites offered easily obtainable information about data controllers and rights of data subjects. An extreme example of this may be in the case of the loyalty card scheme operated by a national supermarket chain. The main website of the company does not have a traditional link for privacy or data protection. Although a search function is available, a search for "ochrana osobnych udajov" (data protection) produces only one PDF document with no relevant information. The details were found after over 10 minutes of browsing through the site in and we eventually located in a pdf document entitled "Žiadosť o vydanie náhradnej karty- duplikátu" (Request for replacement card- a duplicate) designed for customers who lost their original loyalty card and sought a replacement.[58]

The information tended to be general, formalistic and usually quoted or paraphrased parts of the data protection law, without attempting to "translate" legal terms into understandable language. We found no observable difference between public and private organizations and the quality of information they provide. Three notable general comments may be made here concerning online content. Firstly, with one exception (the public office responsible Border Control), none of the sites provided online or downloadable templates for access requests, therefore missing an opportunity to facilitate more straightforward processes for access requests. Secondly, the only common feature in these cases was that all websites provided *some* information on privacy policy. Aside from this, websites showed little consistency from one to another. Thirdly, generally speaking, in most of these sites, despite being successful in finding data controller details, there was no notable good or bad practice. For example, the Interior Ministry, the data controller for various public sector sites, provided uneven information under one website, which suggests a lack of internal coordination between various departments of the Ministry. In other words, it seems that data controllers are not necessarily attempting to hide information about privacy, but are more likely to be formalistic, without making an attempt to provide easy access to all necessary information in plain language in one place.

In those cases, where we used phone/in person contact, we faced staff with only limited knowledge on data protection matters. However, they nevertheless attempted to be helpful and in some cases managed to provide us with the assistance needed in order to successfully locate data controller details. As a methodological aside however, in four of these cases (GP, primary and secondary school records, NGO) the members of the staff were familiar with us, which may have influenced their responses. In other words, the fact that we were well known to these people probably influenced our ability to get information we needed without raising suspicion.

Strategies of facilitation

[58] Available at: http://coop.sk/sk/zakaznik/vernostny-program-coop-jednota/nakupna-karta-coop-jednota/ziadost-o-vydanie-nahradnej-karty---duplikatu, Accessed 09/01/2014

What could be considered a good/facilitative practice in context of this country report is the loyalty card of a major department store. We began by visiting their Slovak webpage and, at the obvious place (at the bottom of the front-page), we found a link entitled 'Ochrana osobnych udajov' ("Personal Data Protection"). This section contains several paragraphs that explain various situations in which the company collects personal data and how the data is protected. In comparison to other sites, the company attempts to use plain language which does not copy and paste from legislation and is much easier for a layperson to understand. The page also includes a phone number for more information and a mail address specifically for data request.

Elsewhere, in the case of border control, which comes under the remit of the Interior Ministry, we visited the website of the Interior Ministry. The website demonstrates facilitative practice insofar as the material contained therein had all necessary information about data protection and subject rights, including downloadable templates for access request which had contact details and other necessary information for data request. It was also available in English. However, the problem lies in the fact that the good content was not readily accessible from main webpage, nor straight from using search function (as discussed in greater detail below)

Strategies of denial

Lack of coordination: The Ministry of Interior as data controller

The variations in the quality of information found on public institutions' websites (most of them belonging to the national government) is caused by a decentralized system, where each institution is responsible for their own websites. Therefore, the websites differ considerably when it comes to their design, functionality, interactivity and depth of information. During the course of this research, the quality of information about data protection varied significantly within the website of a single ministry, the Interior Ministry of Slovakia, which is the data controller for various sites that are connected to the data protection legislation (Border control, Vehicle Licensing, Passports, I.D. Cards). The website of the Ministry is an example of an old-fashioned site with a static design with almost no functionality. For all cases it was necessary to use the search function, as the front-page of the ministry did not have a direct link(s) for data protection.

In the case of the ID cards, the search resulted in a specific web address for section on IDs[59]. However the section did not provide any information on data protection. Another link[60] provided a section entitled 'rights of subjects' and this section quoted various sentences from 2002 DP legislation, informing readers that subjects have a right to submit a written request to the Ministry. No specific mail address, contact information, or a form is provided.

The situation was somewhat different in the case of border control. As with the ID cards, there was no obvious link on the front-page and one has to use a search function. Again, a search for strings such as 'border control & data protection' did not produce any useful links. The search for 'personal data' produced dozens of links, but only two of them containing

[59] http://www.minv.sk/?obcianske-preukazy
[60] http://www.minv.sk/?a-z-index&sprava=prava-dotknutych-osob

useful details. The first of these links[61] provided general information about data protection and border control, but included 'dead' links for additional documents that were listed at the bottom of the page. The second link[62] was working and, as discussed above, had all necessary information about data protection and subject rights, including downloadable templates for access request which had contact information and other necessary information for data request. Moreover, the page also links to the Foreign Affairs Ministry webpage[63], which has comprehensive information about data protection and access request with mail and e-mail contacts, as well as providing a template for request and contact details for the Slovak DPA. While this case is an example of a good practice insofar as the data controller providing not only enough information about requests but also downloadable templates and contact information, on the other hand, the content is hidden deep in the website of Interior Ministry and one has to search for a while to get to information. Here then, one experiences both facilitative and restrictive practices simultaneously. The content is excellent but is effectively buried beneath so many obstacles as to render is almost useless. The data subject is essentially forced to dig out this information which inevitably takes time and effort as well as, potentially, some level of existing knowledge or expertise regarding data protection matters in order to filter out the plethora of irrelevant information.

In both cases (IDs and border control), the Interior Ministry provides no easy access to information on data protection and effectively forces subjects to use the search function. A search however performs poorly and offers too many links that have nothing to do with data protection. Once one finds a correct link, the quality of information varies enormously which begs the question: why the differences? One explanation goes back to the Slovakian legal analysis for WP5.1 which argues that the technocratic nature of the harmonization of EU law in Slovakia produced reasonable results in the transposition phase, but is lacking when it comes to the implementation phase. In other words, the law in books is not the problem, the law in real life is. When there is a lack of external pressure to comply, as is case for ID cards, the quality of information is poor. On the other hand, when there is an external actor willing to apply pressure, as was in the case of border control (Schengen, 2007-08), the quality of information is reasonable. In the case of Slovakia, and other new EU member states, entry to Schengen system was postponed until the countries fulfilled additional conditions from the EU. This may also explain why the request forms are provided in English.

Elsewhere, in the case of access to police records, the lack of a systematic communication strategy is also visible when it comes to the information on data protection and access requests to police systems. There is no available information on the website of the Interior Ministry, but the information is instead provided on the website of the DPA[64], together with a mail address for data requests. While in this instance the Slovak DPA fills the void created by Interior Ministry's lack of information, it is the exception. In no other cases does the DPA provide this type of information, so the aforementioned case is an exception, not the rule.

International Sites: Google, Facebook and problem of localisation

[61] http://www.minv.sk/?prava_dotknutych_osob
[62] http://www.minv.sk/?Prava
[63] http://www.mzv.sk/sk/cinnost_ministerstva/politika_ochrany_sukromia
[64] http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=969&buxus=d661ae5ffc66c41b682b69c77f9b2ced

A number of broad problems were experienced in international sites such as Google and Facebook. These included circularity, absence of contacts, and the inability to locate the "right" request form. However, alongside these issues, we experienced an additional level of frustration concerning the localisation of these sites into Slovak. While the main interfaces are usually localised/translated into Slovak, more specific sections are not always offered in Slovak and the user is automatically switched to English or other "big" languages. In the case of Facebook, a user can select the Czech language, which is similar to Slovak and is easily understood by most of the Slovak population (due to the popularity of Czech TV and common state experience). However, this is a "solution" that essentially works by accident and not by choice. Whilst browsing Facebook, we used a wiped browser (deleted all the cookies and history) and used the Slovak version of the Facebook site. The section called "Data requests" was located at the usual place (i.e.: the bottom of the webpage), but when we clicked on the link, the content was not offered in Slovak. However, it was available in Czech, together with a direct link for data requests[65]. We sent a request and within a few minutes we were advised how to download our data. Whether the information we are able to download provides a full account of the data that our Facebook account holds is another matter and indeed previous research as called this into question[66].

In the case of Google, we used a cleared Chrome browser, and typed Google.sk and changed the language to Slovak. At the bottom of the main page, we located a link on data protection[67]. There were several paragraphs of text in two columns. The first is mostly about security, the second about data and legislation, both of them reasonably informative. In the last section there was a link for terms and policies.[68] In the first sentence it informs in Slovak that services are provided by Google Inc.[69] and a U.S. mail address for Google is listed. It is not clear whether the address can be used for data request. Another link[70] directs users to an FAQ which is in Slovak. This reveals a direct link to an online request form about data protection. The link[71] opens a privacy trouble-shooter where the language automatically switches to English. From there, the form is very general and it is not clear what would be the best option for an access request. Moreover, after privacy trouble-shooter automatically switched to English, we attempted to change the language to Slovak but got an error message which redirected us back to the trouble-shooter in English.

In both cases therefore, i.e. Facebook and Google, we encountered a number of denial strategy which were significantly exacerbated by the additional restrictive practice of poor localisation of deeper parts of websites concerning privacy.

CCTV and signage: Who is the data controller?

The sites that operate CCTV also provide additional evidence to the general finding that the lack of legal or good practice guidelines leads to a confusing experience with identification of data controllers and subjects' rights. Part of the problem with CCTV also lies in the legal regulation. Paragraph 2 of the data protection law establishes exceptions and prohibits access rights to the data recorded by video or audio devices (e. g. CCTV). Furthermore, according to

[65] http://www.facebook.com/help/contact_us.php?id=166828260073047
[66] See for example Europe v Facebook.
[67] http://www.google.sk/intl/sk/policies/?fg=1
[68] http://www.google.sk/intl/sk/policies/terms/
[69] So sídlom na adrese 1600 Amphitheatre Parkway, Mountain View, CA 94043, Spojené štáty americké
[70] http://support.google.com/bin/static.py?hl=en&ts=1291807&page=ts.cs
[71] https://support.google.com/policies/troubleshooter/2990837?rd=1

§ 10 (7) of the law "the premises accessible to the public may be monitored by means of a video recording or audio recording only for the purposes of the public policy and security, disclosing criminal activities or interference with the State's security, provided that the premises are clearly marked[72] as being monitored".[73]Moreover, if the recording is not used for the purposes of criminal/misdemeanour proceedings it has to be destroyed within seven days[74] from the day following the recording.

A CCTV system in a public space may therefore operate under different legal regimes. It results in a situation in which two CCTV systems are located next to each other and one will need to be clearly marked while the other not if it operates under a special law. In this scenario, an individual has no idea who might be data controller for a camera with no signage that is mounted on the building of a business centre and pointing at the sidewalk on to a busy street next to the central bus station in Bratislava (see Picture 1).

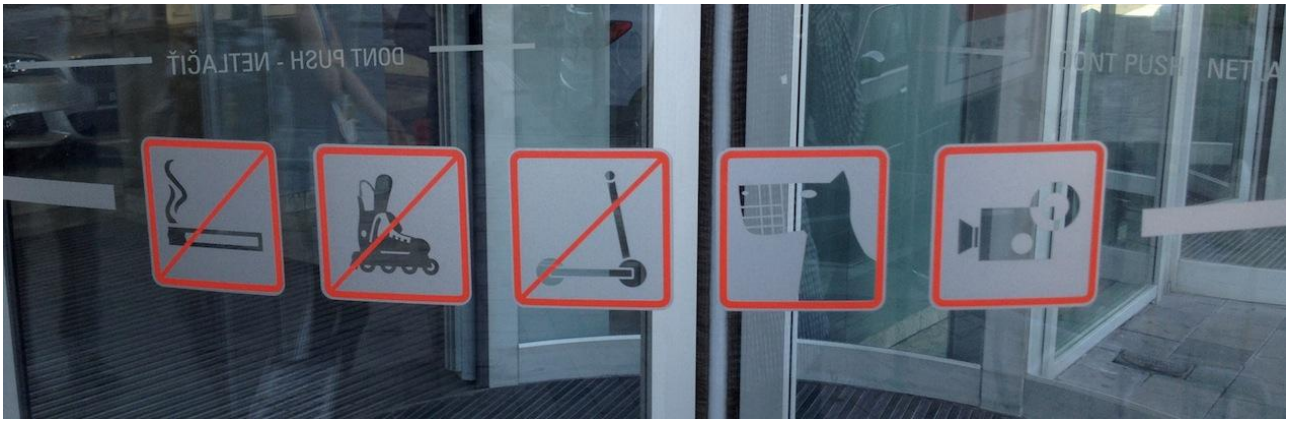
[72] The signage that the premises are being monitored is not required if it is not stipulated by a special law. E.g. law No. 483/2001 on Banks, section 93s(7) " The premises of a bank, branch of a foreign bank and the National Bank of Slovakia, and ATM machines and currency exchange machines not located in the premises of a bank or branch of a foreign bank, may be monitored by video or audio recordings even where there is no notice that the area is under surveillance". For English version of the law see: http://www.nbs.sk/_img/Documents/_Legislativa/_BasicActs/A483_2001.pdf, Accessed 29/06/2013. Or see Act No. 215/2004 Coll. on Protection of Classified Information, § 53 (6) according to which the premises and the protected areas protected by technical security means which allow producing of audio, video or audio-video recordings are not requested to be marked pursuant to the general regulation on personal data protection.

[73] This exception remains unchanged in the new law of 2013, where it is defined in §15 (7).

[74] Unless otherwise stipulated by a special law, e.g. the Law No. 483/2001 on Banks, Paragraph 93a (7) allows for 12 months period. For English version of the law see: http://www.nbs.sk/_img/Documents/_Legislativa/_BasicActs/A483_2001.pdf, Accessed 29/06/2013

Picture 1: Business Centre, Bratislava

If one enters one of the buildings of the company responsible for the business centre, a signage of CCTV, without any details, is displayed on the revolving doors (see Picture 2). There is no clarification of whether the signage refers to the cameras inside the building only or outside as well. When we entered the building, we asked a young woman at the reception who the operator of the CCTV was. She was polite, but did not have any answer. However, she pointed us to a door where the security team had an office to ask. No one responded when we rang the doorbell. As a result, we attempted to locate the data controller of the company using other means and we visited the organisation's website. From the company's webpage it is not very clear as the site referred frequently to the developer of the business centre, which was a different company. We wrote an e-mail to an address which was provided on the website in a section containing general contact information. Within 30 minutes, we received a reply with a name, e-mail and phone number for the security manager of the business centre, who was willing to provide me with additional information. Generally speaking, what is clearly lacking is a general instruction, perhaps provided by the DPA, on what should be included on the signage and how the data subject may identify a data controller. One is confronted with various pictograms that lack any information whatsoever and seem to be purely of aesthetic value (see Picture 2).



Picture 2: Business centre building, Bratislava

In only one site, the Central Bus Station in Bratislava, did signage include at least some information about data controller (see Picture 3): 'this CCTV is operated by the City Police of Bratislava'. At the entrance of the bus station, there were three stickers informing data subjects that CCTV was monitoring the area. Two of these stickers included information that the City Police of Bratislava operated the CCTV. Inside, in the main hall, we found another three stickers with a camera pictogram, without any additional info about the operator.

Picture 3: The signage at the Central Bus Station: "This area is monitored by CCTV system of City Police". Mlynské Nivy, Bratislava

We visited the website of the City Police in Bratislava[75]. At the main page there is nothing about data protection, only a central column with contact details. We used a search function

[75] http://mestskapolicia.bratislava.sk/

and found a short article[76] about CCTV entitled "CCTV in the city is not for fun". The article outlines why CCTV is used in Bratislava and explains that legal restrictions do not allow individuals to request their data. It also mentions that citizens has in the past complained to the City Police that cameras in the city are not clearly identified. The article responds by pointing to the Local Police Law which allows this practice. It is obvious from the article that the City Police receives questions about CCTV cameras in the city, but again the lack of a proactive communication strategy means that citizens are left without any clear sense what is their legal status vis-a-vis CCTV in the city and their respective legal rights.

A comparably worse experience was found in the case of CCTV in a department store in Bratislava. CCTV signage was located at the entrance (sliding doors) together with other information about opening hours, the name of the manager, mail contact for the company's local branch and signage for the security team operating in the store (see Picture 4).

Picture 4: CCTV located at department store's entrance

We asked a member of staff where we could find any information on who the operator of the CCTV in the store is and we were referred to the website of the company. The website has some information about privacy and data protection, but they were related only to web browsing rather than *all* types of data collected by the company. We therefore had to use an online contact form and ask about CCTV in the store. We received a reply by e-mail the next working day from the manager of the store, who described our e-mail as confusing and replied that "the details of security are a private matter of the company".

In only one instance was the identification of data controller straightforward. In our local bank, we asked security officer for information about the data controller for CCTV installed outside and inside bank, and was provided with necessary details. In this case therefore, the organisation illustrated facilitative practice insofar as the security officer held sufficient data protection knowledge to enable him to answer our query satisfactorily.

Concluding remarks

[76] http://mestskapolicia.bratislava.sk/vismo/dokumenty2.asp?id_org=700011&id=1019&p1=1019

A range of both facilitative and restrictive practices were therefore experienced as part of this research. The majority of successful cases were completed online but this should not be taken to mean that online content was good. In several cases, the content online displayed neither especially good nor bad practice but simply provided a minimum amount of acceptable information. Some sites, in particular the Interior Ministry, displayed both facilitative and restrictive practices simultaneously by providing a good depth of information regarding access rights but 'hiding' this information amongst several pages of irrelevant content.

Non-online interactions showed that data controller representatives often lacked the requisite data protection expertise to answer our questions but nevertheless endeavoured to help. Whether this was due to our status with these respondents is unclear however. In cases of CCTV, the law in Slovakia appears to lack clarity and this was reflected in the mixed practices of the sites visited. Some sites did not display any signage whatsoever whilst others displayed signage lacking any contact information. In only one instance was a member of staff able to provide us with clear, unequivocal advice about the identity of the CCTV operator.

With these experiences in mind therefore, we argue that there is a substantial window of opportunity for the Slovak DPA to establish what constitutes good practices when it comes to public relations in data protection, either by actively providing templates for data controllers, or by using its power to control how data controllers implement legislation.

SUBMITTING ACCESS REQUESTS IN SLOVAKIA

Introduction

This country report reflects the experiences of submitting 19 subject access requests, seven addressed to public data controllers and 12 to private. To date, 16 responses have been received and three remain without any response, even after repeated requests (e.g. CCTV in a public space; Google and Facebook). Out of 19 requests sent, five concerned CCTV footage. While the results outlined below do not claim to reflect all practices and approaches of organisations in response to subject access requests, the chosen sample is nevertheless reflective of domains with and in which citizens interact on a systematic and consistent basis. Thus, the overall trends observed as part of this research may be indicative of the experiences citizen encounters when submitting a subject access request in Slovakia.

Overall Summary

As Slovak data protection law explicitly requires submitting access requests in written form, in all our cases we sent registered letters to data controllers. With one exception, where the letter sent to Vehicle Registration Office was returned twice, no other letters were sent back to us, meaning that they were delivered to postal addresses we identified as belonging to data controllers. While we provided an email contact address for responses, in cases where requests needed additional explanations, most of the communication was conducted through registered mail. On one hand, this legal limitation restricts the availability of choices for data subjects. On the other hand it makes subject access request more formal and leaves a "paper trail" that can be referenced more easily than phone calls or emails, but also used more efficiently as evidence in case a subject wishes to file a complaint with the Slovak Data Protection Authority.

The subject access request procedure in our research was regulated by the 2002 Data Protection law. However, a new law was passed by the parliament in 2013, to be effective from January 1, 2014. The 2013 law does not change the nature and regulation of subject access rights, but places various administrative demands on data controllers and data protection officers. The temporary coexistence of the two laws did create some confusion in legal references provided by some data controllers in their responses. For instance, both the department store responsible for a loyalty card scheme and the mobile phone carrier referenced repeatedly to the new, not yet effective legislation in our conversations.

In three cases, we submitted the access request in the name of another person (wife) due to her ownership of loyalty cards for a large department store, a supermarket and a small store.

While we attempted to follow-up all unsatisfactory or incomplete responses with additional questions by mail or phone, we decided to file a complaint with the DPA only in one case (mobile phone carrier). There were several reasons for this; one has to do with our relative visibility as a researcher in Slovakia due to repeated appearances on TV and radio. Secondly, we had to contact the local DPA repeatedly in 2013, for a case study in IRISS WP3. Thirdly, we plan to continue research on data protection in future outside of the scope of the IRISS project, with the intention of preparing some policy proposals to change data protection policy in Slovakia. Due to these facts, we felt that aggressive follow-ups and repeated complaints to the DPA, when the Slovak DPA deals with only few complaints a year, is not the best long term strategy and could jeopardise our future access to the Slovak DPA.

The 2013 Data Protection law on data protection, which is intended to regulate access rights as of January 2014, states that:

> (1) The controller shall be obliged to satisfy the data subject´s request under Section 28 Paragraph 1 Points a) to c) and h) and Paragraphs 3 to 5 free of charge.
>
> (2) The controller shall be obliged to satisfy the data subject´s request under Section 28 Paragraph 1 Point d) free of charge, except for a fee in the amount not exceeding the amount of material costs accrued in connection with the making of copies, providing technical carriers and sending the information to the data subject, unless otherwise stipulated by a special Act.31.
>
> (3) The controller shall be obliged to satisfy the data subject´s request under Paragraphs 1 and 2 in written form not later than in 30 days' from the date of delivery of the request.

	Site	**Data controller**
1	Public	CCTV in an open street
2	Private	CCTV in an open street
3	Public	CCTV in a transport setting
4	Public	CCTV in a government building
5	Private	CCTV in a bank
6	Public	Local authority
7	Public	Border Control
8	Public	Vehicle licensing
9	Public	Europol
10	Public	Police criminal records
11	Private	Banking records
12	Private	Loyalty card (department store)

	Site	**Data controller**
13	Private	Loyalty card (supermarket)
14	Private	Mobile phone carrier
15	Private	Facebook
16	Private	Google
17	Private	Loyalty card (department store)
18	Private	Loyalty card (department store)
19	Private	Advanced passenger information

Public - Facilitative/Good practice

Local Authority

Our request was made to the Office of the Municipality in a form of registered letter. As this request was made in late November 2013, it also included, proactively, a photocopy of the front page of the ID card of the researcher. The initial problem with the access request stemmed from the fact that it was unclear to the researcher in what situations the municipality did act as a data controller and in what types of databases our data were held. Therefore the request was formulated only generally, asking for any information on personal data in the databases of the local authority, plus two additional questions on third party sharing and automatic decision making.

The response was received on 19/12/13, well within the legal period, by a registered letter. The letter started with quote from our request that included all three questions addressed to the data controller. The response addressed fully the first question on what personal data are held in the databases of the municipality. As for the question on the third party sharing, it was addressed for all five databases operated by the organisation by listing parties that are legally entitled to obtain our data from databases of municipality, e.g. Police, Statistical Office, Tax Authority. The municipality however did not provide further details on what was shared and when. The wording of the answer suggested that our data was not shared yet. The question on automated decision-making was answered also for all databases; however, the answer did not address the processing logic. In all five cases, our personal data existed both in electronic and physical form, therefore was subjected to some automated decision-making. In addition, the data controller explained how these are databases are protected (three level passwords, separate IT room with controlled access, locked file cabinets). We followed up the automated decision-making answer with a phone call to the municipality officer, and were provided with

answer that repeated the written answer and added that the data controller uses both automatic and manual-filing systems that are not processed further.

Overall we identified two facilitative strategies in municipality's approach. The letter itself was sent with a requirement that it should be signed for upon delivery (meaning that it cannot be picked up by a family member for example). This demonstrates high levels of data protection awareness insofar as protecting our personal data enclosed in the letter. Secondly, the fact that the data controller quoted our questions at the beginning of its response could also be considered as facilitative strategy which demonstrates a willingness to address our request in full, but also serves as a reminder to data subject of what was asked in the original request and to the data controller of what needs to be answered in the response. In quoting from our letter, the data controller therefore addressed all parts of our query without completing ignoring any section. Although the responses we received may not be deemed wholly satisfactory, the general approach of at least attempting to answer each of our questions is nevertheless commendable.

Border Control

Our request was made to the Police Force of Slovak Republic, National Headquarters of SIRENE that administers the Schengen Information System for Slovakia. This was the only case out of 19 in which the data controller in our sample provided complete contact details together with downloadable subject access request templates.[77] While templates were not easy to find through the organisation's website, a search for "SIRENE request" via Google produced a second rank link that directly provided all necessary details. Although we did not use the template provided by the website, we had to change legal references in our original template as the SIRENE subject access request is regulated by the Law on The Police Force of Slovak Republic No. 171/1993 Coll. The request was sent by registered mail, together with photocopy of our ID and passport. The data controller responded within two weeks and informed us that no data on us were held in the SIRENE system. The data controller did not address our questions on automatic decision making, preferring instead to make reference to the Law on the Police that establishes narrower access to personal data. In this case, the data controller facilitated easier access for subjects by providing easily downloadable templates that were available both in Slovak and in English. Specifically, these forms included information on the need to provide a copy of ID or passport as a proof of identity, minimizing delays in submitting a complete request and making the access request procedure very clear. Moreover, the response was provided in a timely manner and according to legal guidelines.

Europol & Police criminal records

We sent a registered letter at the end of September 2013 to the national Police force and received a response within the legal period of 30 days. In both cases, the data controller stated that there were no personal data about us stored in databases of Europol and the Slovak Police respectively.

Public - Restrictive practice

Vehicle licensing

[77] Available at: http://www.minv.sk/?Prava, accessed 14/03/2014

Our request was made to Regional Transport Office of the Police Force that administers vehicle licensing in the region of Bratislava. We located only general contact information via the website of the Slovak Police Force. This was in the form of a postal address and we therefore sent a registered letter at the end of September 2013. The letter was returned to us after four weeks due to the fact that the recipient did not pick up the letter. We sent a second registered letter and once again, no response was received within four weeks. After calling the general phone number for the Regional Police Force Office in Bratislava we were advised to send our request to the Regional Police Force Office general postal address. Our third attempt was made in the middle of December 2013 and we received a reply via registered letter on January 16, 2014, within the legal period of 30 days. The reply acknowledged our data was held in four databases of the Police Force, but only two of them were connected to the subject of our request (database Traffic Administrative Agenda; database Vehicle Evidence).

The response addressed the content of the data held via references to specific sections of several laws that regulated evidence of IDs and vehicle licensing. As to the issue of third party data sharing, the response once again referenced the section of the legislation that regulated third party access, but also explicitly stated "that there is no evidence that our data were shared or accessed by a third party". The automatic decision-making issue was addressed only generally, by references to respective laws. In spite of the fact that the actual response was received within the legal period and addressed most of the questions asked in the request, the inability to easily locate contact information for the data controller resulted originally in two failed attempts to deliver request. This has to be considered as a restrictive practice given the significant delays incurred here. Also restrictive is the extensive referencing to the sections of various laws that regulated what data is held on vehicle owners, instead of providing actual records (e.g. Name and Surname, Date of Birth, Permanent Residence, Type of vehicle, etc.). This use of legal jargon made the reply received from the data controller unclear and potentially difficult for a data subject without legal training or data protection expertise to understand. Also, confusingly, the reply addressed our personal data held in other databases operated by the Regional Police, although our request demanded only data connected to vehicle licensing. We therefore had the impression that our request had not been closely examined but rather that the data controller had replied somewhat haphazardly, without carefully examining the specific content of our request.

<u>Private - Facilitative Practice</u>

Banking Records

The request was made to one of the largest banks in Slovakia. Besides the checking account, we use other services of the bank as well, i.e. credit card, savings account and mortgage. While the request was made to access personal data relating to the checking account, the response addressed all bank products that are in our name, therefore making a separate request for credit card records unnecessary. It is also necessary to mention that all data on checking account transfers and history is available for free via our online banking account. The same applies for credit card records. A registered letter was sent to the general headquarters of the bank in Bratislava to an address listed on the bank's website in the privacy section. The letter was delivered on September 30, 2013; the response from the bank in a form of regular letter was received on October 29, 2013, therefore within the statutory time period.

The organisation addressed all three questions from the request. Regarding the personal data held by the bank, a list of 30 categories of information that were processed by the bank were included, such as name and surname, birth number, telephone number, family status, number of kids, net monthly income etc. The bank also addressed third party sharing and explained what type of data is shared, why it is shared and named two companies with whom data is shared (one organisation in the public sector and one in the private sector). In both cases, full contact details in the form of postal addresses were provided for these third parties. In the third case, our data (name, surname and birth number) was shared with a private insurance company that provides credit card insurance. Once again, contact details were provided. As for automated decision-making, the bank answered that it uses automated decision making "that is based on principles of security, trust and with the respect for data protection". While the bank addressed the question, the content of the answer was general and did not provide specific information on the nature of automated decision making and its logic. Overall the bank's approach included several facilitative strategies. They provided both the data itself and the legal reasons for the retention of this data on the bank's database; they fully addressed third party sharing (to whom, what and why), together with providing contact details provided for companies which simplifies matters for data subjects in case they want to make additional requests; and online access to complete banking records via the internet is available free of charge.

Loyalty Card (department store)

This case was one of the few sites in this research that provided well-explained information about privacy and data protection on its website, as well as direct contact information for their data protection department. A registered letter was sent on September 20, 2013. Having received our letter, the company acknowledged our request on September 26 by an email and informed us that they plan to reply within the legal period. With one exception (the mobile phone carrier), this was the only instance in which a data controller acknowledged our request, displaying a good level of self-accountability and clear communication with the requester.

We received a letter from the company’s Slovakian office on 14/10/13, well within the legal period. The two-page document fully addressed our first two questions, and provided some information for automatic-decision making. The reply included information on the name of the information system in which the company stores our data, explained reasons why this data is kept in the database and provided a list of our personal data in the system. The letter also directly addressed the fact that our personal data has not been shared with third parties, but acknowledged that data processing by other organisations for the company does take place. A full list of companies that process our data for the company was included (seven organisations in total), with contact details for every company as well as the reasons for processing our data. As for automatic decision-making processes, the company acknowledged its use and provided additional information on the security of the information system and the existence of a security project required by law. In a recent interview with the economic weekly publication Trend, the general director of the company for our region addressed the use of information gathered from the company’s loyalty card scheme in Slovakia. When asked whether the company can create individualized offers for its customers, as another large department store company does, director replied: "*We are not at that level. We can find age group of a customer, what they buy most, from where they travel to our shop (there is only one store in Slovakia) and how much they spend. But we do not*

have detailed information that would allow us to pick an individual customer and identify what he buys and how much he spends."[78]

Overall the department store demonstrated several strategies of facilitation, from clear and unambiguous contact details for access requests, email confirmation upon receiving our request, to full details on third parties that processed our data.

Loyalty card (supermarket)

The data controller for is an international drugstore chain that operates dozens of facilities all around Slovakia. In our research sample, it was the only data controller that fully addressed all three questions from our request in the first reply. A registered letter with our request was sent on 24/09/2013. The answer was firstly received via the email address we had provided in our original request and was soon followed by a registered letter on 21/10/2013, within the 30-days legal period for reply. The data controller structured the reply by quoting the exact wording of our questions and addressed them point-by-point. For the first question, the answers covered the access scope as defined by the section 15 of the data protection law, i.e. the name of the data controller, the purpose of the data processing and the categories of our personal data processed by the organisation. The loyalty card is connected to an online account that provides all details on transactions in which the loyalty card was used and specifics of personal data stored in the company's database. As for third party sharing, the reply acknowledged its existence, explained full reasons for sharing, the extent to which this takes place and provided contact details for two companies with whom our data is shared. As for the third question on automated decision-making, the reply provided:

> "a confirmation that the company uses database software that collects data on our purchases (i.e. date and time of purchase with loyalty card, content of the purchase, place of purchase). All data are collected together with anonymised information, i.e. our ID number of customer for purposes of Marketing program, e.g. identification of needs of customer, optimization of procedural operations of company, distribution of marketing materials, test samples, including phone control for delivery of packages, distribution of electronic newsletter, etc."

Within the context of our sample, the reply from the company could be considered as a model one, as it was received within the legal limit, included full disclosure of personal data, and provided a satisfactory response concerning the details of their automatic-decision making processes. Therefore all necessary information was received in a single correspondence, saving both the time and money needed for follow-up correspondence.

Loyalty Card (department store)

The company in question is a Slovak toy chain that provides loyalty cards to its customers that allow them to buy merchandise for "special" prices that are usually 7% lower than without using the card. As in other cases, a registered letter was sent at the end of the September to the data controller. A reply, sent by registered letter, was delivered within the 30 days legal period. The data controller used an external law firm to deal with our request and informed us that no personal information were stored in their system due to the fact that

[78] See: Ako funguje svet Ikea (How World of Ikea Works), Trend.sk, 17/03/2014, available at: http://firmy.etrend.sk/firmy-nefinancny-sektor/ako-funguje-svet-ikea-prilis-sebavedomi-a-arogantni-u-nas-nepreziju.html, accessed 17/03/2014

the card number we used as an identifier in our request was not connected to our or any other name as the company uses non-personalized loyalty cards.

Private – Restrictive Practice

Google and Facebook

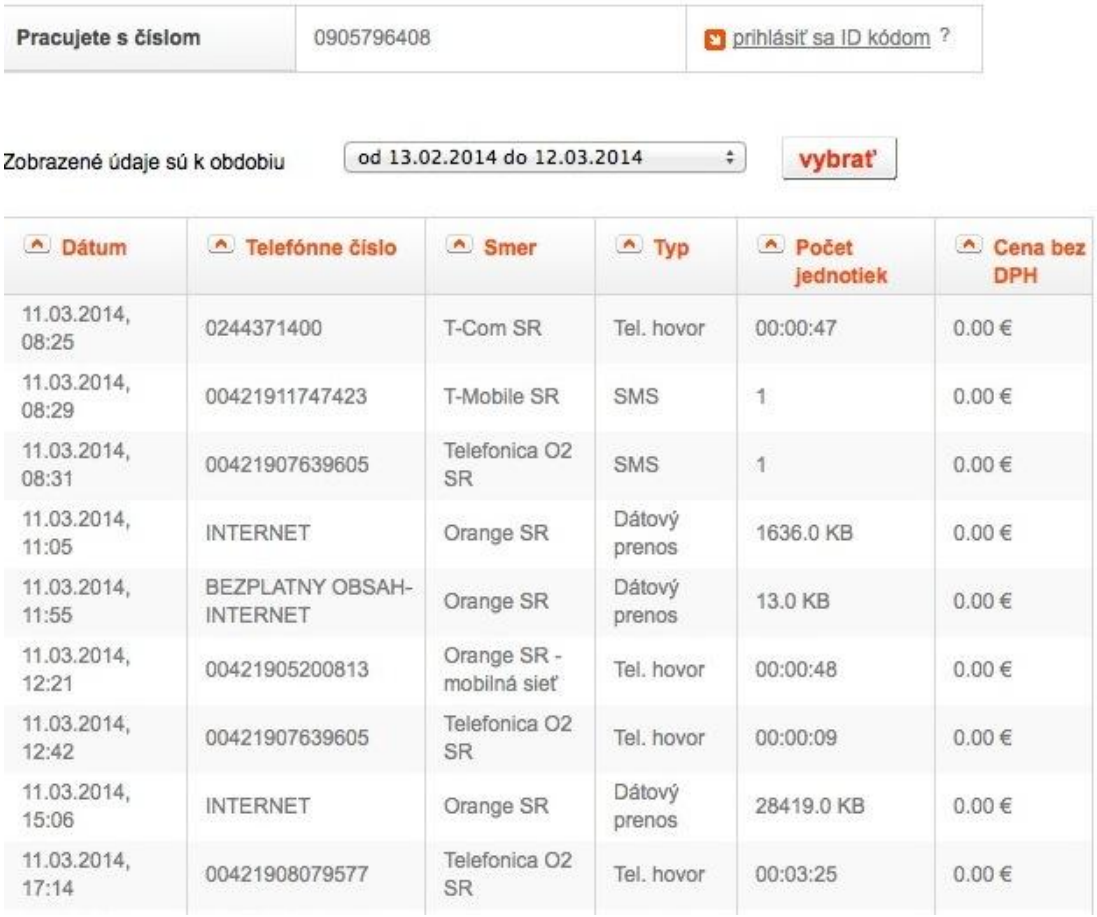
In both cases, requests were sent in late October 2013 by registered mail to general addresses in California, USA (Google) and Dublin, Ireland (Facebook), as neither of these organisations have official representation in Slovakia. In both cases requests were made in Slovak language. To date neither Google, nor Facebook responded to our request.

Mobile Phone Carrier

In this case we started our access request by visiting the official website of the carrier which is the biggest mobile carrier in Slovakia with 2.8 million customers. The website does not have privacy policy section at all. A search for "privacy policy" produces dozens of links, some of which include legal documents that have some information on privacy and also provide contact details for data controller. The online content of the website therefore demonstrates a restrictive approach by not providing a privacy policy section and direct contact details for the data controller. Further restrictive behaviour was demonstrated by the organization when dealing with our request. The request was sent by registered mail at the end of the September 2013 and although customer services contacted us by the phone to confirm that they received our request in early October, the response itself was received only on 20/11/2013, three weeks outside the legal period. This was the only occasion in our research when a data controller located in Slovakia failed to comply with the 30 days legal period.

The reply explained the type of data held about us and legal and contractual reasons for it, but no comprehensive personal data was included. The website of the company allows customers to log into their accounts where they can see some of the data held by the company, e.g. name, address, type of contract, list of services activated, and last month's data (see picture 1) on incoming and outgoing calls (date, number, length, type). But this data is far from being complete and does not include all metadata, e.g. localization information. The third party sharing issue was addressed only in general terms. The organization stated that due to our decision not to make our phone number private the number was shared, together with our address and full name with publishers of public phone directories, other companies that provide information services about phone directories and other persons through the information phone line operated by the company. The letter also explicitly mentioned that third party sharing for specific purposes (public security) is outside the scope of our legal rights. However, this assertion was made without providing any legal arguments based on the current DPA law. Automated decision-making was only acknowledged briefly and it was explained to us that "due to the number of customers it would not be possible to use other methods". The response concluded with the declaration that "processing our data by automated process is done according to the legislation and does not have negative impact on our legal rights." Given that the reply failed to address the issue of metadata, we responded with an additional request that was once again sent by registered mail. In this request we specified what we meant by personal data and referenced the relevant section of the telecommunication law that provides specifics on what is collected by mobile carrier.

A second reply arrived within the legal period of 30 days at the end of December 2013. In it, the data controller argued that the legislation obliges data controllers to provide only a "list of personal data that is processed by the organization", not the data itself. However, this reply referenced new legislation that was effective from January 1 2014, while our subject access was filed under the old legislation. There is a slight difference in the wording between the old and the new law. The new law allows subjects to access only a "list of personal data", while the old law enables access to a "copy of personal data that is subject of processing". The organization also stressed that our personal data is accessible through the website. In addition, the company refused to grant access to operational and localization data because they argued that this falls outside of the access rights of a data subject and is covered by a public security exemption. As a result, we submitted an official petition to the Data Protection Agency, seeking the agency's position on both the legislative wording problem between old and new law and also the refusal to grant access to metadata by the company. To date, we have received no response from the Slovak DPA.



Pracujete s číslom	0905796408	prihlásiť sa ID kódom ?

Zobrazené údaje sú k obdobiu od 13.02.2014 do 12.03.2014 vybrať

Dátum	Telefónne číslo	Smer	Typ	Počet jednotiek	Cena bez DPH
11.03.2014, 08:25	0244371400	T-Com SR	Tel. hovor	00:00:47	0.00 €
11.03.2014, 08:29	00421911747423	T-Mobile SR	SMS	1	0.00 €
11.03.2014, 08:31	00421907639605	Telefonica O2 SR	SMS	1	0.00 €
11.03.2014, 11:05	INTERNET	Orange SR	Dátový prenos	1636.0 KB	0.00 €
11.03.2014, 11:55	BEZPLATNY OBSAH-INTERNET	Orange SR	Dátový prenos	13.0 KB	0.00 €
11.03.2014, 12:21	00421905200813	Orange SR - mobilná sieť	Tel. hovor	00:00:48	0.00 €
11.03.2014, 12:42	00421907639605	Telefonica O2 SR	Tel. hovor	00:00:09	0.00 €
11.03.2014, 15:06	INTERNET	Orange SR	Dátový prenos	28419.0 KB	0.00 €
11.03.2014, 17:14	00421908079577	Telefonica O2 SR	Tel. hovor	00:03:25	0.00 €

Picture 1: An illustration of data available on the mobile phone carrier's website

Loyalty Card (department store)

A registered letter was sent to the general address provided at the webpage of the department store at the end of September. A reply was received within the legal period of 30 days. The data controller addressed all three questions from our access request. However, only two of our queries were answered in any detail, namely the disclosure of our personal data stored and information on data sharing with third companies. As for automated decision making, the

data controller answered only in general terms by referencing to passages from the relevant legislation which outlines that a data subject may object to automated decision making if it results in a decision that has legal or serious impact on the data subject. Since this was not the case in our situation, we are unable to object to such practices according to this legal interpretation.

Advanced Passenger Information

A registered mail in Slovak was sent to an airline company's Privacy Office in the Netherlands based on the fact that we used the airline in 2012 for a trip to the United Kingdom. The company's privacy officer contacted us on 9/10/13 by email, written in English and asked us to provide more details, as they were unable to process our request further. We replied a few days later, in English, and provided more details on our flight (e.g. destination, e-ticket number). A few weeks later we received a registered letter in English that informed us that "the use and disclosure of this information is in accordance with (the airline's) general conditions of contract we agreed upon at the moment of purchasing a ticket". The letter included a copy of our email conversation and two pages of our data stored in the company's system. While we received our personal data therefore, we found some restrictive practices here insofar as the data controller's reply was in English and appeared to assume that we could also speak English.

CCTV and signage

This part of our research was limited due to the nature of restrictive legal regulation of CCTV in Slovakia. The DP law does not grant access rights to CCTV footage (i.e. the data recorded by video or audio devices) due to an exemption in the law. With this limitation in mind, we submitted five requests to various sites (public/private) in order to find out how data controllers respond to access request for CCTV footage. In an ideal scenario our expectation was that data controllers would respond to our requests, denying access but explaining the restriction of access rights for CCTV footage as defined by the DP law.

Generally speaking, CCTV signage in cases in which we submitted access requests were problematic and could be considered as poor practice. This finding reinforces our experiences whilst attempting to locate data controllers, in which we argued that neither the data protection law[79], nor the Slovak DPA provide necessary guidelines where signage should be placed and what should be included on the signage itself, which leaves location and content of signage in the hands of CCTV operators.

[79] Although the DP law demands that premises have to be clearly marked as being monitored, it also allows numerous exemptions for specific laws.

Notification via signage that premises are being monitored is not required if it is not stipulated by a special law. E.g. law No. 483/2001 on Banks, section 93s(7) " The premises of a bank, branch of a foreign bank and the National Bank of Slovakia, and ATM machines and currency exchange machines not located in the premises of a bank or branch of a foreign bank, may be monitored by video or audio recordings even where there is no notice that the area is under surveillance". For English version of the law see: http://www.nbs.sk/_img/Documents/_Legislativa/_BasicActs/A483_2001.pdf, Accessed 29/06/2013. Or see Act No. 215/2004 Coll. on Protection of Classified Information, § 53 (6) according to which the premises and the protected areas protected by technical security means which allow producing of audio, video or audio-video recordings are not requested to be marked pursuant to the general regulation on personal data protection.

Picture 2: CCTV operated by the City Police

As an example, a CCTV camera operated by the City Police at the corner of one of the main squares in Bratislava, which was subject of our request, lacked any signage. However, the presence of another CCTV camera operated by the City Police at the Central Bus Station is indicated by several signs at the entrance. As a result, this legal and enforcement vacuum results in huge variations in locations and content of CCTV signage and, ultimately affects not only the ability of individuals to identify operators of CCTV, but also their public accountability.[80]

CCTV in a government building; Open street CCTV in city centre; CCTV in transport setting

In these three cases, we received full and legally correct explanations as to why our access requests were denied, citing specific provisions of the DP law. All three responses cited §15 of DP law that regulates use of CCTV and explained in detail that footage was recorded solely for purposes of criminal prosecution and therefore could be accessed only by police authorities. All three responses also informed us about the 15 day period for retention of footage after which it will be destroyed. As an additional indicator of good practice seeking to protect our data, the response from Transportation Company Bratislava also informed us that a copy of our ID which we had attached to the request would be destroyed. As such, although we did not obtain copies of the footage, since Slovak law does not allow this, these responses represented good practice since they were enlightening, courteous and legally compliant.

CCTV in a bank

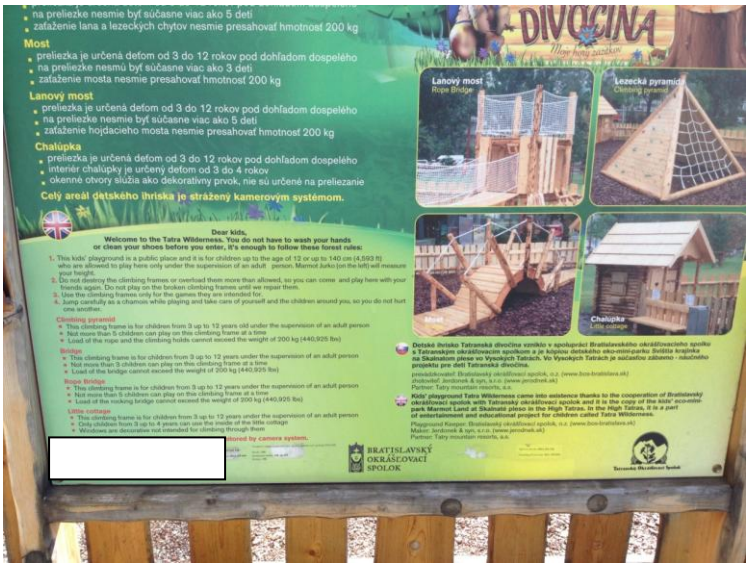
In one case (CCTV in an ATM machine located inside a bank) we received a response denying access to CCTV footage due to the fact that we were not a customer of the bank; therefore the bank was not able to identify us. Because of this, we were apparently "not fulfilling personal criteria according to DP law". We replied to this response with an e-mail to the contact identified in the bank's letter, in which we included a copied proof of our

[80] E.g.: In one of the projecs that were prepared as a part of the course on surveillance at the Comenius, students mapped CCTV in the center of the Bratislava, an area that included several streets. Out of the 187 cameras that were identified, 19 were operated by the City Police, the rest by other subjects.

identity (ID card) and explained that we used an ATM machine of the bank, and therefore entered into "contract" with the bank. Despite several subsequent e-mails, our query has gone unanswered to date.

CCTV in a public space (private)

In the last case, we attempted to obtain CCTV footage from an outdoor playground in a modern shopping and residential centre in Bratislava. Although the CCTV was not immediately visible to the naked eye, the information panel at the playground stated that the premises of the playground were monitored by CCTV.



Picture 3: Information panel at the public playground

The panel also included contact information for the operator of the outdoor playground, an NGO based in Bratislava. Our registered mail went unanswered; the same applied for the phone call to the number provided on the information table.

Concluding thoughts

Only one data controller in our sample provided an access request template (Ministry of Interior for Schengen Data), and even in this case, finding the template was not straightforward. Lack of facilitative practices in guidance was also evident in the poor quality of information within privacy policies, specifically concerning access requests. In most of the cases we were forced to use general contact details for data controllers as no specific contact information for access requests was provided. In one case, (vehicle registration) we thought that we had located the data controller, but two of our registered letters were returned by the post office. In a third attempt, we used a general contact address for the regional police office and were provided with an answer within the legal period.

SIGNIFICANCE OF FINDINGS - SLOVAKIA

Evidence gathered in this research points to the fact that receiving subject access requests is still a rare occurrence for data controllers in Slovakia. For example, when accessing our police records, the letter demanding that we provide a proof of our identity was signed by a very high ranking official of the Slovak Police Force, which would suggest that our request was rare and exceptional and therefore had to be dealt with at a higher level of chain of command than may be expected.

We also noted that Slovak law does not strictly oblige subjects to provide proof of their identity when making access requests. In the case of the access request to police records however, we were requested to provide proof of our identity in a form of registered signature. On the one hand, this could be considered a good practice that protects our data and provides additional security. On the other hand, as there is no clear legal basis for such a demand, this enhanced protection creates additional expenses for data subjects that are not envisaged by the law and delays responses to the actual request. As such, there is a significant space for improvement and clarification here that would result in full and unambiguous guidance from the Police, which would streamline the subject access request procedure and save both time and money for data subjects.

Despite numerous shortcomings in the process of submitting requests, the actual responses from data controllers were in most cases of a professional standard and were answered within the legal period of 30 days. However, there were notable differences in ways in which organizations addressed questions that were included in our requests. While most responses to our first question (on personal data) were to the point and mostly complete, responses to our second question were more varied and several data controllers failed to specify either details for third parties or instances during which our data was shared. The most diverse responses were recorded with our question concerning automated decision making processes. Several organizations acknowledged the use of automated decision making, but failed to provide more details. Several organisations (e.g. municipality, bank) elaborated more on security aspects of their databases and stressed the existence of security projects for data protection. Only one organization (the supermarket operating the loyalty card scheme) addressed the question directly and provided satisfactory details on automated decision making. It also has to be stressed that it is not clear how far subject access rights go under Slovak data protection legislation in this area. The law provides a relatively specific scope of access rights and its content, which does not address automated decision making explicitly. The exact scope of subject access rights would have to be tested in front of the Slovak courts, as the national DPA does not have any official position on this.

References

Article 29 Working Party (2008), 11th Annual Report of the Article 29 Working Party on Data Protection, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf, (accessed 14 July 2013).

City Police of Bratislava, http://mestskapolicia.bratislava.sk, (accessed 8 January 2014)

Constitutional Court of Slovakia , Case IV. ÚS 40/03, available at: http://portal.concourt.sk/Zbierka/2003a/190_03a.pdf, (accessed 25 June 2013).

Constitutional Court of Slovakia, Case IV. ÚS 44/00, available at: http://portal.concourt.sk/Zbierka/2001a/10_01a.pdf, (accessed 13 July 2013).

Constitutional Court of Slovakia, Case PL. ÚS 1/09, available at: http://portal.concourt.sk/Zbierka/2011a/1_11a.pdf, (accessed 25 June 2013).

European Commission (1997), Agenda 2000, Commission Opinion on Slovakia's Application for Membership of the European Union, available at: http://ec.europa.eu/enlargement/archives/pdf/dwn/opinions/slovakia/sk-op_en.pdf, (accessed 25 June 2013).

European Commission (1999), Progress Reports from the Commission on Progress towards Accession by each of the candidate countries, October 13, 1999, available at: http://ec.europa.eu/enlargement/archives/pdf/key_documents/1999/slovakia_en.pdf, (accessed 27 June 2013).

European Commission (2001), Regular Report on Slovakia's Progress Towards Accession, 2001, available at: http://ec.europa.eu/enlargement/archives/pdf/key_documents/2001/sk_en.pdf, (accessed 15 July 2013).

European Commission (2003), Comprehensive monitoring report on Slovakia's preparations for membership, available at: http://ec.europa.eu/enlargement/archives/pdf/key_documents/2003/cmr_sk_final_en.pdf, (accessed 28 June 2013).

Falkner, Gerda, Treib, Oliver (2008), Three Worlds of Compliance or Four? The EU-15 Compared to New Member States, In: Journal of Common Market Studies, Vol 46(2) pp. 293–313

Foreign Ministry of Slovakia, http://www.mzv.sk, (accessed 8 January 2014)

Google, http://www.google.sk, accessed 08/01/2014

Interior Ministry of Slovakia, http://www.minv.sk, (accessed 8 January 2014)

Láštic. Erik (2013), The report for IRISS WP4 on general history of surveillance in Slovakia, IRISS project, 7.FP, unpublished manuscript

Law No. 122/2013 Coll. on Protection of Personal Data, in English, available at: http://www.dataprotection.gov.sk/buxus/docs/Act_12213-en_1.pdf?buxus=b2d2c8fe581c72242fad72dd73c45843, (accessed 8 January 2014)

Law No. 428/2002 Coll. on personal data protection as amended by the Act No. 602/2003 Coll., Act no 576/2004 Coll., Act No. 90/2005 Coll. and the Act No. 583/2008 Coll.

Law No. 483/2001 on Banks, in English, available at: http://www.nbs.sk/_img/Documents/_Legislativa/_BasicActs/A483_2001.pdf, (accessed 29 June 2013)

Linklaters (2013), Global data protection legislation, available at http://www.linklaters.com/pdfs/mkt/london/2013_Data_Protected_PDF.pdf, (accessed 19 July 2013).

Privacy International (2010), Report: Slovakia, available at: https://www.privacyinternational.org/reports/slovakia/iv-governance-issues, (accessed 11 July 2013).

Slovak Data Protection Agency, http://www.dataprotection.gov.sk, (accessed 8 January 2014)

Slovak DPA (2005), The 2004 Annual Report, available at: http://www.dataprotection.gov.sk/buxus/docs/status_report_2004.pdf, pp. 34-35, (accessed 11 July 2013).

Slovak DPA (2006), Opinion on birth numbers, available at: http://www.dataprotection.gov.sk/buxus/docs/MSSRst150306v2.pdf, (in Slovak), (accessed 25 June 2013).

Slovak DPA (2009), The 2007-2008 Annual Report, available at: http://www.dataprotection.gov.sk/buxus/docs/status_report_2008.pdf, (accessed 26 June 2013).

Slovak DPA (2011), The official opinion of the DPA on 2011 Census, available at: http://www.dataprotection.gov.sk/buxus/docs/Stanovisko_Uradu_k_scitaniu.pdf, (accessed 19 July 2013).

Slovak DPA (2013), The 2011-2012 Annual Report, available at: http://www.dataprotection.gov.sk/buxus/docs/Sprava_o_stave_ochrany_osobnych_udajov_za_roky_2011_a_2012.pdf, (accessed 11 July 2013).

Slovak Government (2005), Explanatory report for the 2005 amendment to the Protection of Personal Data Law, in Slovak, available

at:http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-29206?prefixFile=m_), (accessed 15 July 2013).

Slovak Spectator (2011), Anonymity of census data questioned, 30/05/2011, available at: http://spectator.sme.sk/articles/view/42801/2/anonymity_of_census_data_questioned.html, (accessed 23 July 2013).

Slovak Spectator (2013), Protection of personal data gets revamp, 11/3/2013, available at: http://spectator.sme.sk/articles/view/49355/24/protection_of_personal_data_gets_revamp.html, (accessed 25 June 2013).

Socialbakers.com 'Social Media Report, Facebook Pages in Slovakia' available at: http://www.socialbakers.com/blog/1513-february-2013-social-media-report-facebook-pages-in-slovakia, (accessed 8 January 2014)

Staroňová, Katarína, Láštic, Erik (2012), Into the Labyrinth: The Rewards for High Public Office in Slovakia. In: B. Guy Peters, Marleen Brans (eds.): Rewards for High Public Office in Europe and North America, Routledge.

Szekely, Ivan (2008), Hungary, in James B. Rule and Graham Greenleaf (eds.), Global Privacy Protection: The First Generation, Edward Elgar Publishing Ltd., Cheltenham, UK, pp. 174–206.

The 1992 Constitution of Slovak Republic, available in English at: http://www.nrsr.sk/web/Static/en-US/NRSR/Dokumenty/constitution.doc, (accessed 13 July 2013).

The Supreme Court of Slovakia, case No. 5 Cdo 83/2008, available in Slovak at: http://www.nssr.gov.sk/data/att/7858_subor.pdf, (accessed 11 July 2013).

List of Abbreviations

ATM – Automated Teller Machine

CCTV – Closed Circuit Television

DP law - Data Protection Law, No. 122/2013 Coll. on Protection of Personal Data

EC – European Commission

EU – European Union

MP – Member of Parliament

NGO – Non-governmental Organisation

SIRENE - Supplementary Information Request at the National Entry

SIS - Slovak intelligence agency (Slovenská informačná služba)

Slovak DPA- Slovak Data Protection Authority (Úrad pre ochranu osobných údajov SR)