Balancing the interests in the context of data retention (INVODAS)

Slovakia

Martin Maxa

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

Yes

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional

law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?

N/A

3. **Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?**

   No, further transposition is not needed.

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

   N/A

- ***If transposition has been <u>accomplished</u>:***

General questions

5. **Is there an English version of the texts available? If so: Please indicate the respective URL.**

   http://www.teleoff.gov.sk/data/files/357.doc

6. **Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?**

   The relevant provisions entered into force on 1 April 2008.

7. **What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe**

   a) **whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and**

   b) **whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.**

   All existing rules meant to transpose the Directive's provisions are in a form of an Act of Parliament.

This type of legal act corresponds to the legal acts usually chosen in Slovakia for similar kinds of matters.

8. **Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?**

   The terms defined in art. 2 para. 2 of the Directive are defined in the national law transposing the Directive. There is no material difference between the two sets of definitions.

Dimension 1 (State - citizen)

9. **What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?**

   The categories of data to be retained specified in the Directive and the national implementing legislation are virtually identical. The categories of data defined in the national implementing legislation do not go beyond nor fall short of those specified in the Directive. Data on unsuccessful call attempts have to be retained.

10. **Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.**

    No, within the subject matter of this questionnaire, national law does not provide for a more extended scope of data retention obligations.

11. **According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?**

    Data retention is mandated for the purposes of investigation, detection and prosecution of the crimes related to terrorism, unlawful business, organised criminal activity, leakage and endangering of classified matters and to crimes committed by dangerous grouping.

12. **Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly**

protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?

No, within the subject matter of this questionnaire there are no such specific rules.

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefor.**

The undertaking is obliged to retain traffic data, location data and data of the communicating parties from the date of completion of the communication during the period of

a) 6 months, in the case of the internet access, internet e-mail and Internet telephony, and
b) 12 months in the case of other types of communication.

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

Law enforcement authorities, courts and other authorities of the Slovak Republic. Other state authorities are armed forces, Police Corps and state authorities that fulfil the tasks in the area of the protection of the constitutional establishment, national order and security and state defence, within the scope determined by special regulations.

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?**

The data retained may be used for the purposes of investigation, detection and prosecution of the crimes related to terrorism, unlawful business, organised criminal activity, leakage and endangering of classified matters and to crimes committed by dangerous grouping.

Courts in a civil action do not have the right to request retained data. In a civil action, retained data may be disclosed only if the party to which data pertain explicitly grants his/her consent.

16. **Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?**

The law does not set out any *specific* requirements on top of those mentioned in the answer to question 15.

17. Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?

It is required to obtain a court order. It is not required to hear the aggrieved party.

18. Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?

It is not provided that the aggrieved party shall be notified of a data access.

19. Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?

The law does not set out any particular right to be informed about the data accessed.

20. May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?

Yes, the aggrieved party can seek protection from courts against illegal data access.

The aggrieved party has a right to lodge a damage claim action against tortfeasers.

Upon a written application the data subject is entitled to request from the controller *inter alia*:

- rectification of inaccurate, incomplete or not updated information, which constitute the subject of the processing,

- destruction of his personal data, provided that the purpose of their processing under has been fulfilled;

- destruction of his personal data, which constitute the subject of the processing, provided the law has been breached.

The data subject is further entitled to object to the controller anytime upon a free-of-charge written request or personally, provided that the matter brooks not delay, to the processing of personal data in defined cases by stating the legitimate reasons or by submitting evidence of infringement of his rights and legitimate interests that are or can be violated by the processing of personal data in a concrete case; if it is proved that the objection of the data subject is valid and the legitimate reasons do not prevent it, the controller is obliged to block the personal data, the processing of which was objected by the data subject without undue delay and destroy them as soon as possible,

The aggrieved party may also notify the Office for Personal Data Protection and the Telecommunications Regulatory Authority of breaches of the Act on Personal Data Protection and the Act on Electronic Communications and demand initiation of an administrative action. The above mentioned authorities may then issue a decision identifying administrative torts committed by undertakings/controllers and levy a fine.

21. Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.

Retained data shall be subject to appropriate technical measures and organisational measures ensuring that the data will be made accessible only to authorised persons acting on the basis of authorisation or proxy of the undertaking or to the authorised state authorities and their authorised or otherwise approved members or employees.

22. When do the accessing bodies have to destroy the data transmitted to them?

There is no provision setting out specific time limits for destruction of information on retained data by accessing bodies.

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

Every person that is authorized to provide network, service or network and service in the field of electronic communications, regardless of the legal form and the method of financing.

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?

There is no applicable exemption.

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

Traffic data necessary for billing and accounting of payments, including prices for interconnection of networks. Traffic data include mainly telephone numbers, address of user, type of the terminal equipment or other facilities, tariff code, total number of call units billed in the billing period, type, date, time and duration of connection, volume of transmitted data.

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?

An undertaking shall be obliged to adopt appropriate technical and organisational measures for protection of its networks, services or networks and services, which shall, with respect to the state of technology and costs of implementation, ensure security at the level appropriate to existing risk.

Retained data shall have the same quality and be subject to the same treatment and protection as data processed or retained by the undertaking in the framework of the provision of networks or services.

The data should be subject to appropriate technical measures and organisational measures for the protection of data against the accidental or unlawful destruction, accidental loss or modification, unauthorised or unlawful retention, processing, access or publication.

27. Which additional costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in total from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?

Unfortunately, we are not aware of any statistics on aggregate costs of undertakings with respect to the retention of categories of data on top of those collected and retained before the Directive entered into force.

28. Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?

There is no provision for reimbursement of costs.

29. What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?

There are no special provisions governing cooperation of the parties.

30. Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.

A damage claim action may be filed.

The aggrieved party may also notify the Telecommunications Regulatory Authority and the Office for Personal Data Protection of breaches of the Act on Electronic Communications and demand initiation of an administrative action. The above mentioned authorities may then issue a decision identifying administrative torts committed by undertakings/controllers and levy a fine.

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

There is no provision for a public intermediary between the party retaining data and an entitled body.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

No.

33. What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?

There are no special rules on cooperation between different bodies concerning the retained data.

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

The exchange of retained data works on the basis of various international agreements. Foreign state bodies cannot ask undertakings retaining the data directly to grant them an access to the data. Slovak law enforcement authorities are responsible for cross-border data exchange.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is

applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

Telecommunications Regulatory Authority of the Slovak Republic and the Office for Personal Data Protection. Both authorities should act with complete independence.

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

We are not aware of any lawsuits or administrative proceedings.

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

We are not aware of any lawsuits with European courts except the 2009 decision of the ECJ on the question whether Article 95 provides sufficient legal basis for enactment of the Directive. Ireland supported by Slovakia brought this action for annulment (Case C-301/06).

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

National law transposing the Directive does not specify where the data should be stored. The data are stored under service provider's control, not with the State.

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have

the companies involved in the storage (both in your country and abroad) been obligated to?

The data can be stored abroad. If stored within EU, a contract with data processor established in other EU country must be concluded. Special rules apply to data transfers outside the EU.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

Yes.

Careful assessment of legal obligations and observance of all relevant legal duties. Supervision of the Telecommunications Office.

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

We are not aware of the existence of special technical interfaces. The companies divulge the required data to authorized agencies only after thorough assessment of their legal obligations.

c) data are not used for purposes other than those they are permitted to be used?

Assessment of legal obligations and appropriate training of the personnel involved.

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

It is my understanding that all measures you have described in your question are applied by companies in Slovakia. There are no special measures applied by the parties accessing the data.

e) **data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?**

Business Continuity plan should be in place to ensure timely and irrevocable destruction of retained data.

f) **the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?**

There are no measures ensuring that aggrieved parties are notified of the data access.

g) **sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?**

Within the subject matter of this questionnaire there are no specific rules on retention and transmission of sensitive data.

41. **Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?**

Yes, oversight of the Telecommunications Authority, Office for Personal Data Protection and in-house data protection officer.

The Telecommunications Authority supervises performance of obligations relating to the retention of data and imposes sanctions.

The Office for Personal Data Protection is a state authority that supervises observance of personal data protection rules and regulations and imposes sanctions.

Data Protection Officers perform internal supervision of statutory obligations in the field of personal data processing in private entities that process personal data.

42. **What technical (de facto and/or de iure) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?**

There are no unified standards applied across the board by all undertakings retaining the data.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

Undertakings retaining the data consider all requests by state bodies for access to the retained data on an ad-hoc basis by ascertaining whether statute obliges them to disclose the data. All requests for access need to be made in writing. Undertakings can store the data only in electronic form.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

Procedure found in the Council Directive 2002/187/JHA on setting up Eurojust.

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

I would say that society is vaguely aware that some form of public surveillance is going on, but is not aware of the scope of the surveillance and their particular rights. This general ignorance on the part of public is to a certain extent caused by the lack of information and public debate on introduction of data retention rules in Slovakia.

46. Are there any obligations in your country to retain other personal data without a specific reason (e.g. passenger name records (PNRs), employment data, etc)?

Postal data and Banking data.

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

We are not aware of any statistics and/or studies on the effectiveness of data retention.

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

We are not aware of any information on modification of communication patterns.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

No such discussions are going on in Slovakia.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law1 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

Right to protection of personal data, right to protection against unlawful collection, publication or other exploitation of personal data, right to privacy. These fundamental rights result from the constitution. As concerns the right to secrecy of telecommunications, it pertains only to the content of communication. Traffic and

[1] In the following, „national (constitutional) law“ means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

location data are not considered to be the content of communication. It is not legal to retain the content without specific reason.

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

The constitution refers to regular Acts of Parliament that should set out particular exceptions from applicability of the fundamental rights mentioned under question 50.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

There is no relevant constitutional jurisprudence in Slovakia.

53. Does national (constitutional) law safeguard an absolute limit as to the maximum degree to which public surveillance measures collectively may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

Regular Acts of Parliament provide exceptions to the protection of fundamental rights mentioned under question 50. The Acts of Parliament providing exceptions from these fundamental rights are based on a balance of interests approach.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

Constitutional law does not provide for any specific exemptions from the obligation to retain or transmit data mentioned under question 12.

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

The restrictions are in line with constitutional law. The Constitutional court would undertake a balance of interests approach. It would consider the relative importance of the interest protected by the state and the restriction imposed upon natural/legal persons with an objective of establishing a just balance of countervailing interests.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

Obligations can be imposed only on the basis of an Act of Parliament (or international treaty art. 7(4), government ordinance art. 120(2)). Limitations of fundamental rights and freedoms have to apply in the same way to all cases fulfilling the same conditions. Obligations can be imposed only with the aim of reaching a specific goal.

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

It is not imperative to provide for reimbursement of the costs incurred.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

They have precedence over ordinary Acts of Parliament.

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

Conditions for vertical Direct Effect of Directives as pronounced by the European Court of Justice in its case law. No special rules in Slovak law.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

Slovak Constitutional Court derives transfer of sovereignty to supranational bodies such as the EU from the Slovak Constitution instead of the Treaty on Functioning of the EU. Despite this fact, it has not ruled so far on limitation of competence already transferred to the EU.

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

The leading authority overseeing observance of data retention rules is Telecommunications Office of the Slovak Republic. Related specific issue of protection of personal data is overseen by the Personal Data Protection Office of the Slovak Republic. There are no regional territorial authorities vested with own powers.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

On a constitutional level, there are no special rules regarding transmission of retained data to other countries.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

In my opinion, a specific right of being informed of any access to retained data needs to be adopted. The undertakings/authorities should be obliged (subject to specific conditions and time limits) to inform customers on access to retained data as well as on the identity of all subjects/authorities that accessed the data. If retained data are enclosed in an administrative/criminal file, they should be sealed in a separate envelope and an access to the envelope should be duly recorded in the file.

Balancing the interests in the context of data retention (INVODAS)

Slovakia

Martin Husovec

Part 2: Overarching issues and country-specific questions

A. General part (Questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

Slovak constitutional law does not explicitly provide for a right to communicate anonymously. However, the right to communicate anonymously could be theoretically derived from the art. 26 of Slovak Constitution (corresponds to art. 17 of Charter of Fundamental Rights and Basic Freedoms) in a same way as e.g. right to informational self-determination was invented by Czech Constitutional Court (applying same laws) without any explicit wording in the Charter of Fundamental Rights and Basic Freedoms. There is currently no case-law of Slovak Constitutional Court (herein after also as Constitutional Court) on the right to communicate anonymously.

2. Please illustrate in detail any amendments to current data retention legislation that are presently discussed/have been adopted in your country since the submission of the first questionnaire (September 2010). How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in the answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?

Since September 2010, there was no amendment to the relevant parts of the Electronic Communications Act or any other piece of relevant legislation. However, at the moment, absolutely new act on electronic communications is being discussed in the Parliament. This is due to the fact that several European directives (so called 'Telecoms package') had to be transposed into the national law. Electronic

Communications Bill (the 'Bill') sets the day of its effectiveness on 1 January 2012. In regard to data retention regulation, the only significant change is that the Bill propose to extends the retention period of Internet traffic related data from 6 months to 9 months. Furthermore, in the meantime, Constitutional Court handed very important case concerning the shift of the costs of wiretapping instruments onto providers of electronic communication services. Objected provisions of Electronic Communications Act (herein after also as ECA) were held unconstitutional, namely in breach of right to the peaceful enjoyment of possessions according to the art. 1 of the first protocol to the European Convention on Human Rights (case no. PL ÚS 23/06 issued on 2 June 2010). The ruling of the Constitutional Court however invalidated only respective 'wiretapping costs provisions' as provisions dealing with the data retention costs have not been part of the complaint and the Constitutional Court could not go *ultra petitum*.

There is virtually no public debate about data retention in Slovakia. In fact, the only 'debate' occurred after European Information Society Institute filed its complaint with the General Prosecution Office and later after the ruling of Czech Constitutional Court (on data retention). This debate was however very subtle and limited only to few news services that focus on technology related news, not among the public in general. The public in Slovakia is not yet very 'sensitive' about privacy issues in general. In spite of that, the greater privacy debated occurred in the last few months when Statistical Office carried out the population census in a very unprofessional and privacy invasive (possibly unconstitutional) way. This event drawn the attention of mainstream media and eventually produced some discussion on protection of citizen's privacy. However, data retention regulation and its implications were not part of this debate. Hence, neither right of being informed (that is actually partially present in our legal systems by virtue of Penal Procedure Act – see below), nor solution legislated in art. 16(2) of Convetion on Cybercrime was discussed among the general public (in fact, art. 16(2) of Convention on Cybercrime is already present in the national law in art. 90 of Penal Procedure Act that explicitly legislates "quick-freeze" option – there is already also some case law of Constitutional Court concerning this provision).

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

   Private entities in Slovakia have quite broad obligations to co-operate with public authorities. These obligations are legislated in number of national acts, among which, the most important are the Police Corps Act (Act No. 171/1993 Coll.) and Penal Procedure Act (Act No. 301/2005 Coll.).

   Penal Procedure Act provides that every natural and legal person shall co-operate with police, prosecutors and courts in course of criminal proceedings and shall notify them anytime they witness any criminal offence (section 3). This broad obligation is specified further in the other provisions of the Act (e.g. institution of

releasing of the evidence stipulated in section 89, preservation of computer data and their releasing stipulated in section 90, disclosure of the telecommunications traffic data that are subject to the telecommunications secret protection (art. 116), etc.);

Police Corps Act provides that police has powers to request any information that may contribute to the clarification of the criminal offence and its perpetrator (section 17a). This rather general provision is followed by sets of more specific provisions such as section 76a(1) that enables police to request the personal data from legal or natural person that process them.

Only other significant *ex ante* retention duties I am aware of are postal and banking data storage. From the *ex post* retention duties, already mentioned "quick-freeze" option stipulate in section 90 of Penal Procedure Act should be mentioned. This provision enables the police and prosecutor to order expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system. The order have to be issued either by court if criminal proceedings is before a court already, or prosecutor if criminal proceedings is only in the stage of investigation.

Failing to notify the relevant authorities about the fact that criminal offence was committed, may even eventuate into criminal liability of said person (section 340 of Penal Code).

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

I will discuss this questions in two different regimes. The first regime applies when person accused of crime ('accused') refuses to testify or deliver evidence against himself. The second regime applies to a witness who shall not be subject to testimony in some cases.

The first regime; The accused can refuse to deliver a testimony in his own case under every circumstances. Doctrine of *„nemo tenetur se ipsum accusare"* is based on art. 50(4) and art. 47 of the Slovak Constitution (art. 40(4) and 37(1) of the Charter of Fundamental Rights and Basic Freedoms). However, *"nemo tenetur"* doctrine is limited to those types of evidence when accused is required to take some active steps to produce evidence against himself (e.g. to provide voice sample). To put it differently, the accused must not be compelled to produce any evidence against himself which requires him to take any active steps. For instance, according to the law, he could not be compelled to provide sample of his handwriting or voice sample (art. 123(2)), but is obliged to provide biological material such as his own blood (art. 155(2)). Therefore, as far I understand the German legal doctrine, the

situation should be quite similar to one in Germany (BVerfGE 47, 239,248; BVerfGE 16, 194, 202; BVerfGE 17, 108, 117; BVerfGE 27, 211).

The second regime; A witness who would breach a duty of secrecy set by national or international law by the virtue of delivering testimony, shall not be subject to any testimony about said circumstances of the case (section 129 of Penal Procedure Act). This typically applies to lawyers and doctors. However there is an exemption to this rule in case of some criminal offences enumerated by the Penal Code (Act No. 300/2005 Coll.). Pursuant to the section 341 of the Penal Code, this exemption covers very serious criminal offences such as some types of corruption offences and offences with more than 10 years of the upper range of sentence.

In addition, a defense counsel of the accused enjoy even more special regime among the lawyers and persons that are subject to second regime (see above). Penal Procedure Act contain several specific provisions protecting the communication of defense counsel and his client. These provisions thus create another special regime, which is not available to other persons within the category of second regime.

It is clear that first and second regime, because of their limited application, can not anyhow conflict with the access to the retention data (no active steps required for accused and no testimony to be delivered by person protecting respective secret). Situation is however different in regard to defense counsels of the accused. Thus only the special case (regime) will be discussed below.

It is not permitted to physically monitor a relationship between the lawyer and his defence counsel (section 113(3) of Penal Procedure Code). If obtaining such information, they must not be used in criminal proceedings and shall be destroyed. Moreover, the communication between a defense counsel and his client must not be subject to wiretapping also. If in the course of wiretapping, it is found that accused is communicating with his defence counsel, the information obtained must not be used for the purposes of criminal proceedings and shall be destroyed (section 115(1) of Penal Procedure Act). There is no corresponding provision in section 116 which is used for obtaining the information retained on the basis of data retention laws (herein also as ‘retention data’) in the criminal proceedings. There is also no relevant case-law and legal literature, to my knowledge, that would deal with the question whether retention data between the defense counsel and his client could be presented as evidence before a court. However, assuming that retention data actually unveil some of information that would be typically retrieved by physical monitoring of the accused and that some information may also suggest the content of the phone calls, I am of opinion that retention data between defense counsel and accused must not be used before a court. However, it shall be noted that there is no explicit provision in the Penal Procedure Act unambiguously supporting this.

5. **Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?**

Law does not provide any specific regime for data storage of retention data. Hence only general rules will apply.

Police Corps Act stipulates several rules on the storage of date obtained and processed in the course of criminal investigation (section 69a Police Corps Act). According to these rules, Police Corps shall collect personal data only for certain purpose, to extend and for a limited period of time that is required by this purpose. These data shall be separated from the other data available to Police Corps in order to fulfil some other tasks. Police Corps are entitled to process personal data without prior consent of the respective person. They shall however respect the privacy of said person. If a proper fulfilment of Police Corps tasks within criminal proceedings won't be jeopardized, the Police Corps shall destroy all the personal data. However personal data that are stored non-electronically (stored in file and not processed automatically) shall not be destroyed. Therefore, if personal data are not being destroyed because of this provision, Police Corps shall at least notify said person about the data they are storing. Section 69c explicitly provides a right of every person to request the information about all the data that are being stored about him.

On top of that, there is also general regime that applies to every personal data storage. It is stipulated in section 6, section 13 and section 14 of Personal Data Protection Act. These provisions provide that when the purpose of processing of personal data is being fulfilled, the controller shall provide for destruction of personal data without undue delay (section 13). The Personal Data Protection Act even stipulates that the controller of the data shall notify the data subject and every person to whom he provided personal data of this rectification or destruction, within 30 days from its execution (it is however subject to some exceptions). Moreover, liquidation of the personal data in this case may be also requested by the concerned individual under section 20 of the Personal Data Protection Act.

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

Electronic Communications Act sets in section 59a(10) that every 'electronic communications provider' shall annually provide Telecommunications Office of Slovak republic with anonymized data concerning the retention data usage they have encountered. Upon a request based on the Information Freedom Act, *European Information Society Institute* obtained following data from respective Ministry:

Year	Total number of requests	Number of cases in which data have been provided to competent authorities	Number of cases in which data could not have been provided to requested party
2008	384	319	65
2009	5371	5214	157
2010	7417	7126	291

B. Country-specific questions

7. Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.

First and foremost, I believe that blanket monitoring of electronic communications of all the citizens endangers the fundamental core of the privacy. Today, perhaps half of the people's life in Europe is being lived either on the Internet or with assistance of the mobile phones, and this proportion will only increase in the future. If one half of people's life is being carefully monitored for sake of national security or fight with the terrorism, to me, there is a undeniable parallel with world of 1984 created by George Orwell.

It is very important to understand the value of retention data and possibilities of its automatic processing and misuse when discussing its constitutionality. I am convinced that retrospective access of several months to the traffic data and localization data is more privacy invasive than monitoring of the content of the communications itself. It would be unimaginable for a state to impose general wiretapping regulation. I am therefore wondering that it is actually possible when it comes to data retention. I believe this unbalanced approach springs from the fact that value of the retention data and its inherent threats for the future are being heavily underestimated.

Furthermore, from the statistics of crime rates that are available in several European countries that implemented data retention regulation, one common conclusion could be perhaps drawn already. That is to say in no country data retention caused any *dramatic* (if any) change in statistics numbers - whether in terms of crime rate or overall success of criminal investigations. Accordingly I view the data retention

regulation as an huge unconstitutional experiment, which proved to be ineffective in accomplishing its outlined aims and shall be therefore abandoned as soon as possible. Predominantly on this argument, I believe that blanket retention of electronic communications data is in breach of proportionality rule. Hence, I can not see any way in which Data Retention Directive could be implemented into national law without leaving all this arguments open. Therefore, I am of opinion that data retention in today's form as such fails to pass the proportionality rule test, regardless of whether its aimed only at serious crimes and regardless of the security measures that will be taken to protect this data from the misuse. Thus I believe that Directive itself shall be invalidated respectively.

Slovak implementation; As you will see in the lines below, current legal provisions were not designed for data retention regulation at all, what leads some public authorities to incorrect and unconstitutional application. Especially the procedure of obtaining data does not meet any requirements of legal certainty that shall be observed in case of such privacy invasive regulation as data retention. This is one of the grounds why I believe that data retention shall be invalidated. There are however also numerous other arguments such as

a) the safeguards and technical procedures are not precisely outlined by the law;

b) the system is carried out by private entities which are not aware of the legal issues concerned,

c) the scope of stored information is too broad (one used for billing purposes would be more accurate);

d) the means of the control by concerned citizens is unsufficient, etc.

8. Are the data to be retained in accordance with the Directive covered by the secrecy of correspondence, as provided for by the national (constitutional) law of your country?

'Retention data' are covered by secrecy of correspondence stipulated in art. 22 of Slovak Constitution (art. 17 of Charter of the Charter of Fundamental Rights and Basic Freedoms). This fact was repeatedly stressed by both Constitutional Courts interpreting Charter of Fundamental Rights and Basic Freedoms (Slovak and Czech). Czech Constitutional Court confirmed this in cases such as Pl. ÚS 24/10, IV. ÚS 78/01, II. ÚS 502/2000, I. ÚS 191/05 or II. 789/06 and Slovak Constitutional Court indirectly in cases III. ÚS 68/2010, II. ÚS 53/2010 and II. ÚS 96/2010. The interpretation follows and refers to highly influential jurisprudence of the European Court of Human Rights (Malone v. the United Kingdom, judgment of 2 August 1984, Copland v. the United Kingdom, judgement of 3 April 2007).

9. **Please explain the impact of the proportionality rule when assessing the constitutionality of a measure limiting fundamental freedoms, and what interests have to be balanced within the scope of such assessment.**

   Proportionality rule under Slovak constitutional law doctrine (see e.g. PL ÚS 23/06, PL. ÚS 3/09, PL. ÚS 3/00, PL. ÚS 67/07) is very similar to proportionality rule employed by European Court of Human Rights in the context of the art. 8(2) of the European Convention of Human Rights. It comprises three steps:

   a) test of legitimate aims that asks whether measure limiting fundamental freedoms is able to achieve intended aims (in this case the protection of public interest in the form of national security and public order). If the measure is not effective enough to achieve intended aims it is in breach of rule of law (Rechtsstaat); Second part of this step is embodied in the question whether the instrument is rationally interconnected with its intended aim (rationality connection test); and

   b) test of necessity that asks whether there isn't less invasive measure conflicting with the respective fundamental freedom; and

   c) test of proportionality stricto sensu that asks whether the detrimental effect to the respective fundamental freedom, which is a result of conflicting interests, is still proportional; In this case, it is the interest of the state to strengthen its national security (public interest) versus fundamental right to privacy.

10. **Please explain the history and outcome of the motion of 10 April 2010 filed with the General Prosecutor by the European Information Society Institute. What potential violations of the law have been claimed, and how did the General Prosecutor respond to them? Are you aware of any other action that has been taken against the current Slovak data retention law? If so: what is the current state of affairs in this regard?**

    European Information Society Institute (herein also as 'EISI') filed a complaint with General Prosecutor Office demanding it to initiate proceedings before the Slovak Constitutional Court. EISI claimed violation of

    • art. 13(4) of Slovak Constitution – proportionality rule; art. 16(1) of Slovak Constitution – right to privacy; art. 19(2)(3) of Slovak Constitution – right to privacy and protection against the unlawful collection of the data; art. 22 of Slovak Constitution – privacy of correspondence;

    • art. 7(1), art. 10(2)(3) and art. 13 of constitutional law No. 23/1991 Coll., which introduces the Charter of Fundamental Rights and Basic Freedoms (same rights and interests as outlined above), and

    • art. 8 of European Convention on Human Rights;

General Prosecution Office rejected request of EISI on a very strange basis. It claimed that there is a new act being discussed in the Parliament and therefore until this new act will come into effect, there is no need to scrutinize objected provisions before the Constitutional Court. General Prosecution Office probably meant that any objections could be possibly made in the Parliament. EISI is currently waiting for the new act and will then file another complaint with General Prosecution Office, this time with assistance of several other NGOs and using argumentation and precedent of Czech republic. As Czech republic is very close jurisdiction not only geographically, this could increase our chances. If General Prosecution Office rejects to file the complaint with the Constitutional Court again, EISI will most likely initiate civil litigation against either state or one of a electronic communications providers. In course of civil proceedings then, EISI will demand the civil court to refer the provisions for constitutional scrutiny before the Constitutional Court. This is necessary because direct constitutional complaint seeking invalidation of the respective provisions is not possible under current legislation.

There are no other actions against data retention in Slovakia.

11. Please describe the following safeguards of the rule of law in detail, providing legal references (legal norms applying) in each case:

- **catalogue of the "crimes related to terrorism, unlawful business, organised criminal activity, leakage and endangering of classified matters and to crimes committed by dangerous grouping", the investigation, detection and prosecution of which would allow the entitled bodies to request the data retained;**

  There is no category of *"terrorism related crimes"* in the national law. Penal Code recognize only crime of *"terrorism"* and crime of *"participation in terrorism"*. Both of these crimes are set in section 419 of Penal Code; I believe that "terrorism related crimes" also refers to crimes committed by terrorist groups (section 129(5) of Penal Code) and also crime of *"establishment, plot or support of the terrorist group"* set in section 267 of Penal Code. For the explanation of the notion of terrorist group see the definition bellow.

  The term *"unlawful business"* ('nedovolené obchodovanie') is rather wrong translation. The term is again not used elsewhere in the national law. By restrictive interpretation of the term and use of systematic and teleogical arguments, I am coming to the conclusion that crimes of unlawful trafficking with guns (section 294), people (section 179), children (section 180), foreign currency (section 251) and unlawful trafficking of drugs (section 171) were meant by the legislator. On the other hand, by this interpretation I knowingly exclude less serious crimes such as non-authorized trading (section 251).

  The term *"organised criminal activity"* refers to criminal offences committed by so called *"organized group"* within a meaning of section 129 of the Penal Code. This category include any criminal offence committed by common activity of at least three people with some certain distribution of tasks between its members,

characterized with more systematic and coordinated activities, thus also higher probability of successful committing of a crime.

Term *"crimes committed by dangerous groupings"* refers to criminal offences committed by *"terrorist group"* or *"criminal organization"* (see section 141 of Penal Code).

"Criminal organization" is a structured group of at least three people that exists for some certain period of time and acts in mutual coordination with the aim to commit one or more felonies, crime of the legalization of income gained from illegal activity (money laundering) or some of the crimes of corruption committed for the purpose of the gain of direct or indirect financial or other benefit.

"Terrorist group" refers to structured group of at least three people, which exists for certain period of time for the purpose of committing a crime of terror (section 313) or a crime of terrorism (section 419).

"Leakage and endangering of classified material" refers to criminal offence of *espionage* (section 318), *endangering of classified material* (section 319) and *endangering of confidentiality and exclusivity of the information* (section. 353).

- **the requirement of a court order prior to the data request: Please describe the steps the entitled body has to take in order to obtain a court order prior to the data request, if so required. What will the court examine before taking a decision on whether or not to issue the order? Are there any situations (e.g. "emergency cases") that are exempt from the requirement of a court order? If so: who will decide in these situations whether or not access to the data may be requested?**

  Generally speaking, there is no provision specifically designed for the access of retention data. To the contrary, provisions that have been previously used for other purposes (e.g. access to telecommunications secrets) are now being used also for retention data disclosure. This however causes a lot of trouble while provisions are not always very clear. It eventually results in the current *status quo* when the interpretation is very uncertain and public bodies often misuse and misinterpret respective provisions in a way that suits them best. Following lines will discuss the interpretation problems and will also offer the most appropriate interpretation.

  Electronic Communications Act explicitly sets the purpose of the storage of retention data. It says that data are being stored to help with investigation and revealing of *"crimes related to terrorism, unlawful business, organised criminal activity, leakage and endangering of classified matters and to crimes committed by dangerous grouping"*. This wording does not necessary require that retention data are to be accessed only in course of criminal proceedings. It enables to access the data also out of criminal proceedings provided that it concerns investigation or prevention of said crimes. Access to data in course of criminal proceedings is clearly regulated by section 116 of Penal Procedure Code. In case

of ‘out of criminal proceedings’, situation is more complicated. There are several non-amended legal instruments left in various acts which do not reflect serious and invasive nature of data retention because they previously aimed at different information (e.g. provision enabling police to access the data that are stored by electronic communication providers – see below). Plus, there is also the Act Against Wiretapping (Act No. 166/2003 Coll. on protection of privacy against the unauthorized use of information-technical instruments). This Act applies if the instrument falls within the category of so called *‘information-technical instruments’* (definition is very open). The Act Against Wiretapping basically protects the citizen against excessive use of wiretapping and similar technologies by police or intelligence agencies that occurs out of criminal proceedings. In my opinion, the Act shall also apply to activity of accessing the retention data as the activity arguably fall within a category of information-technical instruments. The access will be therefore discussed in these two regimes (Penal Procedure Act and Act Against Wiretapping).

Electronic Communication Act explicitly states only that provider shall provide the data upon written petition of the *prosecutor*, *police*, *court* or ‘*other public body of Slovak republic*’ (section 59a(8)). ECA also uses and defines in section 55 the term *“public bodies of state”* which refers to state authorities that fulfil the tasks in the area of the protection of the constitutional establishment, national order, and security and state defence, within the scope determined by corresponding special acts. Its is unclear why two different terms are used in this regard. However this shall not be serious problem as to be able to request the data, public body has to have powers legislated in the special act which ECA herein refers to. Moreover, ECA sets another authorities that can access ‘*the Telecommunications Secret’*, which retention data are being part of. There is therefore a lot of space for various interpretations, not to mention obsolete provisions left in special acts of public bodies.

However, I believe only the following interpretation is correct as the retention data shall enjoy special regime because of their very privacy invasive nature. First and foremost, Law Against Wiretapping shall apply. Application of this Act then excludes any other means of obtaining the access, especially various obsolete provisions that were not amended with the introduction of Act Against Wiretapping. So the access is possible in these two regimes:

In the criminal proceedings, retention data are to be accessed pursuant to section 116 of Penal Procedure Code. This legal instrument was enacted before the data retention regulation came into the effect. It enables Police Corps, prosecutor and court to access telecommunications traffic and localization data in course of criminal proceedings. Formerly, this article aimed at the data stored by providers for the purpose of invoicing its customers. Today, it is predominantly used to access retention data. According to the explicit reading of the provision only *“intentional crimes”* are required in order to use this provision. This again clearly conflicts with the aim for which the data retention data shall be stored as expressed in the ECA. Therefore when accessing retention data, court shall require one of the crimes set in the ECA. It is however

it is very likely that this is not the case. Other requirements of section 116 of Penal Procedure Act are that requested data have to be necessary for investigation of respective crime, the order shall be issued by the court and the request itself shall be supported with certain evidence. Moreover, the court has to justify his order.

Outside of the criminal proceedings, retention data could be accessed pursuant to provisions of Act Against Wiretapping (herein also as AAW). Article 5 of AAW requires that written request for the information have to be submitted to the court. Authorities authorized to make this request are Police Corps, Slovak Information Service, Army Intelligence Service, Customs Administration and Corps of the Prison and Court Guard). Every request shall include following details:

a) type of information-technical instrument, which is being applied for, place of its use, proposed time of use and information about the person which is subject to this request;

b) information about previous ineffective or substantively hindered investigation and documentation of the activity,

c) grounds for use of the information-technical instrument.

According to section 3 of AAW, information-technical instrument may be used only in limited number of cases if it is neccessary in democratic society to ensure the national security, state defense, prevention and investigation of criminal activity or protection of rights and interests of others.

The court examining such request will then grant or dismiss such application for retention data disclosure; The Act Against Wiretapping sets also so called *"express procedure"*. This requires exceptional circumstances. There have to be reasonable suspicion of the person committing the criminal offence, the case have to be urgent and consent of the judge can not be obtained. In this case, Police Corps shall notify the judge of the commencement of use of information-technical instrument within one hour and also submit the request for its use as outline above. If the Police Corps do not obtain the consent of the judge within 12 hours from the commencement of use of information-technical instrument, the information obtained this way must not be used in any way and shall be immediately destroyed, about which the Police Corps shall notify the judge. There is no express procedure for Slovak Information Service, Army Intelligence Service, Customs Administration and Corps of the Prison and Court Guard.

Only to mention one of the provisions that is being heavily misused for accessing of retention data. Section 76a(3) of the Police Corps Act sets that every 'provider of electronic communications' shall upon request provide the police with traffic data and data of communicating parties (without any prior court request). This provision appeared in the Police Corps Act before 2004 while above mentioned provisions of Penal Procedure Act and Act Against

Wiretapping came into effect later (1.1.2006 and 1.7.2004). Section 76a(3) clearly contradicts provisions of the AAW as well as Penal Procedure Act. In my opinion therefore this provision is obsolete as interpretation argument *lex posterior derogat legi priori* shall be used in this case. However, Police Corps repeatedly use this provision to obtain data retention data even in the case of administrative wrongs.

As previous lines suggest, the procedure of obtaining data does not meet any requirement of legal certainty that shall be observed in case of such privacy invasive regulation. Based on the wrong reading of the acts, some state authorities demand the retention data even in case of administrative wrongs (*European Information Society Institute* has explicit evidence in this matter). As 'electronic communication providers' are often small companies lacking any legal departments, they without hesitation handle this kind of data when requested by the Police Corps.

- **rights of the data subject: does national data protection law provide for any right of the aggrieved party to know that their data have been accessed?**

  Section 69c of the Police Corps Act explicitly provides a right of every person to request the Police Corps about all the data that are being stored about him. It also sets the cases when Police Corps shall notify the person about data being stored *(see the answer to question 5)*. Furthermore, section 115 of Penal Procedure Code provide certain notification duty of the police, prosecutor and courts in case of wiretapping. If the data obtained through wiretapping were proved to be irrelevant to the present case, respective body shall immediately destroy the data (section 115(8)) and notify aggrieved person within three years of the end of the case. Even thought corresponding provision is absent in section 116 of Penal Procedure Code, based on the systematic (*argumentum a rubrica*), *"constitutional-conform"* (human rights favouring interpretation) and historic argument (this provision was previously aimed at less sensitive data), such obligation of the state would be possible to establish also in the case of retention data. However, this interpretation is not so obvious again. Act Against Wiretapping does not contain any similar provisions.

  On the other hand, Personal Data Protection Act provides in section 20 that upon a written application, the data subject shall be entitled to request from the controller

  a) information about the state of processing of his personal data in the filing system in a generally intelligible form;

  b) exact information, in a generally intelligible form, about the source from which the controller obtained his personal data for their processing;

  c) a copy of his personal data, in a generally intelligible form, which constitute the subject of the processing;

d) rectification of inaccurate, incomplete or not updated information, which constitute the subject of the processing;

e) destruction of his personal data, provided that the purpose of their processing under was fulfilled; if any official documents containing personal data constitute the subject of the processing, he may request their returning,

f) destruction of his personal data, which constitute the subject of the processing, provided that the law was breached.

12. **Are there any rules preventing the same data from being retained more than once (e.g. when the network operator and the service provider are different legal personalities who, in principle, would both be covered by the retention obligation)? If so: please describe the content of these rules.**

No, there is no such rule.

13. **Are there any specifications regarding data security with respect to storage and transmission (objectives to be achieved – e.g. "adequate confidentiality" – and/or quality requirements to be fulfilled – e.g. an obligation to encrypt the data before transmitting them to the authorised bodies)? If so: Are the technical and organisational measures necessary to implement these legal requirements standardised or specified in any other way, e.g. through guidelines issued by the supervisory authority? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.**

In particular: do they provide for measures in one or more of the following areas:

- **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**
- **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**
- **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**
- **access logging**
- **secure (irreversible) deletion after expiry**
- **error correction mechanisms (e.g. hash functions, checksums)**
- **secure data transmission (cryptographic security, postal delivery)**

- **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**

- **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**

- **staff training/internal control mechanisms to ensure compliance with the law and other rules**

- **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

Do the technical and organisational measures described apply specifically and exclusively to the storage and transmission of data in the context of data retention, or to any data processing (in electronic communications)?

Only provision specifically applicable in this regard is Section 57 (1) of Electronic Communications Act. It requires the providers to take *"appropriate technical and organizational measures for protection of their networks and services"*. This measures shall reflect the state of art. No further specific guidelines are given by the law. On the other hand, existence of Personal Data Protection Act shall be observed also. Especially section 15 and section 16 are relevant (English version of the Act can be consulted here http://www.dataprotection.gov.sk/buxus/docs/act_428.pdf, amended only once since then). Relevant excerpts from the law:

Section 15 (1) The controller and the processor shall be responsible for security of personal data by protecting them against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorized access and making available, as well as against any other unauthorized forms of processing. For this purpose he shall take due technical, organizational and personal measures adequate to the manner of processing, while he shall take into account above all

a) the existing technical means,

b) the extent of possible risk that could violate security or functionality of the filing system,

c) confidentiality and importance of the processed personal data.

(2) The controller and the processor shall take the measures under Paragraph 1 in the form of a security project of the filing system (hereinafter the "Security Project").

(5) The audit of the filing system's security may only be performed by an external, professionally qualified legal or natural person, who did not participate in development of the Security Project of the respective filing system and there are no doubts about its impartiality.

Section 16 (1) The Security Project shall define the extent and manner of the technical, organisational and personal measures necessary for elimination and minimizing of the threats and risks affecting the filing system from the viewpoint of impairing its security, reliability and functionality.

(2) The Security Project shall be developed in accordance with the basic rules of filing system's security, the issued security standards, legal regulations and international treaties binding for the Slovak Republic.

(3) The Security Project shall include above all

a) a security policy,

b) analysis of the filing system's security,

c) security directives.

(4) The security policy shall specify the basic security objectives that must be achieved for protection of the filing system against violation of its security and it shall contain above all

a) specification of the basic security objectives and the minimum required security measures,

b) specification of the technical, organisational and personal measures for ensuring protection of personal data in the filing system and the manner of their use,

c) definition of the filing system's environment and its relation to the possible security violation,

d) definition of the limits determining residual risks.

(5) Analysis of the filing system's security shall mean a detailed analysis of the state of the filing system's security containing above all

a) qualitative risk analysis, within of which the threats affecting individual items of the filing system capable of violating its security or functionality are identified; the result of the qualitative risk analysis shall be a list of threats that could endanger confidentiality, integrity and availability of the processed personal data, while it shall also state the extent of the possible risk, proposals of the measures eliminating or minimizing the affect of the risk and a list of the remaining risks,

b) use of security standards and determination of other methods and means of the protection of personal data; evaluation of conformity of the proposed security measures with the applied security standards, methods and means shall constitute a part of the analysis of the filing system's security.

(6) Security directives shall specify and apply the conclusions resulting from the Security Project to the concrete conditions of the operated filing system and they shall include above all

a) description of the technical, organisational and personal measures defined in the Security Project and their use in concrete conditions,

b) the scope of powers and description of the permitted activities of individual entitled persons, the manner of their identification and authentication in accessing the filing system,

c) the scope of liability of entitled persons and of the personal data protection official

d) the manner, form and periodicity of performance of the inspection activities focused on observation of the filing system's security,

e) procedures during breakdowns, failures and other extraordinary situations including preventive measures for restricting the occurrence of extraordinary situations and possibilities of an effective restoration of the state before the breakdown.

In addition, section 59a(8) of the ECA stipulates that data retention information shall be stored only electronically.

14. **Please describe the rules for co-operation between the party retaining the data and the party (public authority) accessing them in detail. What steps have to be followed in each case in order for the respective entitled body to obtain access to the requested data?**

There are unfortunately no specific provisions on co-operation between the party retaining the data and the party accessing them. Explanation of certain conditions that have to be met in order to get an access to retention data is already provided above.

15. **Please describe the rules for co-operation among the different bodies accessing the data and between these and other public authorities in detail: Are there any provisions that allow the bodies entitled to obtain access to the data retained to transfer these data, once obtained, to other authorities for their respective purposes? If so, please describe the requirements that have to be fulfilled for such transfer.**

Law does not stipulate any specific provisions for sharing of retention data. It is generally necessary to grant the access to the retention data on the individual basis by court, whether in the criminal proceedings or outside of criminal proceedings.

Of course, in criminal proceedings, police and prosecutor are allowed to share such data. There are however no specific provisions on this cooperation.

Outside of criminal proceedings the relevant provision is section 7(1) of the AAW. This provision only provides that data obtained can be communicated to other relevant public bodies within their powers only in accordance with the specific acts.

Any access to shared retention data shall be limited to the purposes for which they have been initially stored.

16. **Please provide more details about which – and how – EU legislative acts and international treaties on cross-border co-operation (i.e. rules specifically designed for data retention as well as general rules applicable to data retention) are applied in Slovakia.**

There are no specific rules on cross-border exchange of retention data. Therefore general rules will apply. I should mention especially: the rules set in Penal Procedure Act that concern cross boarded exchange of evidence within criminal proceedings, the rules that concern establishment and practice of EUROPOL and EUROJUST and the rules on cross boarder exchange of personal data (section 23 and section 23a of Personal Data Protection Act). There are also numerous bilateral agreements on co-operation between states in criminal proceedings and possibly also outside of criminal proceedings. The former bilateral agreements precede over the general provisions of the Penal Procedure Act.

In course of criminal proceedings, sections 532 to section 536 of Penal Procedure Act is usually used. This provisions stipulates that Slovak authorities shall request the data from foreign jurisdictions via General Prosecution Office or Ministry of Justice. Section 537 then deals with the case when foreign authorities apply for data stored by electronic communications provider in Slovak republic. Foreign public authorities shall address their requests to the Ministry of Justice, which then proceeds the request directly to the appropriate district court. The court will then follow requirements stipulated in section 116 of Penal Procedure Act.

Other sources of law that provide some general rules on co-operation are:

- Council decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information;

- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters;

- Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences;

- Art. 15 of consolidated version of Council Decision 2002/187/JHA on the setting up Eurojust, as amended by Council Decision 2003/659/JHA,

- Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust.

In order to carry out the obligations within EUROPOL system, the National Center of Europol Office was established. This unit is organized within the structure of Police Corps and Ministry of Interior of the Slovak republic.

Slovakia is also part of the INTERPOL system since 1993. Again, in order to carry out the obligation arising from the membership, the National Center of Interpol was established.

17. Please provide more details about the scope of competence and about the independence of the supervisory authorities referred to in the answer to question 35 of the first questionnaire.

Telecommunications Regulatory Authority of the Slovak republic has following scope of competence (see Section 6(3) of ECA):

a) co-operating with the Ministry in elaboration of the proposal of the national frequency spectrum table and administers the frequency spectrum,

b) protecting the interests of end users with regard to quality and prices of services,

c) fulfilling obligations supporting competition, development of common market of the European Union, interests of all persons of the European Union member states in the territory of the Slovak Republic, access to networks, interoperability of networks and services and protects freedom of carrier selection applying technical standards,

d) issuing generally binding legal regulations within the limits of this Act,

e) leading out-of court dispute resolution,

f) providing information to end users related services, performs users researches, publishes them and uses them in its activities,

g) fulfiling tasks related to limitation of proprietary rights to real estates in respect of using of real estates for the purposes of service provisioning and tasks related to limitation of proprietary rights to movable assets by limitation or ban on using transmitting telecommunications facilities and lines in times of war or belligerency,

h) supervision of electronic communications providers,

i) imposing sanctions for breach of the rules, etc.

Statutory body of the Telecommunications Regulatory Authority of the Slovak republic is a Chairman who is elected and recalled by the Parliament upon a proposal of the Government. Budget of the Office is separated from any ministry or other public body. The independence of the Telecommunications Regulatory Authority was hotly debated in 2006 (due to financing and so called ‘structural separation’), 2008 and 2009 (due to change of the chairman). European Commission even initiated proceedings against Slovak republic objecting too broad range options of the Parliament and Government of recalling the chairman. Eventually European Commission abandoned all the initiatives due to the changes within the ECA in April 2010. These changes were claimed by European Commission as sufficient

enough to ensure the independence of the Telecommunications Regulatory Authority.

The Office for Personal Data Protection of the Slovak republic (*„the Office"*) is a budgetary organisation. The Office shall submit a proposal of the budget as a part of the General Treasury Administration category. Only the Parliament may decrease the approved budget of the Office in the course of a calendar year. The President of the Office is elected and recalled by the Parliament upon proposal of the Government. The President of the Office must not be a member of a political party or political movement and is responsible for his activities to the Parliament. Inspectors of the Office are responsible for the enforcement of the Office powers. The Office repeatedly stress that it lacks appropriate resources for the enforcement it is in charge of. Especially lack of inspectors and lack of financial budget is being objected. Its powers are as follows:

a) monitoring the state of personal data protection, registering information systems that are processing personal data and supervising them,

b) issuing guidelines for security of personal data in information systems,

c) providing binding opinion in case of cross-boarder flow of personal data,

d) controlling lawfulness of processing personal data in information systems,

e) imposing fines in case of breach of the provisions of Personal Data Protection Act,

f) approving the implementing legal acts within its competence,

h) assisting in the preparation works of new legislation;

18. Which public bodies are responsible for supervising *that the bodies entitled to obtain access to the data retained* (police etc) act within the law? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?

Two authorities are in charge of the supervision of the bodies entitled to obtain access to the retention data. Firstly, it is The Office for Personal Data Protect of the Slovak republic („the Office"). This public body supervise all the public authorities handling personal data, except for security agencies which are supervised directly by Parliament. Therefore it supervise the practice of Police Corps, prosecutors and of the courts.

Intelligence agencies such as Slovak Information Service (*„Slovenská informačná služba"*) or Army Intelligence Service (*„Vojenské spravodajstvo"*) are being supervised directly by the Parliament. Parliament elects special committee of members of Parliament that has to supervise the lawfulness of activities of these intelligence agencies. This committee sits four times a year. (see art. 6 of the Act No. 198/1994 Coll. and art. 60 of Act No. 350/1996 Coll.). The committee is also in

charge of supervision of activities carried out on the basis of AAW (section 9). Therefore it also supervise the practice of Customs Administration, Corps of the Prison and Court Guard and Police Corps when accessing the retention data out of criminal proceedings.

Apart from the fact that the committee shall submit the report to the Parliament twice a year, there is no detailed guidance on the work of the committee in the law.

Independence of the Office for Personal Data Protection of the Slovak Republic was discussed above. Independence of Parliament is probably not necessary to discuss.

Slovak Update on the Data Retention (August 2013)

Since the submitting of the national report, lot of things have changed in Slovakia.

First of all, the national data retention transposition together with some access grating laws are currently being reviewed before the Constitutional Court of Slovak republic, as a result of the complaint of some members of the Parliament that was organized by a local NGO, European Information Society Institute (EISi)[1]. The reasons of the complaint are alleged breach of

art. 13(4) of Slovak Constitution – proportionality rule; art. 16(1) of Slovak Constitution – right to privacy; art. 19(2)(3) of Slovak Constitution – right to privacy and protection against the unlawful collection of the data; art. 22 of Slovak Constitution – privacy of correspondence;

art. 7(1), art. 10(2)(3) and art. 13 of constitutional law No. 23/1991 Coll., which introduces the Charter of Fundamental Rights and Basic Freedoms (same rights and interests as outlined above), and

art. 8 of European Convention on Human Rights;

The complaint was filed in October 2012. It the meantime, the judge-reporter was assigned to to the case. Requested preliminary reference to the Court of Justice of European Union was not granted yet. Because in the meantime, Austrian Constitutional Court referred identical questions, Slovak Constitutional Court is now unlikely to submit it's own, but will probably wait for the CJEU.

Second change is related to laws that were analyzed in the national report. Both the Electronic Communication Act as well as Personal Data Protection Act were entirely substituted by new acts. Namely, Act No. 351/2011 Coll. on Electronic Communications[2] and Act No. 122/2013 on Personal Data Protection. The most important issues related to the analysis, however, did not substantially change.

1 English press release is available here at http://www.eisionline.org/index.php/projekty-m/data-retention-m/49-slovak-case-on-data-retention

2 English version of the act is available at www.teleoff.gov.sk/data/files/22211.pdf