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

Slovenia

Klemen Tičar, attorney at law

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. The Directive has been fully transposed into national law by the Amendments to the Electronic communications Act (hereafter: ECA) in the year 2006 (OJ RS no. 129/06). Subsequently the ECA was last amended by the end of 2009 and the amendments covered also data retention provisions.

- ***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)?**

   /

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?**

   Following informal information a new set of amendments of the ECA is being prepared by the ministry with the aim of transposing the recently adopted EC Directives, there are however no draft versions available yet.

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.**

   /

- ***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.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/DEK/Elektronske_komunikacije/Zakoni/ZEKomB_Law_Official_consolidated_version__ZEKom-UPB1_.pdf

   Please note that the accessible translated version does not contain the most recent amendments of the ECA that apply from the beginning of 2010 onward.

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

   The Directive was first transposed with the 2006 amendments of the ECA. However as some clarifications were necessary in order to ensure full compliance (although there were no obvious non-compliances, some solutions proved somehow undefined in practise) and another set of amendments was adopted in December 2009, where certain obligations were clarified (i.e.: that the retention obligation applies only to operators having its registered seat or subsidiary in the Republic of Slovenia; and retention obligations in respect of the use of e-mail, internet and internet telephony where separated to ensure clarity) or improved in the applied terminology (i. e. the

term internet telephony whas replaced by telephony services using an internet protocol) Other changes aimed for improving the processes between different competent authorities (information commissioner, NRA, Police, the courts, SOVA, MOD). Partly however, this was done also for political reasons as the retention period was shortened from the general rule of 24 to 14 (telephone services) and 8 (all other services – internet telephony and internet use) months, respectively.

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**

   According to the Slovene legal system and constitutional practice the whole Directive can only be transposed by an Act of the Parliament (Law). Only strictly technical, operational issues were left over to administrative regulations. However those have no direct link to the wording of the Directive but merely represent a more precise definition of institutes that are provided by law.

   Two issues are regulated more precisely by the following subordinated regulations:

   - *Handover of retained data* is governed Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication network (OJ RS no. 103/2009), adopted by the competent Ministry (currently Ministry for higher education and technology)

   - *Storage of data* is regulated by the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored (OJ RS no. 123/2008), adopted by the National regulatory agency (hereafter NRA)

   - (further regulations that might be worth observing) are also Special rules for retention of Police data are governed by Rules on the retention of data on electronic communications of the Police and on the access to Police data collections (OJ RS no. 103/2006, 59/2007) adopted by the Ministry of the interior

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.**

Yes. The implementation approach used in this case is very much standard in the Slovene legal system. Mostly an Act of the Parliament is chosen to transpose the whole subject of the directive and issues that require further regulation are then left over to other administrative acts (Decree of the government or Rules of the Minister or Decisions or General Act of other public bodies (e.g. NRA's))

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?**

No, not all terms from Article 2/2 of the Directive are defined specifically. The terms "data" and "user ID" for example are not defined specifically, however both terms are very well understood from the context. Another example of deviation from the provisions of the Directive is the term "internet telephony", which was transposed by the ECA into national law as "telepohy serviced, using an internet protocol", which could be – if interpreted strictly - in its meaning understood broader as the Directive.*Dimension 1 (State - citizen)*

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 scope of data to be retained according to Slovene law (Article 107b ECA) follows directly the provisions of Article 5/1 of the Directive:

Data necessary to trace and identify the source of a communication:

A. concerning fixed network telephony and mobile telephony:

i. the calling telephone number;

ii. the name and address of the subscriber or registered user;

B. concerning Internet access, Internet e-mail and Internet telephony:

i. the user ID(s) allocated;

ii. the user ID and telephone number allocated to any communication entering the public telephone network;

iii. the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

Data necessary to identify the destination of a communication:

A. concerning fixed network telephony and mobile telephony:

i. the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

ii. the name(s) and address(es) of the subscriber(s) or registered user(s);

B. concerning Internet e-mail and Internet telephony:

i. the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

ii. the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

Data necessary to identify the date, time and duration of a communication:

A. concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

B. concerning Internet access:the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

C. Concerning Internet e-mail and Internet telephony the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

Data necessary to identify the type of communication:

A. concerning fixed network telephony and mobile telephony: the telephone service used;

B. concerning Internet e-mail and Internet telephony: the Internet service used;

Data necessary to identify users' communication equipment or what purports to be their equipment:

A. concerning fixed network telephony, the calling and called telephone numbers;

B. concerning mobile telephony:

i. the calling and called telephone numbers;

ii. the International Mobile Subscriber Identity (IMSI) of the calling party;

iii. the International Mobile Equipment Identity (IMEI) of the calling party;

iv. the IMSI of the called party;

v. (v) the IMEI of the called party;

vi. in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

C. concerning Internet access, Internet e-mail and Internet telephony:

i. the calling telephone number for dial-up access;

ii. the digital subscriber line (DSL) or other end point of the originator of the communication;

Data necessary to identify the location of mobile communication equipment:

i. the location label (Cell ID) at the start of the communication;

ii. data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

These rules do not include additional retention obligations with regard to traffic data that would go beyond the obligations in the Directive and more or less also follows the systematic approach of the Directive completely. No shortcomings in respect of the Directive can be identified.

Only data on unanswered calls has to be retained (Article 107a ECA, para. 4). To this end it should be noted that a distinction is made by law between unsuccessful call attempts (where a connection was not established) and calls where a connection

was established, however the call remained unanswered. The first are not subject to retention whereas the latter are.

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.**

    In principle only data specified in Article 107b (as described above) are subject to retention.

    However the operators are allowed to keep other data (especially customer records) if the provided service to the customer is disputed (e.g. the customer refuses to pay the bill for the provided services, see Article 104/2). In such cases data may be retained until the eventual claims fall under the statute of limitations.

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

    There are three groups of purposes to which data retention is mandated:

    (1) For the purposes of prosecution of crimes pursuable on official duty, according to the provisions of the Criminal procedure Act

    (2) For the purposes of ensuring national security and the constitutional order, and the security, political and economic interests of the state, according to the the Slovenian Intelligence-Security Agency Act

    (3) For the purposes of national defence as stipulated by the Defence Act.

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)?**

    Although Slovene law provides for a special regulation of privileged communications (as the examples given) there are no specific retention rules in national law respectively. Those communications are subjected to retention like any other.

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 recent amendments of the ECA shortened the retention period (from the previous general rule of 24 months retention period) to:

(1) 14 months for publicly available telephony services

(2) 8 months for any other service

There was some upraising when the Directive was first transposed with the ECA 2006 amendments, which stipulated for a 24 months retention period. The operators in general, parts of the civil society, the Information Commissioner and some political parties argued that the retention period is too long and that there are no legitimate reasons whatsoever to implement the longest possible retention period. The operators argued in general that retention will trigger significant additional costs to their businesses which are increasing even more with the duration of the retention period. Subsequently the issue was put to the political agenda of certain political parties of the governing coalition and the retention was shortened with the 2009 ECA amendments. The main political reason which was expressed during the public debate was that the new regulation is a far more proportionate solution in almost every respect. Thereby the distinction between the both groups of services is grounded on the consideration that it is far easier to ensure retention to telephony services (as the whole billing systems is adapted very much to retention) than in the case of internet services (where in fact a flat rate billing principle in prevailing), where there are no appropriate retention means available already in the scope of the provision of the service, hence all retention infrastructure has to be in principle customized. But also the scope of data to be retained is much bigger in the case of internet services as it is in the case of telephony services. If we summarize, the main reasons for the distinction between different types of retained data are the following:

(1) scope of date to be retained;

(2) suitability of existing service infrastructure for retention.

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)?**

Retained data may be accessed by the Police, the Slovene security and intelligence Agency and the Defence Intelligence Office from the Ministry of defence (Article 107a. para. 1 ECA).

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)?

See reply no. 11. Data may be retained for the purposes of prosecution of crimes pursuable on official duty, according to the provisions of the Criminal procedure Act (hereafter: CPA, Article 149b), purposes of ensuring national security and the constitutional order, and the security, political and economic interests of the state, according to the the Slovenian Intelligence-Security Agency Act (hereafter SISAA) and for the purposes of national defence as stipulated by the Defence Act (hereafter: DA).

Apart from one can access retained data only on the basis of PDPA, however this right is granted only to the individual the data are referred to.

16. **To this end it should be noted that data cannot be accessed in a civil procedure, however if the data would be accessed and subject of a criminal investigation (or accessed by other legitimate means) they could be also used in a civil litigation (e.g. copyright claims) by the rights holder. The latter is only seldom used in Slovenia (in fact there are no reliable data of such occurrences in practice, although the courts and the Ministry of justice have a lawful obligation to prepare an annual report (Article 107e ECA) on the practical use of retention provisions).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)?**

    (1) According to Article 149 b of the Criminal procedure Act the data retained may be accessed if reasons for suspicion (not probable cause[1]) of any crime which is pursuable on official duty exist. The fulfillment of the criteria is adjudicated by the competent investigation judge on District court level.

    (2) According to Articles 24 and 24a of the SISAA the data retained may be accessed if secret activities against the independence, sovereignty and territorial integrity of the Republic of Slovenia or its strategic interest exist (some examples are further defined in the SISAA). Access may be granted by the president of the Supreme court (or his deputy) and on the proposal of the SISA director.

    (3) Regulation of Access to retained data from the Intelligence Unit of the MOD is not specifically regulated, however as the analogy to the SISA framework applies (Article 34, DA) we may observe that also in this case access to data retained is granted

[1] Slovene law makes a distinction between reasons for suspicion and probable cause. The latter is a in theory described as the formal start of criminal proceeding and a significantly higher legal standard. The conditions for probable cause are its precedence, articulation and focusto a certain crime and person. While reasons for suspicion are a less defined and lower standard.

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?

A court order is required in order to grant access to data retained, however hearing or involvement of the aggrieved party is not mandatory. To this end it should be noted that in case of criminal offences access to retained data is subjected to an order of an investigation judge (district court), whereas in all other cases (access following the SISAA and the DA access is subjected to an order by the president of the Supreme court (or in his absence his deputy).

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 required that the aggrieved party is notified of data access. However the aggrieved party may request insight into personal data (according to the PDPA) and obtain this information from the operator (See also response no. 19.), which would eventually include also access to retained data information.

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

Yes. The aggrieved party may request insight into personal data (according to the PDPA). Accordingly the aggrieved party may request from the operator to provide her with all personal data information, related to her, which would eventually include also access to retained data information. If the operator should reject such request a legal remedy is ensured before the Information commissioner and the party has also the possibility of judicial recourse against this decision.

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?

If a data controller refuses access to personal data of a specific person under his control, the person by appeal this decision before the Information Commissioner according to the rules governing the administrative procedure. Recourse to the court (administrative dispute) is permissible against the decision of the Information commissioner.

This is, of course, without prejudice to a possible damages claim if the concerned party suffered damages because of a breach of the data controller.

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.

Yes. The basis is provided already in the ECA where a secure registration of any access to retained data is prescribed already by law. Furthermore the data retained shall be of the same quality as network data. The General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored contains more detailed information on the information system requirements for data retention. Accordingly the following additional requirements are worth observing:

1. the information system must enable a revision track record of any action pertaining to retained data;

2. the information system must be independent from all other systems of the operator;

3. access to retained data shall be granted only to employees with the necessary authorisations, whereby a list of authorisations shall be kept with the operator

4. the retention information system must ensure adequate means of protection against loss or alteration with a regular production of back-up copies;

5. when transmitting retained data at least one cryptographic method shall be used.

6. a revision track record shall be kept for the whole retention period by using secure signatures and secure time stamps.

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

Retained data that were accessed together with the relevant access data shall be retained by the operators 10 years after they had been accessed (Article 107č ECA). There is no direct provision on deletion of accessed retained data, however the analogy with other retention data regulations suggest that also accessed retention data with the operator is deleted after 10 years. This is however in our opinion without prejudice to other bodies that subsequently had access to the data retained (e.g. retained data eventually became part of a criminal file do not fall under those deletion provisions).

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.

The retention regime applies only to providers of electronic communication services (operators), which are defined by the 2002/21/EC framework Directive[2] as services normally provided for remuneration which consist wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services. What is perhaps even more important is that such definition excludes information society services, as defined in Article 1 of Directive 98/34/EC[3], which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

In principle this means that the Directive applies only for operators notified by the NRA, which includes Slovene established legal entities and branches of foreign registered operators (which have to be however also registered with the Slovene NRA). In the majority of cases this will not cause any problem. However it is more or less obvious that the retention regime does not apply to e.g web e-mail service provider or other (newer) communication tools or channels as long as they do not require notification to the NRA.

This notion is in reality a problem of community law and will also have to be solved at that level.

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?

No, there is no such distinction. Any legal entity which qualifies as an operator is obligated to comply with data retention requirements.

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

---

2 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

3 Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations. As amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations

entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

The Slovene operators were very reluctant to provide any information respectively, as there was a general obligation provided in the ECA from 2004 that all communication traffic data shall be deleted after they are no longer necessary for billing purposes (to this end it shall be noted that Slovenia did not make use of the 2002/58 privacy in electronic communications Directive's provisions exemptions that would permit storage of certain other data for legitimate purposes). This would factually mean that the majority of retained data would have to be destroyed within one months after being generated. The operators would actually admit breaches of the ECA if they would admit that they retain certain data also for other purposes.

However there was a general (although unofficial) estimation by experts that all of the data, specified in the Directive had already been retained by the operators for a certain period of time for billing, statistical, analytical and general business purposes. The only exemption may have perhaps been internet telephony 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)?**

See response no. 21.

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)?**

It is almost impossible to give a competent answer to this question as the operators were obligated to ensure the whole data retention free of any charge. As also contracts regulating joint retention are not public it is rather impossible to estimate the incurred costs.

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?**

No. Operators are obligated to ensure retention free of any charge.

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

The operator shall handover retained data that are specified in the extract of the court order received from the competent authority in principle immediately and in

the maximum period of 3 days after he receives the extract of the court order (Article 4 of the Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication network)

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.**

    The ECA provides for fines in the amount between 50.000 and 400.000 EUR for any violations of the data retentions provisions (which are in fact the same as in the Directive).

    Fines are sentenced in the misdemeanour procedure by the Information Commissioner and are without prejudice to possible civil lawsuits for damages from the concerned individuals. Against a decision on a misdemeanour by the Information Commissioner judicial recourse is possible before the regular circuit criminal court.

    This is without prejudice to compensation payments which are however subjected to general rules of tort liability.

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?**

    The competent authority itself: Police, SISA or MOD.

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. Slovenia has no regional/local entities with such powers.

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?**

    No specific rules on cooperation in respect of data retention have been adopted. However, according to the general rules (Article 142 ECA) all the competent authorities that are allowed access to retained data are obligated to co-operate with each other and inform mutually on events that could fall within their respective competences. Otherwise also provisions regulating cooperation in inspection

proceedings (Inspection Act[4], Article 11) and administrative proceedings (General Administrative Procedure Act[5], Articles 33 and 34 regulating mutual assistance) would apply.

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)?

Notwithstanding the fact that Slovenia is a signatory of the CoE Convention on Cybercrime from 2002 onward we have no knowledge on proceedings according tot the cybercrime convention occurring in practice. Foreign state bodies are not entitled to access data directly as they will be unable to obtain the required court order.

In theory this means that cross border police cooperation would have to be used, according to which the Slovene Police would make an application to the Investigation judge to issue a relevant court order and, if successful, convey the retained data received to the requesting Authority.

As an example Slovenia has relevant police co-operation agreements with the following states:

- Austria (Agreement between the Republic of Slovenia and the Republic of Austria on Police Cooperation)[6],
- Hungary (Agreement between the Republic of Slovenia and the Republic of Hungary on cross-border co-operation of law enforcement authorities[7]),
- Belgium (Agreement between the Republic of Slovenia and the Kingdom of Belgium on Police Cooperation[8]),

From the official list of treaties there are no other bilateral or multilateral treaties that could trigger direct enforceability of retention rules from third countries.

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

---

4 OJ RS no. 43/2007

5 O.J. RS no.. 70/2000, 52/2002, 73/2004, 22/2005-UPB1, 119/2005, 24/2006-UPB2, 105/2006-ZUS-1, 126/2007, 65/2008, 47/2009 Odl.US: U-I-54/06-32 (48/2009 popr.), 8/2010

6 OJ RS. no. Int Treaties, 15/2004

7 OJ RS. no. Int Treaties, 4/2007

8 OJ RS. no. Int Treaties, 17/2001

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)?

Information commissioner is the supervisory authority for all personal data protection related issues. (www.ip-rs.si/).

The information commissioner is an independent authority, nominated on proposal of the president of the Republic directly by the national parliament for the term of 5 years. In administrative sense it is an independent institution of the state administration, without any other superior administrative authority. Its decisions are final in the administrative procedure and may only be challenged before the Administrative court in the administrative dispute procedure.

As far as data protection issues are not concerned the authority monitoring compliance with retention rules is the NRA (APEK).

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?

As a final assessments of the legality of the national law transposing the Directive would be in any event published in the OJ RS, we can confirm that no such proceeding has been concluded for now.

We would further assume that there are also currently no pending proceedings on the legality of the Directives transposition as it is very likely that a relevant opinion and/or decision would be available from the information commissioner.

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 have no information on any such proceedings. See also reply no. 36.

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?

The data are stored with the operators. The storage/retention obligation is on the operators, however they may ensure joint storage. Joint storage is specially regulated as a contractual relationship between two operators we do not have insight into this relations, but for their existence. As explained however it is to be expected that data is retained at the transport (backbone) network level by the relevant operator for all other access network providers using his backbone network. Within this meaning it could be said that retention is somehow centralised.

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?

We do not see any legal reservation why retention outside the country could not be permitted. It should be however noted that the retention obligation would still remain with the Slovene operator. Hence, the risk of non-fulfillment of a relevant court order would be his.

If data would be stored in other countries relevant personal data transfer provisions would have to be respected (see also response no. 62) which basically leaves three possible situations:

(1) in case of EU countries transfer is not subjected to any formal requirements (a contractual relation governing retained data transfer is sufficient).

(2) if the country is on the list of countries with adequate data protection (whereby this is deemed for Safe harbour registration in the US) it is not necessary to obtain a decision on adequacy of this countries regulatory framework, however it is still necessary to obtain a decision from the Information Commissioner permitting the transfer of personal data (permission decision); and

(3) if the country is not an EU country nor on the list of countries with adequate data protection it should be necessary to obtain both the decisions on adequacy and the permission decision respectively.

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

a) no data are retained beyond what is permitted?

There is a lawful obligation of the operators to delete the data. Fines in the amount between 50.000 and 400.000 EUR are prescribed for any violation. The Information Commissioner is supervising compliance with this requirement (Article 152 ECA).

The information commissioner ensures compliance with regular and/or irregular inspections with the operators, as those procedures are not public. According to publicy available information up until now there were no final decisions referring to violations of the ECA.On operational level retention is further regulated by the regulations referenced under question no. 7, which regulate specific question on the handover of retained data (see also reply no. 42), Storage of retained data and Retention of police data. To this end it should be noted that the latter regulates merely the access to police registers of retained data, among those also 112 and 113 emergency calls and not to data retained under the provisions of the directive. However as also retained data under the Directive might eventually become part of a police register a connection to data retention cannot be denied.

Storage of retained data further regulated by a General Act on the Secrecy, Confidantiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored adopted by the NRA in 2008. It sets forth a more detailed obligation on the operators namely to set up a specific risk management system (SUVI) defining technical and organizational aspects of managing information systems threats, but especially data storage treats internally with the operators. In respect of data retention the operators are obliged to use cryptographic methods (secure digital signature and secure time stamping) of their choice in all aspects of data retention (storage, handover, deletion) and to ensure respective revision track records. In case of alleged incompliance the burden of proof is with the operators. SUVI's have to be annually reviewed by the operators and the NRA has to be informed thereof.

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)?**

There are no special technical and/or organisational measures that would guarantee that the state bodies cannot get otherwise access to retained data. On the other side there are also no technical interfaces enabling them to do so. As however indicated in the responses to the second part of the questionnaire any other access than with a court order might qualify as a criminal offence against public duty and authorisation. As any transmission of data retention is subjected to an irreversible registration, such offence would be easy to prove and it is rather unlikely that public bodies [or respective individuals] would make use of means referred to in the question.

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

The information system of the operator must also be separated from other similar systems.

Failure to ensure compliance with this requirement would most likely, but not necessary, prove that data is used by the operator also for other purposes and accordingly fines in the amount between 50.000 and 400.000 EUR could be sentenced (Article 152 ECA) .

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.**

The operators must establish a special internal authorisation scheme. Further a revision track on accessing the retained information must be kept and securely electronically signed and time stamped.

Failure to ensure compliance with this requirement could be fined according to the above provisions.

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

Telephony services data have destroyed after a 14 months retention period, provided that they had not been transmitted to the competent authorities and data retained on other services is destroyed after the expiration of the 8 months

retention period. Deletion has to be in both cases irrevocable and has to be ensured in a way that it is impossible to restore the data with any technical means (violation is sanctioned under point 71, Article 152 ECA).

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 is no automatic notification of the aggrieves parties. See also response no. 18.

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

No special regulation in respect of retention applies to sensitive data. It is however possible that such data are privileged and therefore useless for the purposes for that they were accessed (e.g. for the reasons of Article 236 CPA, see also cf. response no. 54). However it is impossible to determine whether privileged data are being retained before actually accessing them. See also response no. 12. As traffic data are also communication data it is our understanding that it would be inadmissible in a criminal proceeding to use such communication 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. The operator must ensure proper internal control and organisational measures (as defined by the NRA General Act). Public control is ensured by the inspection of the Information commissioner.

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?

The only technical standard that is specifically referenced is SIST-TS TS 102 657 V1.1.2.

On operational level the handover procedure is governed by the Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication network. Accordingly the accessing party must transmit to the operator parts of the relevant court order, granting access to retained data. As the operators may ensure joint retention (i.e. it is far more cost effective for the operators to retain data on transport network level, which in practice means that data is as a rule retained on the transport network level, by the transport network operator, who retains data for other operators using his communication network) which may not be the same as the operator actually retaining data it is important to note that the court order will be addressed to the

specific operator, which may not be the same as the operator actually retaining data. In such a case the addressed operator fulfils its lawful obligation if he ensures that retained data are handed over by the operator actually retaining data or by connecting its network to the network of the actual retainer in a way that enables fulfilment of the court order.

In this sense it is necessary that the operational systems of the operators are interoperable, however we cannot confirm that the system is interoperable with the competent authorities accessing data.

The court order granting access shall be as a rule transmitted to the operator with the use of secure electronic communication means and standard SIST-TS TS 102 657 V1.1.2. must be respected. Other (physical) means of transmission are allowed only as an exception, but also here security must be ensured. Those regulations apply also vice versa in the process of data handover.

Again, as a rule, data shall be handed over immediately but in 3 days at latest. If cryptography or other storage methods used, the transmitted data shall be provided in a decrypted version. Retained data shall be transmitted by and to authorized personnel only.

After the transmission the operator must register transmission of data retention. Registration must be undersigned with a secure electronic signature and secure time stamp.

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.

On operational level the court order is transmitted (by e-mail or physical means) from the authorised sender on the side of the Police to the authorised recipient on the side of the operator. from here on there are two possibilities: (i) the authorised recipient will either prepare the requested retained data by himself or, in the case of joint retention (ii) forward the order to the authorised recipient of the operator actually retaining data. After retained data is prepared in a way required by the order, data is transmitted to the sender of the order by the addressed operator in the same way at it was received.

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?

We do not have knowledge of any such proceedings occurring in practice. In theory the general means of cross border police cooperation, following the provisions of 514 - 520 CPA (as indicated in the reply to question no. 34, there are currently three bilateral agreements in force that could be subject to those provisions) would have to be used, according to which the Slovene Police would make an application to the Investigation judge to issue a relevant court order. In such case, apart from the request itself the only possible working language would be Slovene.

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).

Apart from the wider internet community (comprising i.e. "advanced" internet users and experts of different types) it can be observed that the general public is quite unaware of data retention but also other applied surveillance methods. This holds true also for the relevant legal profession concerned who are in general not only unaware of data protection rules and even more on data retention. Like this also the public debate in the implementation process can be described: the operators unsuccessfully only followed the aim to be reimbursed for data retention, whereas other parts of civil society that raised questions on the legitimacy of the institute itself but also on the period of retention, proportionality and other open issues, where silenced by the relevant Ministries that simply opted for the only obvious solution from the prosecution perspective.

To this end credits must be given to the Information Commissioner who not only very efficiently supervises all topics related to personal data, but with his public appearances and opinions in fact raises public awareness on the importance of this subject matter.

As to the rules that applied before implementing the Directive: the 2006 ECA amendments replaced the previous ECA regulation on traffic data, which required immediate deletion of any data as long they are no longer necessary for service provision or billing. It should be noted that Slovenia did not make use of its rights from the 2002/58 Directive in implementing any retention measures. Thus access is only possible to data stored for the purpose of billing or service provision. As this first ECA was primarily an implementation measure of the new regulatory framework for electronic communication Directives it is only short lived; it entered into force together with the Slovene EU accession in May 2004. From the subject matter it replaced the second Telecommunications act enacted in May 2001, which itself replaced the first Telecommunications act from 1997. The second Telecommunications act has very similar provisions regarding the deletion of communication data to those in the Electronic communications act. However contrary to the latter, the second Telecommunications act sets out conditions for a longer storage period alternatively, thus allowing an interpretation, though only weakly grounded, that data can be legally stored until they fall under the statute of

limitations. As those are in Slovene law set to 1, 3 or even 5 years, depending on the nature of the contractual relationships, these periods are more than sufficient in the light of criminal pursuit. The first Telecommunication act had only very general provisions on that subject matter. However for the period of the duration of the contractual relationship between the operator and his user, basically any data would be retained legally. Thus retention or deletion of these data was more a question of the operators' policy.

The evolution of the Slovene criminal procedure act in this respect is perhaps not as turbulent but also very interesting. To its last amendment, enacted just after the Slovene EU accession, the Criminal procedure act contained no specific provision on access to retained communication data. Nevertheless access to retained data was possible, even without judicial control. Data could namely be accessed on general investigation powers of the police.

Our short analysis provides us with the following conclusions: until may 2001 police could access any retained data without judicial control if only reasons for suspicion of any crime pursuable on official duty was given. Thus as there were also no specific rules on data retention, the actual data that could be accessed dependent mostly on the operators' policy on communication data storage. There are strong reasons to believe that such practice continued even after the adoption of the second Telecommunications act in may 2001, which was far more restrictive in respect of communication data storage. Yet legislation still allowed for such interpretation and more importantly, access was still possible without any judicial control. The Electronic communications act, together with the last amendments of the Criminal procedure act represent in this respect a breach of existing practice, the first providing for immediate deletion of data when no longer needed for billing and the second guaranteeing judicial control by means of a warrant over any access to retained data.

However, as the Electronic communications act was adopted in the framework of transposing the Acquis to Slovene law- which was just before accession was most turbulent- the analysis offers another conclusion. The impact of opting against any retention measures, according to the 2002/58 Directive on criminal proceedings, was most likely overlooked.

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)?

No. According to the Slovene constitution retention of personal data without a specific lawful purpose is illegal. Data retention is very specific in this respect as it is perhaps the only group of personal data which has no purpose at the time of retention and the lawful reasons may appear only in a later moment.

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.

According to Article 107e ECA the District court issuing orders on access to data retention must keep a record on the issued orders and the Ministry of justice is obligated to prepare annually a report on data retention execution which is subsequently notified also the the European Commission. The first report should be already prepared in 2007, however on the relevant pages of the Slovene Ministry of Justice, no such document can be found.

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?

There are no visible signs on changed communication patterns after data retention in Slovenia.

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?

As explained those discussions were ongoing in the years 2008 and 2009 and the result was a shortening of the retention period.

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) law[9] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a *specific* reason?

Slovenia has a very strict constitutional framework in respect of personal data and especially communication data.

Protection of personal data is regulated in Article 38 of the Constitution. Accordingly the use of personal data contrary to the purpose for which they had been collected is prohibited. Collection, processing and confidentiality of personal data shall be provided by law. Another important notion is that anyone has the right to obtain personal data that relate to him and may recourse to the court if his rights are violated.

However in respect of retained data the perhaps more important provision is contained in Article 37 of the Slovene Constitution, governing confidentiality of letters and other means of communication. Accordingly it can be provided only by law that the confidentiality of communications is revoked for (i) certain period of time, on a (ii) court order of the competent court and (iii) if this is necessary for the purposes of a criminal proceeding or for national security.

A further noteworthy observation that was also reaffirmed by the constitutional court on some occasions is that traffic data are also subjected to special constitutional protection on communication data. According to the case law of the Slovene Constitutional court there is no distinction between communication content and traffic data as both are given the same constitutional protection.

Considering the above it can be observed that the relevant constitutional provisions were respected in the event of the Directives transposition. Namely: access to data retained is only allowed in criminal proceedings and if national security (inner or

---

[9] 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).

outer) is in question; access is always subjected to judicial control and for a certain period of time (this is in principle defined in the relevant court order however maximum periods are already defined by law).

The only somehow problematic issue of data retention respectively is that the purpose of retention is unknown in a particular case in the moment when the data is retained. However, it would be rather difficult to argue that such a solution is not proportionate as it is very much clear that the only purpose of retention can be a constitutionally highly protected value (criminal proceeding and/or national security).

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?

A general constitutional rule is that civil rights and freedoms may only be limited to the extent which is absolutely necessary to achieve a certain aim which is a prevailing public interest. The Slovene Constitutional court elaborated well developed guidelins in its Case-Law, it should be however noted that (i) as cases are decided on a case by case basis the case-law may be subject of change and that therefore (ii) no rules as such exist. The constitutional doctrine on phenomena of the principle of proportionality goes however well beyond the aims of data retention (at least insofar there is no relevant case law available).

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?

For now there is no such jurisprudence, neither existent, nor pending. However it has been ruled by the Constitutional court that traffic data are also communication data and therefore subject of special constitutional protection

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?

A general constitutional rule is that civil rights and freedoms may only be limited to the extent which is absolutely necessary to achieve a certain aim which is a prevailing public interest however assessment/balance of interests has to be carried out and adjudicated in each individual case

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)?

Although there is no direct constitutional provision regulating that matter the result would be very likely very much the same as if., As these information (cf. 12

question) are privileged in a criminal proceeding (based on Article 29 of the Slovene Constitution more précised rules on privileged data are laid down by Article 236 CPA – privileged witnesses), their procedural value is null. In a criminal proceeding they would have to be excluded and no evidence obtained on their bases (fruit of the poisonous tree) would be allowed.

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 retention obligation interfers with the constitutional freedoms of privacy of communication (Article 37) and right of personal data protection (Article 38). There simple (but strict) constitutional provisions stipulating that such data may only be retained if (i) so provided by law and (ii) that the rights may only be suspended for (ii-a) a limited period of time by (ii-b) decision of the competent court of law. Those criteria have to be fulfilled by any regulation on data retention. In practice this means that – apart from the very technical implementation measures – (i) every regulation on data retention has to be provided by law (which has to respect laso certain time limitations) and (ii) that any access to retained data is subjected to judicial control.

To this end it should be noted that there are ongoing discussion in academia and jurisdiction on the legitimacy of the data retention institute itself, however certain legitimate interests to retention cannot be denied. Fact is namely that retention is not new as a police right but merely a detailed definition on what the Police (and others) can expect when gathering relevant information from the operators.

A very substantiated discussion was however focused on the period of retention. When implementing the Directive for the first time the Police, SISA, MOD and the General Attorney represented the position that even the maximum retention period would be insufficient in certain cases and therefore the maximum period was adopted in the ECA. Fact however is that for the time being there were no information by anybody how one or other solution would affect their work. In fact this solution was adopted quite “over the thumb” without any particular legitimate reasons. For that very reason it was argued in academia and general public that the solution was not proportionate also from the constitutional perspective which requires that limitations of civil rights and freedoms shall be proportionate.

As explained this was in a way put also on the agenda of the governing coalition and the respective ECA provision was subsequently changed and it is rather a speculation whether the previous regulation would stand the constitutional test.

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)?

National law is very broad in this respect. According to Article 148 of the Slovene Criminal procedure act provides that if suspicious cause is given, the Police may take the appropriate measures to secure any object or collect any information which might be used as evidence in criminal proceedings. Factually this means that the Police may require data from anybody storing data if the Police thinks those data could be of use in a criminal proceeding.

Up to its last amendment, enacted just after the Slovene EU accession, the Criminal procedure act contained no specific provision on access to retained communication data. Accordingly data could be accessed on the general investigation powers of the police described above. Apart from electronic communication retention data only certain financial transactions data are specifically regulated in the Criminal procedure Act. This means that only those two groups of entities have a specially regulated obligation in respect of the criminal procedure.

Other entities may be drawn for the purposes of data retention, however the competent authorities will have to rely on information stored according to their own business practice and sector specific regulations.

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

There is no such obligation in the Slovene constitutional law. In fact, according to national law (e.g. Article 148 CPA) private entities are obliged to assist public bodies in performing their official duties.

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?

International treaties, ratified by the Parliament apply directly, provided of course that the relevant treaty provision are in itself capable of direct application and/or effect and so that they do not require any further legislative intervention. If so, international treaties ratified by the Parliament are in the hierarchy of norms placed directly under the Constitution and thus also above other Acts (laws) adopted by the Parliament.

The ECHR has a special position within the legal hierarchy as accordingly the European Court of Human Rights is given the authority do adjudicate violations of human rights, stipulated by the ECHR when all other legal remedies before the national courts are exhausted.

Please note that not all international treaties have the same position in the hierarchy as the Slovene legislation also provides for the possibility to ratify certain less important treaties (regulation mostly operational issues of an already parliamentary ratified treaty) with a governmental decree.

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?**

    According to Article 3a of the Slovene Constitution EC Regulations and in certain cases (according to ECJ case law) also Directives may have direct/immediate effect. With this Article also certain sovereignty rights were transferred to the EU.

    In general however a Directive is transposed with a necessary national regulation. Mostly this will be an act of the Parliament as a Directive is likely to influence human rights and liberties which can only be limited / regulated by law.

    Apart from that strictly technical legislation is however transposed with administrative regulations on the Governmental or even Ministry level.

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?**

    See response no. 59 above. There are no such limitation under national law.

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 Ministry for higher education, science and technology (under which competences the Directorate for information society and further the Sector for electronic communications are) is responsible for the legislative framework.

    Regulation of technical questions pertaining to data retention is split among the Ministry for higher education, science and technology, (which in consent with the Ministry of the Interior, the National security and intelligence Agency and the Ministry of defense) adopts and the NRA.

    Privacy protection issues are under the competences of the Information Commissioner who has also inspection powers re.

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

There is no such direct limitation on constitutional level. However adequacy of the receiving countries legal system must be established.

Transmission of retained data - which are also personal data - to other countries falls under the relevant provisions of the PDPA. As according to Directive 95/46/EC of the European Parliament and of the Council of 24th of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data inter EU transfer of personal data is to be considered equally as a transfer Accordingly there are in principle the following different regimes that can apply dependant of the receiving third country.

(1) the transfer to a third country is permissible if the National supervisory authority (Information Commissioner) issues a decision about the country to which the data is exported providing a proper level of personal data protection.

(2) The previously mentioned decision is not necessary if a third country is on the list of countries referred to in Article 66 PDPA for which it is determined to have fully or partly ensured an adequate level of protection of personal data, or have not ensured such protection.

(3) Following Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Guidelines and related frequently asked questions issued – FAQ ("guidelines") by the US Department of Commerce, organization registered under the Safe Harbor Guidelines are considered to ensure an adequate level of protection for personal data transferred from the Community to organizations established in the United States.

Notwithstanding any of the indents above, the person intending to transfer personal data must obtain a decision from the Information Commissioner permitting the transfer of personal data. The person may then transfer personal data only upon receipt of the decision permitting transfer. Such transfer is recorded (Article 71 PDPA) and the decision communicated to the competent body of the European Union and to the Member States of the European Union (Article 70/5 PDPA).

To summarize there are in principle 3 possible situations in respect to third countries in respect to transmission of retained data:

(1) in case of EU countries transfer is not subjected to any formal requirements.

(2) if the country is on the list of countries with adequate data protection (whereby this is deemed for Safe harbour registration in the US) it is not

necessary to obtain a decision on adequacy of this countries regulatory framework, however it is still necessary to obtain a decision from the Information Commissioner permitting the transfer of personal data (permission decision)

(3) if the country is not an EU country nor on the list of countries with adequate data protection it should be necessary to obtain both the decisions on adequacy and the permission decision respectively.

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?

It is rather difficult to identify any useful improvement on strictly national level. This is an issue that will have to be resolved anyhow on the EU level.

Notwithstanding the above the Data retention Directive doubtlessly is an invasion of privacy. However the assessment as a measure, which is not necessary in a democratic society, can only be hardly accepted if at the same time we agree that legitimate interests of criminal pursuit and state security and defense on data retention exist. The very idea of data retention is therefore legitimate. The way in was put into practice under Slovene law can be described as balanced. One can only hardly imagine a more strict approach in the respect of access (mandatory court order, in certain cases from the Supreme court) and storage (strict provisions and requirements) to data, then in the existing legal framework.

However, a different question is the very technical regulation of data retention, where some questions remain open and where there will always be room for improvement. The rather rigid concept of regulation is primarily suitable for long existing fixed telephony services, while already in case of mobile telephony due to the rapid development of new services problems are inherent to the very development. The integration and convergence of services, equipment and communications makes it rather difficult for data retention to be effective. In other words: culprits aware of data retention will always find appropriate means to circumvent primary retention aims, putting the whole retention framework under question. It is our belief that improvements can and should be expected on this part of the retention framework.

The fast development of new forms of communications making use of the internet requires a different approach to data retention. Perhaps a dynamic approach, focusing on the provision of legal basis for actually stored data by the individual operator which is evolving with the service itself, could provide for a new concept in this respect in the future.

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

Slovenia

Ulčar & partners Law Firm ltd., Klemen Tičar, Attorney at law

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*?

National constitutional law regulates protection of personal data in Articles 37 and 38. The cited Articles govern protection of privacy of correspondence and other means of communication (Article 37) and the protection of personal data.

Accordingly privacy of correspondence and other means of communication is guaranteed and only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a limited period of time necessary for the institution or course of criminal proceedings or for reasons of national security.

Irrespective of the cited provisions setting very strict limitations to the legislator when regulating privacy of communication issues, there is in itself no constitutional right to communicate anonymously within the meaning of not being disclosed as a participant of the communication to others.

2. **Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country. 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 your 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?**

   Currently there are no amendments to current data retention legislation that would presently discussed in public. Although the ECA was very recently (on April 28th 2011) amended in order to [provisionally] comply with provisions of the new regulatory framework (Directives 136/2009/EC and 140/2009/EC), data retention provision remain unchanged and hence also no public debate was opened.

   In the general public among the most recent events and debates where data retention issues were discussed we may observe a report the Article 29 Working party report as of July 2010, identifying lack of compliance with data retention provision and lack of supervision was subject of a certain degree of attention (by the Information commissioner) and activities of the Institute of Criminology at the Faculty of law in Ljubljana.

   It should be however noted that the debate focuses on rather general and principal questions of data retention, whilst particular technical, organizational and/or legal questions and concrete solutions or improvements are not particularly debated.

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?**

   On principal level provisions regulating the cooperation of private actors with public authorities are defined very broadly and on a general level, whilst sector specific legislation (other than electronic communications) does not regulate the retention of data for purposes which would fall outside the core business activities. Notwithstanding the above on certain sectors (banking, insurances) provisions regulating mandatory keeping of archives for a defined period of time, combined with the general rules o cooperation (e.g. Article 148 CPA, see below) may have a very similar effect as data retention (retention of traffic and location data of electronic communication).

   This is possible due to the fact that the relevant Acts, regulating access to documentation of private actors by the public authorities (apart of certain exceptions to the banking sector) may in principle apply without limitation to any other private entity and to any data and/or documentation and mostly without any prior judicial control. However as on the other side such data are in principle not subject to any

specific retention regimes, the respective public authorities have no guarantee on their scope, quality and (to a certain extent) even existence.

In respect of access to such date it can be observed that Slovene legislation contains only very broad and general provision on the scope of cooperation. For example Article 148 CPA provides that police may – in case of suspicion a publicly pursuable offence was committed – take all necessary measures to identify the perpetrator and to secure traces or objects that could be used as evidence in a criminal proceeding [...] among these the police may [...] in the presence of the lawful representative search company premises and documentation and take other appropriate means necessary.[...]. Within this provision the police certainly has the possibility to access in principle any data.

A somehow different provision can be observed in the SISAA (Slovene Inteligence and Security Agency Act, its relevant provisions apply simultaneously also in the Defence Act), where following Article 16 data controllers are obligated upon request of the Director General of SISAA to allow insight and access to personal data under their control. As retained data on electronic communication are regulated separately (Articles 21-25), those provisions (presented in the I. questionnaire) apply according to the lex specialis rule.

Although both approaches are quite different, they lead to a similar result as far as data other than retained data are concerned as they in principle allow access to any data available and under the control of the private entity concerned.

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?**

The privilege against self incrimination is provision by Article 29, indent 4 of the Slovene Constitution regulating constitutional guarantees criminal proceedings. Accordingly a defendant is granted the right to refuse testimony which would be self incriminating or to confess his guilt. Following relevant case law of the Constitutional court this right (e.g. Decision no. 134/97 as of 14.3.2002) is one of the key procedural guarantees an element of the constitutionally granted presumption of innocence. The practical consequence is that the defendant may remain completely passive in the procedure leaving the burden of proof completely to the District attorney. The same provision is repeated in Article 5 CPA.

The rights of other persons to refuse/be absolved from testimony are regulated in Article 236 CPA. Accordingly the defendant's spouse, all his blood relatives in the direct line, blood relatives in the side line to the 3rd grade, in-laws to the 2nd grade, his adoptee, confessor or similar, attorney at law, physician, social worker,

psychiatrist or any other person who within his profession had been acquainted with certain facts on the defendant may be absolved to testify on such facts; this privilege does however not apply to criminal offences against sexual integrity, protection of minor and human trafficking. The same privilege applies also for information which is classified under the provisions of the Act on classified information until such classification is in force.

Neither of the above refers or includes retained data on electronic communication. It can be therefore concluded that those data cannot be subjected to the privileges explained above. As those privileges refer to the subject of certain communication and not to the very fact a communication occurred it is also hard to identify any possible conflict between both of them. It is namely inherent to the privilege from Article 236 CPA to admit a communication occurred, which would be basically all the information that can be possibly obtained from data retention for evidence purposes.

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?**

   The body requesting and receiving data must keep the data according to the provisions of the CIA and PDPA, if applicable. In practice this means that the body has to observe rules on technical, organisational and legal protection of the data as provided by an internal act of the relevant public body. In practice this means that the data subjected to limited access on a separate computer, likely without outside connection and that a access protocol is kept.

   Otherwise the General Act on the Secrecy, confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored regulates only storage with the operators.

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.**

   Although the Ministry of justice is by law (ECA, Article 107.e from 2006 onward) obligated to annually (until February 20th) report on the application of data retention access [within the scope, referred to in the question), according to informal information two such reports were elaborated and reported to the EC Commission, however are not published.

   Apart of that the only publicly available statistical source on data retention and access can be found with the Information commissioner, however this statistic is less relevant as it merely refers to the cases of the Information commissioner and not especially to data retention access:

   https://www.ip-rs.si/index.php?id=323

B. Country-specific questions

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

On a general level there are in principle no indications the data retention regime would be violating a certain constitutional right or freedom. In principle it could be observed that access to any personal data [and retained data qualify as such] complies with the constitution, if scope, intention, access, supervision and grounds of collection are provided by law. As the regime as a whole is regulated by law and observing that the law regulates all constitutionally relevant aspects there are in principle no evident general [constitutional] objections to the data retention regime.

A separate question however is whether the relevant constitutional principles – e.g. principle of proportionality - were observed in the specific regulatory solutions. An example is for instance the period of retention: it is likely that the very retention period could be against the constitutional principle of proportionality if the legislator cannot prove plausible and relevant grounds for a certain retention period. As observed there are currently no public data on the use and statistics of the retention regime [although according to informal information an annual statistic was prepared and reported to the Commission], which lead to the conclusion that a retention period was regulated without any just cause. Such legislative approach could be however argued as being contrary to the principle of proportionality for a very principle reason.

To this end it should be noted that this is merely an example of a much deeper and wider general problem of transposing EU rules into national legislation without making reference or observing valid principles of national constitutional law.

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?

Following the applied case law of the Constitutional court (Case no. U-I-92/96 Decision as of 20.3.2002 and no. Up-106/05, Decision as of 2.10.2008) any electronic communication data are subjected to the constitutional secrecy of correspondence. In the latter the Constitutional court explicitly stated that "[…] Considering the above, the subject of privacy of communication shall be interpreted broadly and shall include also traffic data which is an integral part of the communication.[…]".

Consequently the privacy of communication privilege (as provided in Articles 37 and 38 of the Slovene Constitution) applies also to retained data, which are subjected to the same constitutional warranties as any other fact of communication (any scope, intention, access, supervision and grounds of collection must be defined by law).

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.**

   The principle of proportionality is, when assessing the constitutionality of a measure limiting fundamental freedoms [as interpreted by the Slovene Constitutional court], adjudicated by a three part test, elaborated by the case law of the Constitutional court and. Accordingly suitability, necessity and proportionality (strictu sensu) of a given legislative measure are assessed. The suitability test refers to the question whether a certain norm is suitable for the envisaged legislative purpose. Necessity is defined with the notion that a given legislative purpose cannot be achieved through other means [and hence it is necessary to limit a certain human right or freedom], whereas the (strictu sensu) "narrow" proportionality tries to establish whether the applied limitation of a certain human right is reasonably proportionate with the protected value.

   As indicated under response no. 7, although no principle objection to the retention regime is obvious, there are several indications that certain regulations of the retention would not stand the described test of proportionality as the legislator would have difficulties proving necessity and/or strict proportionality of an applied regulatory measure.

10. **It seems that Art. 3a of the Slovene Constitution marks some formal as well as substantial limits to the conferral of powers to the EU (cf. Art. 3a para. 1: "two-thirds majority vote of all deputies"; "based on respect for human rights and fundamental freedoms, democracy, and the principles of the rule of law"). Can you confirm this? If so:**

    a) **Please explain these rules.**

       Actually the wording of Article 3a is not that limiting if we consider the fact that the powers were already conferred to the EU with the ratification of the accession treaties, where a 2/3 majority vote was required. From there on every EC Regulation and/or Directive and/or Decision can/is directly applicable/effective also in Slovenia, however not subjected to any special rules of adoption. The notion on the "respect for human rights and fundamental freedoms, democracy, and the principles of the rule of law" was consummated with the ratification of the same Accession treaties and is not subjected to any posterior adjudication. In other words: with the ratification of the accession treaties all EC secondary legislation is in principle considered as respecting "human rights and fundamental freedoms, democracy, and the principles of the rule of law", those rules are equalized with any national law or regulation.

b) **Is the constitutionally fixed limit to a conferral of national sovereignties to the EU in any way binding for representatives of your country in EU organs and institutions (e.g. the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?**

As indicated a 2/3 majority vote was necessary only for the ratification of the EU accession treaties, whilst any other legislative measure (e.g. an Act of parliament transposing a certain Directive) is not subjected to any special rules and a simple majority vote is sufficient. See also previous response.

c) **Is there any way for national courts to check the compliance of EU law with the Slovene Constitution (and, in particular, the fundamental rights guaranteed therein)?**

There is no specially regulated procedure respectively. It should be however noted that national courts may request from the Constitutional court to assess compliance of a certain law with the Constitution. As this right is not limited only to national provision, it follows that also relevant EC regulations [if applicable] can be in principle subject of such compliance assessment.

11. **Please provide a list of criminal offences for the investigation of which data retained may be requested by the competent authorities upon a court order.**

A request for disclosure of retained data may be granted for any publicly pursuable criminal offence [upon additional request a relevant translation of the offences may be prepared.].

Apart from the offences, defined in Articles 140., 142, 158. to 162. and 166 of the CC, [English version please follow the link below]:

http://www.policija.si/eng/images/stories/Legislation/pdf/CriminalCode2009.pdf

a request for disclosure of retained data may be requested and granted for any other criminal offence.

12. **As regards the rights of the data subject to be informed about the data retained (see your answer to question 19 of the first questionnaire): Please provide the relevant legal norm of the PDPA laying down this right. Does the law provide for any exemptions to the right to be informed? If so: please describe their content.**

Access to personal data is regulated in Article 30/1 PDPA. Accordingly any individual has the right upon request to insight, obtain, request information on disclosure, list of users and the purpose of collection for all personal data, held by a specific data controller. The data controller is obligated to allow such access/insight and to provide the individual the information requested. The access procedure is

further regulated in the following provisions (Articles 32-35 PDPA) and the access right is subject to judicial control in the course of an administrative dispute.

An exception to the rule can be identified in the provision of paragraph 4) Article 149.b, CPA, explicitly prohibiting the operator of electronic communications to disclose any information on the access to data retained by the public authorities. Accordingly the concerned individual will be denied access under PDPA to any information on disclosure of retained data to the competent authorities. This does however not anyhow impede his rights of access to information in the course of a criminal proceeding.

13. **As regards question 30 of the first questionnaire: Does the law provide for any criminal liability in case of an infringement of data retention provisions? If so: please describe the relevant norms.**

Apart from the relevant provisions on minor offences (misdemeanours) the CC does not provide for an explicit norm incriminating infringement of data retention provisions. As indicated, in principle an infringement of data retention provisions would be qualified as a misdemeanour (minor offence) under the ECA.

However, irrespective of the above an infringement of data retention provisions could still qualify as a criminal offence under CC [under certain general qualification]. Especially offences against official duties and public authorisations could apply [if committed by a public official] as provided by chapter 26 of the Slovene CC (Article 257 – 260) and/or a criminal offence of abuse of personal data.

Abuse of Office or Official Duties is defined as the act of an official or a public officer who, with the intention of procuring any non-property benefit for himself or another, or of causing damage to another, abuses his office or exceeds the limits of his official duties or fails to perform his official duties.

Misfeasance in Office is qualified as the act of an official who knowingly violates regulations and other prescriptions or fails to exercise due supervision or performs his duties in an otherwise unscrupulous manner, even though he predicts or should and could predict that such conduct might cause a serious violation of the rights of another or major damage to public property or a major loss of property and such a violation or damage actually occurs.

Another possibility is described by the offence of "Forgery or Destruction of an Official Paper, Book, File or Historical Archives" which is defined as an act of an official who enters false information or fails to enter any relevant information in an official paper, book, or file, or certifies such a paper, book or file containing false information with his signature or stamp, or renders the creation of such a paper, book or file possible, and/or use of a false official paper, book or file as genuine, or hiding or substantially damaging papers, books or files useless, shall be punished to the same extent.

The most likely applicable offence in case of data retention rules violation would however be "Disclosure of Classified Information. As provided in Article 260 CC

disclosure of classified information is committed by an official or any other person who, in non-compliance with his duties to protect classified information, communicates or conveys information designated as classified information to another person, or otherwise provides him with access to such information or with the possibility of collecting such information in order to convey the same to an unauthorised person. As namely retained data are subjected to the same regime as classified information any unlawful infringement of those could also qualify as unlawful disclosure of classified information.

Another possible qualification of a data retention rules violation can be found in Article 143 CC which regulates the Abuse of Personal Data. This offence is defined as unlawful use of personal data, which may be kept only on the basis of the law or on the basis of the personal consent of the individual, to whom the personal data relate and/or braking into a computer database in order to acquire personal data.

14. **In your answer to question 23 of the first questionnaire, you mention that only "providers of electronic communications services (operators)" are obligated to retain data. However, according to Art. 3 no. 23 ECA, "Operator shall mean a network operator or service provider". Does this mean that both operators of public communications networks and providers of electronic communications services shall be obligated to retain data under the national data retention regime? If so: 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.**

    There are no explicit rules preventing the same data from being retained more than once. However as the retention obligation would always refer only to a certain network access point, only the respective service provider, providing services to the end user is obliged to retain data. But as he is for the same reason also the only entity who has the necessary legal foundation to retain data, retention of the same data by others is unlawful – as such service provider is the only lawful data controller. It is however possible that other retain data on his behalf – as data processors. In this case they act on behalf of the data controller by using his initial right to retain/control data.

15. **Please describe in detail the content of the technical and organisational specifications laid down in the "Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks" and in the "General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored" (as mentioned in your answer to question 7 of the first questionnaire). In particular: how are the following areas regulated by these specifications:**

a) **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**

Provisions regulating physical protection of the retained data can only be found in the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored provides in respect of retained data that. Accordingly the data retention information system shall be independent and separated of any other information system of the operator, who shall on his internal level prescribe relevant compliance procedures. Apart from this program norms there are no other provisions regulating physical protection more closely.

The Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks do not contain any provisions on physical protection.

b) **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)**

There are no special rules in the ECA defining or prescribing mandatory the use of a specific method to ensure security. However, as the operators are obliged to follow Article 107c ECA (according to which it is mandatory to take the appropriate technical and organisational measures to ensure safe and secure storage of retained data), the use of cryptographic methods is likely to be the only applicable solution.

Such approach was more explicitly confirmed by provisions of the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored, where the use of secure electronic signatures and time stamps is mentioned, however still keeping thepossibility of other appropriate methods.

The notion that cryptography with the use of secure electronic signatures and time stamps shall be used is further confirmed by certain provisions of the Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks (e.g. Article 2, paragraph 1, indent 8 and Article 4) which imply the use of cryptography when regulating certain aspects of data transfer to the competent authorities.

c) **rules on internal access restriction and control (e.g. four-eyes principle, secure authentification mechanisms/certificates)**

There are no specific legislative provisions on internal access and restrictions which is left to the discretion of the concerned operator.

d) access logging

According to Article 3, parapragh 2 of the Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks only specially empowered individuals of the operator [and of the competent authority] shall be acquainted with the mere fact of transmission of retained data, its scope and content.

A similar provision is repeated by the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored.

e) secure (irreversible) deletion after expiry

According to the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored the deletion shall be procured with a method ensuring irreversible deletion.

f) error correction mechanisms (e.g. hash functions, checksums)

There are no specific legislative provisions on error correction..

g) secure data transmission (cryptographic security, postal delivery)

Article 3 of the Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks provides that transmission of the court order from the competent authority to the operator shall comply with the communication standard SIST-TS TS 102 657 V1.1.2. In exceptional circumstances, when the use of the cited standard is technically impossible, the order may be transferred by other means (personally).

As a rule the requested data shall be then securely transmitted from the operator to the competent authority to the address indicated by the competent authority, using electronic signatures of a qualified certification authority. The exception may again be that the competent authority indicated another way or means of transmission, which has to be [in this case] respected.

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

The access is based on a access per request procedure without direct access. According to the Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks the competent authority files a request with a transcript of a respective court order and the operator executes the request by preparing and sending data indicated in the court order. In principle in both

communications the use of secure electronic means of communication is prescribed.

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

There are no special measures to ensure that data transmitted is used exclusively for the designated purpose. However, as every data transmission is subjected to a irreversible registration using secure electronic signatures and secure time stamps the purpose (Article 5 of the Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks) any abuse would be easy to prove.

j) staff training/internal control mechanisms to ensure compliance with the law and other rules

In the applicable legislation there are no mandatory - staff training and /or internal control mechanisms to ensure compliance with the law and other rules.

k) 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)

Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks do not provide for any mandatory provision respectively, however they provide for such a possibility. Accordingly an operator may fulfil its retention obligation also through another operator, provided that relevant security measures are respected. It can be observed that the legislator left the decision on the method of retention to the operators, which can opt for different solutions; i.e. to ensure retention on their own, or to retain via another operator (most likely on the transport network). As it is likely that transport network operators will be able to retain data most economically the choose of option is somehow left as a business decision of the individual operator.

l) Please also explain whether 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)?

Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication networks as well as the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored regulate merely the storage and transmission of data in the context of data retention and not any other data processing on electronic communication. Those are subjected to the general rules of the PDPA and ECA.

16. As regards your answer to question 33 of the first questionnaire:

a) At second glance, Art. 124 ECA seems to apply exclusively to the exchange of data between supervisory bodies, so other authorities (including those entitled to request the data retained) might not rely on this provision. Can you confirm or disprove this?

Article 142 [not 124] ECA indeed regulates only cooperation of supervisory bodies under ECA, which means that other bodies cannot rely on this provision. It should be however observed that practically any other public body could in such case rely on the relevant provision of the APA (explained below), which are substantially very much the same.

b) Please describe in detail the general rules (e.g. Art. 11 Inspection Act, Art. 33, 34 Administrative Procedure Act) for co-operation among the different bodies accessing the data and between these and other public authorities.

Article 33 APA provides that public bodies on state and local level are obligated to provide legal assistance to each other within their respective competences. Such assistance refers to the provision of documents, facts and other information, necessary to decide in a specific procedure. The requesting public body may assistance by a special request to the addressee and the addressee shall grant such request with no delay but in any case not later that in 30 days period. The only applicable exception is that the courts may refuse if this would impede a court proceeding. Article 34 APA regulates cooperation with foreign public authorities where the principle of reciprocity applies if cooperation is not agreed by a special bi- or multi- lateral agreement.

Article 11 IA is from a legal perspective merely a more detailed derivation of the presented principle of cooperation described above, which was introduced due to the specific work of inspections, most likely due to the fact that a certain event may fall within the relevant competences of different inspections and therefore even a more coordinated approach is necessary.

17. As regards your answer to questions 34/44 of the first questionnaire: Which body is responsible for conveying outgoing requests for data retained in another Member State?

Outgoing requests for data retained in another Member State are subject of judicial cooperation in criminal matters which is conveyed through the Ministry of Justice. In practice this would mean that a requesting body (e.g. Court or District attorney) would have to file a request for international cooperation to the Ministry of justice, who again would either directly or through the Foreign Ministry communicate such request to the addressee state. The reply would then follow the same path.

To this end it should be noted that such requests are applied very rarely and that we have no information on any practical experience with respect to their conveyance and more importantly reliance in criminal cases.

18. Supervisory bodies:

a) Is APEK an independent authority in the sense of what has been said in question 35 of the first questionnaire?

It can be confirmed that APEK is an independent authority within the meaning of question 35 of the first questionnaire.

b) 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 bodies independent in the sense of what has been said in question 35 of the first questionnaire?

Police is supervised internally and by a special department of the State prosecutor's office (prosecuting police crimes). Organisationally Police is further supervised to a certain level also by the Ministry of the interior.

The SISA and the MoD Security department are supervised by a special parliamentary supervisory commission.